Option #1: Final Capstone Portfolio Project

Liam Bergerson

CSU - Global

ITS481-1

D. Morrill

9/10/23

Option #1: Final Capstone Portfolio Project

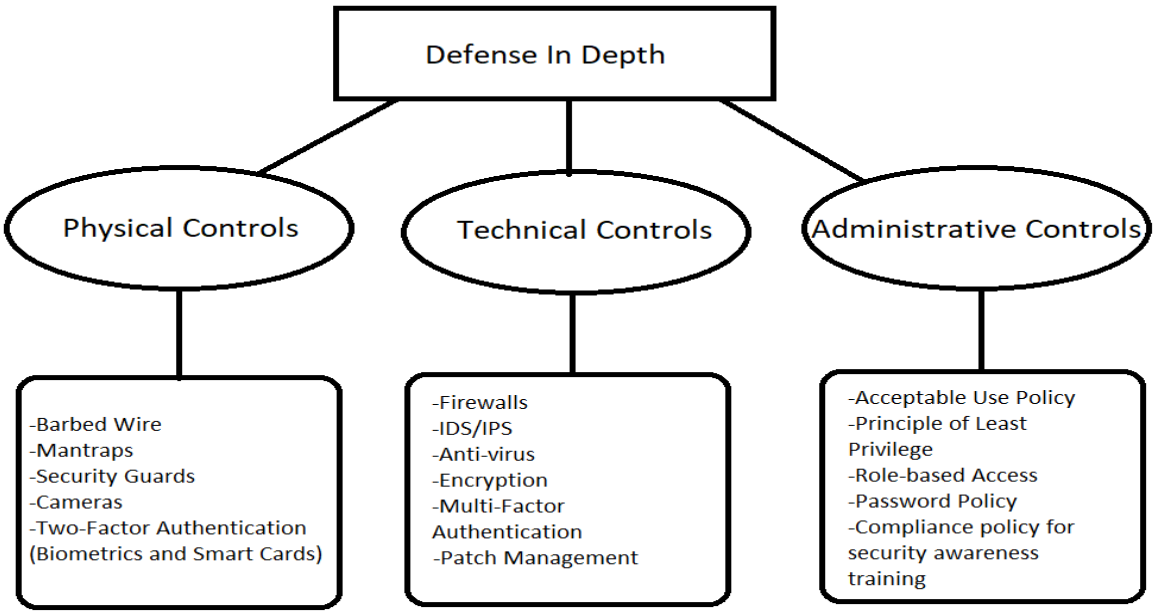
For this capstone project, I will be evaluating security approaches to networking and infrastructure and differentiating those approaches with approaches for securing operating systems. I chose this topic because it is extremely broad and it covers the overall goal of cyber security. It encompases elements of all the topics to choose from for the capstone project including topics not mentioned. This topic can be closely related to a Defense in Depth (DID) approach. A Defense in Depth approach combines physical, technical, and administrative measures to fully secure the organizational infrastructure, network, and the operating systems of each system on the network (Boyens et al., 2012). Measures to secure the physical infrastructure of the building is using smart cards, mantraps, PIN codes, barbed wire, cameras, security guards, etc. (DiMase et al., 2015). Measures to secure the network is using firewalls, Intrusion Detection/Prevention Systems, Demilitarized zones, etc. Measures to secure operating systems is using anti-virus software, encryption software, access control software, etc. Combining all of these aspects will drastically decrease the chances of an organization suffering from a data breach, one of the worst feats an organization can experience.

Project Scope

In this capstone project, security approaches for networking, infrastructure, and operating systems will be defined. However, securing operating systems is slightly different from securing networks and the overall infrastructure. The

difference between securing operating systems and the network and infrastructure will be discussed. In order to determine the scope of this capstone, a Defense in Depth (DID) model will be used. A DID model defines physical, technical, and administrative measures that are to be used to maximally secure the organizations IT infrastructure.

As mentioned before, a DID model has physical, technical and administrative controls that safeguard the IT infrastructure of an organization. The figure below illustrates a diagram of the Defense in Depth model.



Physical controls define what measures are to be used to secure the physical building of the organization. This includes security measures such as barbed wire, mantraps, security guards, cameras, two-factor authentication, etc. There is always a threat that a threat actor may attempt to breach the physical building

and extract sensitive data from the inside. Barbed wire will attempt to deter the threat actor from entering the premises. Security guards and mantraps will verify the authorization of people in order to catch any unauthorized persons. Cameras will record any malicious actions by anyone. Finally, two-factor authentication will secure all doors in the premises, especially ones guarding sensitive data repositories. For the sake of this paper, a fingerprint biometric will be used in conjunction with a smart card for two-factor authentication.

Technical controls define what measures are to be used to secure the network and individual systems of the infrastructure. This includes security measures such as firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), anti-virus, encryption, and multi-factor authentication. Threat actors always try to breach the organization through exploiting vulnerabilities in the network and individual systems. Firewalls will help block any malicious traffic that is not recognized by the firewall. Firewalls also have the capability of opening and closing ports. Threat actors commonly port scan the network to see what vulnerable ports are open, for example, HTTP. A best practice is to always close ports that are not being used. IDS/IPS are used to detect or prevent any malicious traffic on the network. These are typically used in conjunction with firewalls. Anti-virus software will be installed on every individual system to ward off any viruses that are installed on systems. Encryption will be used to encrypt data on repositories or any data that is in transit. This will make it so that threat actors that breach the infrastructure will not be able to use the data unless they

have a decryption key. Finally, multi-factor authentication solutions will be used to secure the login process by requiring the input of a randomly generated number from a third-party application. Securing operating systems are slightly different with securing networks. Securing operating systems usually rely on patch management. Operating systems consistently release patches that fix common vulnerabilities that were found in the previous patch. A patch management plan needs to be implemented to test patches for compatibility with other components and implement them as soon as possible. Network security measures don't rely on patch management as much.

Finally, administrative controls define what measures are to be used to secure the actions of employees. These typically come in the form of policies. Humans are among one of the top reasons security breaches happen. Threat actors exploit the curiosity, helpful and trusting nature, and lack of knowledge towards common security practices that humans typically have (Burnette, 2019). These policies attempt to prevent these vulnerabilities from being exploited. An acceptable use policy will be implemented to define how employees are to use their systems during work hours. This means that casual browsing of the internet will be prohibited, no files are to be downloaded from the internet, and suspicious email attachments will not be opened. The principle of least privilege will be implemented to only give permissions to every employee so that work operations can be performed, nothing more. To implement the principle of least privilege, a role-based access control model will be used. Instead of assigning permissions

for every employee, permissions could be assigned to a role and employees are added to that role. A password policy will be implemented to require employees to create strong passwords and change them every ninety days (WCM, n.d.). Finally, a compliance policy for attending security awareness training will be implemented. This security awareness training will educate employees on how to create a strong password, how to identify phishing emails, and safe internet habits.

Hardware and Software

Now that the scope of the defense in depth infrastructure has been identified, a variety of hardware and software will be needed in order to build a defense in depth infrastructure. A system that will act as the domain controller with Windows Server installed will be used in order to assign permissions to each system that employees will use. This will ensure that the principle of least privilege is implemented along with role-based access. To secure each system from unauthorized individuals, a smart card will be required in order to authenticate into a system (Yfantis, 2021). The Windows Defender firewall is software-based firewall that is an excellent candidate for securing the network. An Intrusion Detection System (IDS) such as the SolarWinds Security Event Manager is a widely known IDS that is an excellent candidate to use in conjunction with the Windows Defender Firewall (Robb, 2023). Regarding anti-virus solutions to use to secure individual systems, a combination of both Windows Defender and Malwarebytes will ensure adequate protection from

viruses. Malwarebytes is a widely known anti-malware solution that is free of charge and properly protects systems from malware. Bitlocker is an encryption software that comes preinstalled on most Windows Operating systems and will be used to encrypt the data that is harbored on Windows systems. Google Authenticator is a multi-factor authentication solution that is used to further secure the login process by requiring the input of a randomly generated number in order to fully log in.

Regarding possible vulnerabilities that will need additional consideration for security measures is vulnerabilities related to web services such as cross-site scripting or SQL Injection. Websites can carry severe consequences if they were to get breached. This is because any databases connected to the website can harbor sensitive data such as credit card numbers. SQL Injection and cross-site scripting are two extremely easy methods that threat actors use to breach websites.

Penetration Testing and Footprinting

In order for the Defense in Depth infrastructure to work effectively, the security measures must be tested to ensure they properly protect the infrastructure. To achieve this, penetration testing and footprinting can be utilized. Penetration testing and footprinting will be highly beneficial for the technical aspect in a Defense in Depth infrastructure. Penetration testing is essentially a security breach drill. The penetration tester acts as a threat actor would act and

try to breach the organization using the same or similar methods a threat actor would use.

The penetration tester would start off with gathering information about the organization, footprinting the infrastructure, infiltrating the infrastructure, escalating privileges, and seeing what data they can access. The organization can implement security measures to protect the individual systems or the network and then a penetration test can be conducted to test those security measures. After the penetration test, the tester can report what vulnerabilities were exploited and the organization will improve existing security measures or implement new ones.

Network and website footprinting are also highly valuable in creating a Defense in Depth infrastructure. Sam Spade is an internet footprinting tool that comes with a graphical user interface and allows the user to perform functionalities such as Whois, traceroute, finger, ping, nslookup, etc. (Atkins, 2013). The main function of Sam Spade is to gather valuable information about a website such as the registry domain ID, the date of creation and when the website was last updated, DNS servers, etc. If this amount of information can be gathered from Sam Spade, this tells the organization that they should use a more secure protocol for their websites, for example, HTTPS. Nmap is another valuable footprinting tool that is mainly used for port scanning networks. Threat actors usually infiltrate networks using open ports on a network. Depending on what ports are open, it may be extremely simple for a threat actor to infiltrate the

network using that port. Nmap can be used to port scan the network and see what ports are open so that unused ports can be closed to prevent threat actors from infiltrating the network through those open ports. Nmap can also be used to check the version of the operating system of the target to see if there are any unpatched vulnerabilities that can be exploited. This function is mainly used for individual systems, however, can be used to see if the organization's patch management plan needs improvement. Superscan is a Windows exclusive tool that is very similar to Nmap in that it can also be used for port scanning, performing TCP SYN scans, and HTML reports (Brinkmann, 2011).

Access Control

In a defense in depth infrastructure, each individual system must be properly secured. Threat actors commonly exploit vulnerabilities within individual systems in order to breach the organization. After they breach the system, they typically escalate the privileges of the victim system to acquire administrator privileges. Access control methods and securing system access are crucial to prevent threat actors from breaching individual systems.

There are many access control methods used in organizations such as Mandatory, Role-Based, Discretionary, and Rule-based Access Control. The method that will be highlighted for discussion is Role-Based Access Control (RBAC). RBAC provides access to every individual user based on a role created within a domain controller (Hoffman, 2022). Instead of assigning permissions individually, a role can be created with permissions assigned and the user is then

added to the role. This saves copious amounts of time when assigning permissions for users. The biggest issue with RBAC is that if a user requires access to files that are outside their role, they will not be able to because of the lack of permissions. An administrator will have to give temporary access to the files for the user.

When configuring RBAC roles, in order to minimize the permissions a user has, the principle of least privilege will be utilized. The principle of least privilege is a concept that states that a user should only have access to the specific data, resources, and applications needed to complete their required tasks and nothing more (Rosencrance, 2021). The principle of least privilege ensures that any threat actors that breach the organization do not have administrator privileges immediately. In order to achieve RBAC, a domain controller with Windows Server installed will be used to create roles and then users are assigned to those roles with the proper permissions.

To safeguard access for all systems, multiple authentication methods will be used. All individual systems will be configured with Single Sign-On (SSO) to ensure that users can securely authenticate with multiple applications and websites by using one set of credentials. When logging into the system itself, the user will be prompted with a username and password. Once the username and password are correctly inputted, the user will then have to scan a smart card to fully access the system. A token-based authentication solution will work as well, however, there are more risks associated with token-based authentication.

Token-based authentication requires constant revalidation of keys and can cause severe consequences if a key is compromised. For example, any applications or websites under a SSO login are compromised if a token that is used to authenticate into the SSO is compromised. Smart cards do not require constant revalidation, but they are, however, more expensive than tokens due to the card readers required.

Methods for Alerts and Notifications

When configuring the technical side of a defense in depth infrastructure, it's important that alerts and general texts such as notifications are implemented. Alerts and notifications are both essential aspects for improving network performance and monitoring (Hein, 2019). Not only do alerts and notifications address problems with network performance, they may notify the security team if there is a potential security breach. It's important to distinguish that an alert is serious and needs to be addressed right away whereas a notification is less serious. For example, a notification when there is a scheduled server maintenance.

Network alerts and notifications can be distributed throughout the network through means of email or text message (Barney, 2023). Both email and text message can be used for alerts and notifications depending on personal preference or severity of the alert. For example, once the alert and notification solution is configured, a form can be distributed to all employees of an organization. Employees can fill out that form whether they would prefer alerts

and notifications in an email or a text message. For more severe alerts, a text message will be used instead of email in order for employees to see it immediately.

Development Processes

Application development is absolutely essential for organizations as it is the process of creating computer programs to perform different tasks that the organization requires. These tasks can be scheduling sales reports, automating processes and increasing efficiency, etc. Within my project, the pros and cons of consumer off-the-shelf development processes and development processes built from scratch will be discussed and one will be chosen for use. It's crucial that whichever method is chosen, that it is secured. Methods to secure the application development process will be discussed as well.

Off-the-Shelf Development Process

Off-the-shelf development processes are essentially software solutions that can be purchased that will allow developers to create applications using preconfigured tools (Quilliam, 2020). Pre-built solutions are initially reasonably priced and quick to implement. The solution is typically updated by the vendor so the organziation doesn't have to fret about updating it. Customer support and community support is also a huge advantage that prebuilt software solutions have if there are any problems that occur. Since prebuilt solutions are owned and managed by the vendor, there is little customizability that the organization has. This has to be considered when choosing a prebuilt software solution. In the long

term, the solution may become quite expensive. Depending on the solution, it may have too many or too few functions that can only be discovered through use of the product after purchase. Finally, it may have issues with integration with other applications.

Development Processes Built From Scratch

With building a development process from scratch, the pros and cons are basically reversed from off-the-shelf development processes. Since it is built by the organization, customization is maximized. It is entirely up to the organization on what functions are included and how they operate. There is greater control with security measures, updates, etc. since the organization has complete ownership (Yurevich, 2022). There is also guaranteed integration since any issues can be solved immediately. There is, however, a significant upfront cost and time for creation as buying the required resources can be quite expensive. The development process creation can take weeks or even months which is detrimental if application development is needed immediately. However, if time is of no concern, the benefits in the long term are worth it.

Securing the Development Process

For the purpose of this project, off-the-shelf software solutions will be utilized for their reasonable price and fast deployment. Since an application development method has been chosen, it's crucial that it is properly secured. Methods and best practices can be used to secure the development process. The OWASP top ten is the top ten security vulnerabilities as it relates to

application development (OWASP, 2021). Security measures must be implemented that patch the vulnerabilities mentioned in the OWASP top ten. Some of the vulnerabilities mentioned in the top ten is SQL injection, broken authentication and session management, cross-site scripting, etc. Some measures to protect against these attacks can be data filtering, strong passwords, session timeout, and data validation and sanitization. Proper logging will ensure that anomalies can be responded to quickly. Encryption of everything will ensure that threat actors cannot read the data without the decryption key. Finally, servers must be properly patched to the latest version to fix present vulnerabilities.

Cloud Integration

Cloud computing is widely used by many organizations as it abstracts the physical components of a computer. An organization can basically run a computer without owning the equipment. This is because a cloud vendor owns and manages all of the equipment needed for the data center. The consumer must subscribe to use the resources of the cloud vendor. This is the case for a public cloud model. For a private cloud model, an organization has to purchase and manage the equipment for a data center. The possibility for cloud integration for this project is very much possible and will, in fact, be used. For the purpose of this project, a public cloud model will be used. Amazon Web Services (AWS) is a popular and reliable public cloud service that is used by many organizations. AWS has a pay-as-you-go model, meaning that you only pay for the services that

are used. Basically, it's not a flat payment plan, it's based on usage time. In times where network traffic is elevated, more resources such as CPU and RAM can be provisioned in minutes and can be released just as quick when they are no longer needed. This is called rapid elasticity. Rapid elasticity is the main reason why cloud computing will be used within this project. The storage benefits that cloud computing brings will also be highly beneficial since data can be accessed anywhere at any time.

Conclusion

Throughout this project, a defense in depth infrastructure has been properly discussed including physical measures, administrative controls, and an emphasis on technical controls. The reason for the emphasis on technical controls is that the network and system infrastructure is the most likely to be exploited in a security breach. Whether it be improperly patched systems, default router configurations, SQL injection, etc., the technical side is the one with the most vulnerabilities. Properly securing the technical controls will ensure that vulnerabilities within the defense in depth infrastructure are minimized and work operations are efficiently and effectively performed.

References

Atkins, S. (2013, December 10). *Sam Spade*. LO4D.com. https://sam-spade.en.lo4d.com/windows

Barney, D. (2023, August 11). Network Alerts—Monitoring and Notifications. *What's up gold*. https://www.whatsupgold.com/blog/network-alerts-monitoring-notifications

Brinkmann, M. (2011). Port scanning networking tool SuperScan. *gHacks Technology News*. https://www.ghacks.net/2008/08/11/port-scanning-networking-tool-superscan/

Boyens, J. M., Paulsen, C., Bartol, N., Shankles, S. A., & Moorthy, R. (2012). *Notional supply chain risk management practices for federal information systems*. https://doi.org/10.6028/nist.ir.7622

Burnette, M. (2019, June 10). *The humanity behind cybersecurity attacks* [Video]. TED Talks. https://www.ted.com/talks/mark_burnette_the_humanity_behind_cybersecurity_attacks

DiMase, D., Collier, Z. A., Heffner, K. H., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, *35*(2), 291–300. https://doi.org/10.1007/s10669-015-9540-y

Hein, D. (2019, October 24). *The essential features of network monitoring alerts*. Best Network Monitoring Vendors, Software, Tools and Performance

Solutions. https://solutionsreview.com/network-monitoring/the-essential-features-of-network-monitoring-alerts/

Hoffman, B. (2022, August 3). Access control: models and methods. *Delinea*. https://delinea.com/blog/access-control-models-methods

OWASP. (2021). *OWASP Top Ten | OWASP Foundation*. https://owasp.org/www-project-top-ten/

Quilliam, E. (2020, May 4). *The Complete Advantages and Disadvantages of Off the Shelf Software*. IT Enterprise. https://itenterprise.co.uk/off-the-shelf-software-pros-cons/

Robb, D. (2023). SolarWinds Security Event Manager – SIEM Product Overview and Insight. *eSecurityPlanet*. https://www.esecurityplanet.com/products/solarwinds-log-event-manager/

Rosencrance, L. (2021). principle of least privilege (POLP). *Security*. https://www.techtarget.com/searchsecurity/definition/principle-of-least-privilege-POLP

WCM. (n.d.). *11.15 - Password Policy and Guidelines | Information Technologies & Services*. Weill Cornell Medicine. https://its.weill.cornell.edu/policies/1115-password-policy-and-guidelines

Yfantis, V. (2021, November 11). Smart Card Authentication | Raise your security levels to a higher standard. *Parallels Remote Application Server Blog -*

Application virtualization, mobility and VDI.

https://www.parallels.com/blogs/ras/smart-card-authentication/

Yurevich, D. (2022). *For New Software, Build vs. Buy: Pros and Cons for your Business*. https://www.syberry.com/blog/build-vs-buy