**Project 2: Security Strategy Implementation Recommendations for Sifers-Grayson**

**Reece Zunino**

**CSIA 310 (6380)**

**7/9/2023**

**Introduction**

There have been two defense strategies chosen to be recommended for implementation into Sifers-Grayson’s Cyber Security infrastructure. One recommended defense strategy is utilizing a demilitarized zone (DMZ) for the R&D center. This strategy will involve using Linksys Business Gigabit VPN Routers to protect and secure the department so that engineers can securely telework from the test range without compromising the network. “Linksys Business Gigabit VPN Routers allow OpenVPN clients to run on employees’ laptops, smartphones, and tablets to connect to the offices using two-factor authentication” (Linksys, 2015). This hardware needs to be purchased by the organization so that the R&D network is protected against attacks. This product will also enhance the department’s firewall against unauthorized users attempting to access the network. These products can be deployed remotely and do not require them to be in a structure. This way, the engineers may utilize them as necessary, and they can be secured when not used.

To accommodate the Linksys VPN router for the DMZ, we recommend using Sonicwall’s network security firewall for your network-based firewall solution. With Sonicwall firewall technology, you can access their network security management tool. “SonicWall Network Security Manager (NSM), a multi-tenant centralized firewall manager, allows you to centrally manage all firewall operations error-free by adhering to auditable workflows” (SonicWall, 2023). We recommend using the McAfee network security platform for your organization’s intrusion detection and prevention system. “McAfee Network Security Platform is a uniquely intelligent security solution that discovers and blocks sophisticated threats in the network. Using advanced threat detection techniques, it moves beyond mere pattern matching to defend against stealthy attacks with extreme accuracy, while its next-generation hardware platform scales to speeds of more than 20 Gbps with a single device to meet the needs of demanding networks” (McAfee, 2013).

The other recommended defense strategy is just as critical as the previous one. This strategy requires recommendations of applications and tools to help secure Sifers-Grayson’s IT infrastructure and not just the R&D department. The applications and tools that we will be focusing on will be an Application Lifecycle Management (ALM) tool from V/SURE, an Identity & Access Management (IAM) tool from SolarWinds, the FTK imager tool as a forensic image capture utility tool, and an Event Management (SIEM) application tool from SolarWinds. For these applications to be implemented, a significant amount of funding must be available for your IT security infrastructure. Some of these tools and applications that have been recommended have multifunction capabilities and will give you the most security for your money. Based on the Red Teams reports Sifers-Grays lacked the capabilities to thwart or even detect an attack in progress. Therefore, these applications and tools are necessary to secure your organization’s IT infrastructure. Implementing defense layers such as these recommendations will help detect, contain, and eradicate threats to your organization while ensuring your company’s information is secure and you comply with Department of Defense (DOD) regulations.

**Security Strategies for Sifers-Grayson**

We will start by securing the R&D department as our first strategy. The R&D department was the most vulnerable during the penetration test and housed your organization’s proprietary information and intellectual property. Since there was a critical point of failure in the security infrastructure, we need to implement more layered security to detect and prevent unauthorized access to the network. Implementing a backup system into the network will help prevent data loss if the network becomes compromised, and the information can be reconstituted after the threat has been eradicated. The systems that will be implemented will help patch all known vulnerabilities that were flushed out during the penetration test. These protections will help prevent and mitigate attacks from internal and external threats. The types of layers we recommend implementing into the security layers are web protection, anti-spam firewalls, vulnerability assessment data encryption, email security, digital certificates, antivirus software, privacy controls, and patch management. We also recommend adding VPNs to the networks DMZ: “In addition to providing greater privacy than secured Wi-Fi hotspots, VPN services establish secure and highly encrypted connections” (Lakhwani, 2023).

The second strategy that we recommend your organization implement is a defense in depth strategy. “Defense in depth is a strategy that leverages multiple security measures to protect an organization's assets. The thinking is that if one line of defense is compromised, additional layers exist as a backup to ensure that threats are stopped along the way. Defense in depth addresses the security vulnerabilities inherent not only with hardware and software but also with people, as negligence or human error often cause a security breach” (Fortinet, 2023). This network security strategy will help secure the organization’s systems and have redundancies in place in case of a more severe attack. This implementation will also create technical, physical, and administrative controls not currently in place across your network. These controls will help prevent attacks and ensure that the company data is not easily compromised as during the penetration test.

**Product Evaluations**

The recommended products will help improve your organization’s security posture and introduce a layered security system throughout the network, including creating the DMZ at the R&D department. With defense in depth, some defensive resources – troops, fortifications, weapons – are further back so that if the front is breached, troops and materiel are still available to stop the enemy advance. In the military context, even if less concentration in the first level makes it easier for the enemy to make an initial breach, they can be ultimately stopped more quickly because their losses will continue to grow as they continue to try to work their way toward the goal (ERICOM, 2023). We recommend Antivirus products from MacAfee to protect against malware, spyware, viruses, Trojans, phishing attacks, spam attacks, and rootkits. The products we recommend are critical to securing the organization’s network and are needed to prevent many different styles of attacks, like what was found in the incident report provided by the Red Team.

Some other products we recommend are VPN routers from Linksys, SEMI tools from SolarWinds, business class firewall by Sonic Wall, application lifecycle management tools, identity and access management tools, security information, and event management tools, and forensic image capture software. All of these tools and applications will create a robust security network to ensure that your information is secure, safe, encrypted, and backed up so that you can implement a proper recovery phase in case of another incident.

**Recommended products for Sifers-Grayson**

**Defense Strategy #1 (Build a DMZ for the R&D Center)**

**Business Class Router with WAP and VPN capability**

* Business Dual WAN Gigabit VPN Router (LRT224): This router has the capabilities and requirements to allow Sifers-Grayson to communicate securely with the test site (Linksys, 2015).

**Business Class Firewall (network-based)**

* SonicWALL NSa SERIES NEXT-GENERATION FIREWALL (NGFW): The SonicWall Network Security appliance (NSa) Mid-Range Firewall is next-generation security explicitly designed for businesses of 250 users and up (SonicWall, 2023).

**Intrusion Detection and Prevention System (network-based)**

* McAfee Network Security Platform: McAfee Network Security Platform is a uniquely intelligent security solution that discovers and blocks sophisticated threats in the network (McAfee, 2013).

**Defense Strategy #2 (Implement enterprise-wide protection, detection, and prevention capabilities)**

**Application Lifecycle Management (ALM) Tool**

* Visure ALM: Enforce full traceability across the entire development cycle to accelerate product & systems development and standard compliance (Visure, 2023).

**Identity & Access Management (IAM) Tool**

* SolarWinds Access Rights Manager: Compliance requirements driven by GDPR, PCI, HIPAA, and other mandates require detailed user access monitoring, particularly for users accessing critical and sensitive data (SolarWinds, 2023).

**Security Information and Event Management (SIEM)**

* SolarWinds SIEM Tools: SIEM tool is designed to streamline and automate key tasks related to both SIM and SEM by delivering monitoring and collecting security log data from sources to provide an overview of possible network threats that would be nearly impossible to detect when using separate, basic tools or with manual efforts (SolarWinds, 2023).

**Forensic Image Capture Utility**

* FTK Imager: FTK Imager is a tool for creating disk images and is absolutely free to use. The Access Data Group developed it. It is a tool that helps preview data and imaging (Zhohadamani, 2022).

**Summary Implementation Recommendations**

Implementing both strategies focusing on layered security and defense in depth, will enhance the organization’s security posture and enable team members to have better detection and response times in case of an attack. “Layered security has long been a significant element of many organizations’ security strategy. In IT, layered security means protecting digital assets with several layers, each layer providing an additional defense” (ERICOM, 2023).

Having network-based security solutions will also enable a more hardened security infrastructure. These security solutions also come with great detection tools like the SonicWALL network management detection program that gives you a complete overview of your network’s security status. Also, Identity and access management systems enable your organization to manage a range of identities, including people, software, and hardware like robotics and IoT devices.

Creating a defense-in-depth security program will also bolster your security systems by implementing controls in all areas, from physical controls to behavioral analysis. With these recommendations and well-known branded security devices, Sifers-Grayson will have impeccable overall protection.

**References**

CrowdStrike. (2023). CrowdStrike | Free 15 day trial. CrowdStrike: Stop breaches. Drive business. https://go.crowdstrike.com/try-falcon-antivirus.html?utm\_campaign=falcontrial&utm\_content=ecom-treq-en-fpro-tct-us-psp-smb-trl-anti-x\_x\_x\_x-x&utm\_medium=sem&utm\_source=goog&utm\_term=antivirus%20for%20business&gad=1&gclid=Cj0KCQjwkqSlBhDaARIsAFJANkh8aZh9lpvlh4kg3F811bX1xipct5XpY46eyvbuFdcZSNpYJNMKdB0aAiXrEALw\_wcB

ERICOM. (2023, February 16). What is layered security? Ericom Software. https://www.ericom.com/glossary/what-is-layered-security/

Fortinet. (2023). What is defense in depth? Defined and explained. https://www.fortinet.com/resources/cyberglossary/defense-in-depth#:~:text=Defense%20in%20depth%20is%20a,are%20stopped%20along%20the%20way

Lakhwani, S. (2023, June 19). Fundamentals of cybersecurity [The basics guide]. KnowledgeHut: Professional Bootcamps and Certification Courses Provider for your Future. https://www.knowledgehut.com/blog/security/cyber-security-fundamentals

Linksys. (2015). Linksys Business Gigabit VPN Routers. Index document. https://downloads.linksys.com/downloads/datasheet/en/LRT214\_LRT224\_English.pdf

McAfee. (2013). McAfee Network Security Platform. McAfee Products & Solutions | WebSecurityWorks.com. https://www.websecurityworks.com/datasheets/ds-network-security-platform-m-series\_new.pdf

OneLogin. (2023). What is identity & access management (IAM)? | OneLogin. OneLogin: Market-Leading Identity and Access Management Solutions. https://www.onelogin.com/learn/iam

Scarfone, K. (2021, January 6). Top 10 cybersecurity best practices to protect your business. SearchSecurity. https://www.techtarget.com/searchsecurity/tip/10-cybersecurity-best-practices-and-tips-for-businesses

SolarWinds. (2023). Access rights manager (ARM) software. Observability and IT Management Platform | SolarWinds. https://www.solarwinds.com/access-rights-manager?irclickid=2wR1wXyhwxyNRkCxC-XsQxInUkFz3HTO83QqRU0&irgwc=1&CMP=BIZ-TAD-CTECH-SW\_WW\_X\_X\_PPD\_DR\_EN\_0\_0-ARM-X\_0\_X\_X\_X\_X-X

SolarWinds. (n.d.). SIEM tools - Security event monitoring software guide | SolarWinds. IT Management Software and Observability Platform | SolarWinds. https://www.solarwinds.com/security-event-manager/siem-tools

SonicWall. (2023). Network Security Manager. https://www.sonicwall.com/products/management-and-reporting/network-security-manager/. https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf

Tittel, E., & Brush, K. (2022, April 25). What is application lifecycle management (ALM)? Software Quality. https://www.techtarget.com/searchsoftwarequality/definition/application-lifecycle-management-ALM?Offer=abMeterCharCount\_var2

Visure. (2023, June 23). Start free trial | Visure vs JAMA. Visure Solutions. https://visuresolutions.com/free-trial/jama?utm\_source=google\_ads&utm\_medium=ppc&utm\_campaign=jama&gad=1&gclid=Cj0KCQjwtamlBhD3ARIsAARoaExq19dUIUman6-sX54G0-ADr5br1NmG9QN2aHU-uBu0hgTNtwEIvlwaAuI1EALw\_wcB

Zhohadamani. (2022, September 5). How to create a forensic image with FTK Imager? GeeksforGeeks. https://www.geeksforgeeks.org/how-to-create-a-forensic-image-with-ftk-imager/