Option #1: Performing an IT Audit (paper)

Liam Bergerson

CSU - Global

ITS462-1

N. Braun

7/9/23

Option #1: Performing an IT Audit (paper)

A software development organization has hired me to perform an IT audit of their infrastructure, operational procedures, and processes. An IT audit can be highly beneficial for an organization because it thoroughly examines the IT infrastructure of an organization (uCertify, 2016). This includes elements such as applications, data use and management, policies, and standards. In this paper, IT environment characteristics such as network infrastructure and software-development practices will be discussed. Operational and security concerns are always present within an IT environment and will be discussed as well. Finally, to address the operational and security concerns, measures to safeguard assets and data will be recommended.

Characteristics of an IT Environment

An IT environment is the infrastructure consisting of hardware, software, and systems that a business relies on every day in the course of using Information Technology (Farrelly, 2022). There are three components that make up an IT environment: hardware, software, and networking. Hardware consists of routers, personal computers, servers, switches, and data centers. Software consists of web servers, applications, and databases. The networking components consist of firewalls, cables,

Demilitarized Zones (DMZs), etc. To discuss networking in more detail, all three components discussed above are included in networking. Servers consist of computers that hold operating systems and software applications that allow multiple computers to run together (Carklin, 2022). Network cables allow media to be transmitted to and from servers. Network switches allow data to be forwarded to the intended recipient and only the intended recipient. Routers essentially perform the same function as switches except they route data to and from networks, not individual systems. Firewalls are the most basic security measure within networks. They inspect network packets and determine if a particular packet should be allowed into the network or blocked from entering the network. To determine whether packets are allowed or blocked, network administrators give rules to the firewall on what packets to allow or block. Network software can be used to monitor the network. Finally, network protocols are services that set rules on how applications and network devices communicate with each other. For example, Hypertext Transfer Protocol (HTTP) is the protocol used to determine how data is exchanged from a system to a web server.

Multiple software development practices can be used to ensure code is written efficiently and effectively for all applications. Foord (2017) gives thirty best practices for software development. However, the ones I feel are

most important will be discussed. YAGNI is a popular acronym that stands for “You Ain't Gonna Need It”. This acronym is used to tell developers not to write code that they think they will need in the future. The future is never set in stone. If the code that has been preemptively written is no longer needed, they wrote unnecessary code. Code should only be written when it is needed at that moment in time. Code can go wrong and need maintenance over time. Less code should be written, code should be deleted when it is no longer necessary, and code that is not needed should not be written. When writing code, the worst case scenario should always be in mind. This will help the developer to catch bugs in the code before they happen. If a function in the code goes past thirty lines, it should be broken up into multiple functions.

Operational and Security Concerns

Every year, threat actors discover new ways to exploit vulnerabilities within the network infrastructure of organizations. This section will discuss some of the most common threats towards security and operations within organizations. Internal security threats make up a majority of the security threats. These are often caused by human error whether it be falling for a phishing attack, careless decision-making, using weak passwords, etc. These internal security threats can negatively impact business operations

and can result in the loss of sensitive data, server downtime, loss of revenue, and disgruntled clients. Distributed Denial-of-Service (DDoS) attacks target servers and websites. The goal of a DDoS attack is to completely crash, malfunction, or ensure servers have slow loading times (Latif et al., 2014). A DDoS attack is especially dangerous because it uses infected computers as a botnet to flood servers and websites with an extremely high number of packets that eventually crashes the server or website. Malware are malicious software programs that are typically used to gather information about victims through compromised devices. After the malware is successfully installed on the system, the threat actor can search for sensitive data and use them to commit identity theft or sell them on the dark web. Ransomware is a form of malware that encrypts sensitive data and forces the organization to pay for the decryption key that is used to decrypt the sensitive data. This attack is especially dangerous because the threat actor can easily collect the payment and refrain from giving the decryption key to the victim. Also, depending on how well the malware is crafted, it can encrypt the backups of sensitive data as well. Rogue security software is also another form of malware that tricks organizations into believing their infrastructure is infected with malware. This fake software will spam the user with warnings and coerce them into paying for a

nonexistent security solution. This malware can also corrupt pre-existing security programs to prolong the attack. Viruses are another type of malware, but slightly different than, for example, worms and trojan horses. Viruses rely on the user executing the file that the virus resides in. The virus cannot affect the system until that file is executed whereas worms and trojans do not require the execution of a file. Finally, phishing attacks are scams where threat actors disguise themselves as a trusted entity and attempt to coerce the victim into unintentionally providing the threat actor access to their system. These attacks typically take form in emails, but can appear in text messages or phone calls. These malicious emails appear to be legitimate and will encourage the victim into clicking a link included in the email. These malicious links typically have malware associated with them and will be installed onto the system when the victim clicks on the link. Spear phishing and whaling are two forms of phishing that targets specific people using collected information about them such as known friends or relatives. They will then pose as that relative or friend and perform their attack. Whaling is the same thing as spear phishing, but attempts to go after a high ranking member of management in organizations such as members of the C-suite.

Methods For Safeguarding Assets

Multiple methods can be used to prevent the threats discussed above from affecting organizations, protect assets, and ensure data integrity. To safeguard assets and ensure data integrity, the network infrastructure must be secured. This includes implementing properly configured firewalls, intrusion detection systems, and proper router configuration. A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic determined by the configured rules (Cisco, 2023). A properly configured firewall should block all unused ports and block certain protocols that are associated with DDoS attacks, for example, Address Resolution Protocol (ARP). An Intrusion Detection System (IDS) should be installed so that suspicious network traffic can be caught before it affects systems on the network. Anti-virus solutions should be installed on all systems to block any viruses that are logged in the virus database in the solution from affecting systems. Proper research of anti-virus solutions should be performed to ensure that the solution will effectively eradicate any viruses. Proper training and education will be required in order to educate employees about phishing attacks, how to spot them, and what to do if an employee encounters a phishing attack. This will lower the chances of an employee falling for a phishing attack.

Encryption methods should be implemented for data at rest and data in transit. Symmetric encryption uses one key for encrypting and decrypting and will be used for data at rest. Asymmetric uses one key for encrypting and another key for decrypting and will be used for data in transit. Finally, a few policies will ensure that internal security threats are mitigated. A password policy will ensure that all employees use strong and complex passwords that are at least eight characters with the inclusion of upper and lowercase letters, numbers, and special characters and change them every ninety days (WCM, n.d.). This policy should require employees to use a multi-factor authentication solution provided by the organization to further protect the login process. A multi-factor authentication solution typically requires the employee to input a randomly generated number after inputting the password to log in. A policy that outlines proper internet habits will ensure employees are not freely browsing the web and visiting random websites while on company systems on shift. This will lower the chance of the employee accidentally installing malware from malicious websites. Finally, a compliance policy for user education training seminars will be required. These seminars will teach employees how to safeguard their general internet habits and protect themselves from phishing attacks.

Conclusion

By outlining the IT infrastructure of this software-development organization such as hardware, software, and network elements, the management of this organization can better understand how an IT audit can identify certain threats towards security and operations of this organization as well as outline methods in order to safeguard assets and ensure data integrity all while the organization operates effectively in order to achieve goals and objectives.

References

Carklin, N. (2022, August 25). What is Network Infrastructure? *Parallels Remote Application Server Blog - Application virtualization, mobility and VDI*. https://www.parallels.com/blogs/ras/network-infrastructure-definition/

Cisco. (2023, March 15). *What Is a Firewall?* https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Farrelly, J. (2022). What is an IT Environment? *Electric*. https://www.electric.ai/blog/what-is-an-it-environment

Foord, M. (2017). *30 best practices for software development and testing*. Opensource.com. https://opensource.com/article/17/5/30-best-practices-software-development-and-testing

Latif, R., Abbas, H., & Assar, S. (2014). Distributed Denial of Service (DDoS) Attack in Cloud- Assisted Wireless Body Area Networks: A Systematic Literature Review. *Journal of Medical Systems*, *38*(11). https://doi.org/10.1007/s10916-014-0128-8

uCertify. (2016). *CISA Certified Information Systems Auditor Study Guide*. John Wiley & Sons.

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