**CYB 250 Final Project**

Douglas Few

Southern New Hampshire University

August 20, 2021

Recently, we have unveiled a new technology within our company. This technology will allow our technicians working in the field to access files and data stored within the shared drive on our network. This data will be accessible via an optical screen on a headset that will be equipped by the technician. The headset will constantly communicate with the network located in the central office, and will connect to the server through the technician’s cell phone via bluetooth. By utilizing this headset, the technician will have the ability to view schematics, emails, or invoices completely hands-free.

Human Factor

This new technology brings with it a lot of benefits, one of which being the ability to minimize the effects of social engineering techniques. Human error is inevitable, and anyone can be susceptible to tactics like “shoulder surfing,” where an individual will hover over the shoulder of another in order to steal their credentials (Business Tech Weekly, 2021). This method allows the person to go back at a later point with falsely obtained credentials to gain access to unauthorized information. This could be a PIN number at an ATM or login information at an employee terminal. By designing our newly unveiled device as a headset, we can virtually guarantee that no one other than the authorized user can access confidential information. Shoulder surfing no longer becomes a threat because potential attackers aren’t able to see the monitor mounted in the device.

A risk that we have to take into consideration when releasing our new wireless headset is the possibility of theft. With technological equipment that is either handheld or small enough to be portable, there is always the possibility that the equipment will either be lost or stolen. If this were to happen, any emails, schematics, or other information already open or downloaded on the headset would be available to whoever currently has it in their possession. Even worse, if the technician’s smartphone still happens to be in range of bluetooth, the thief that has possession of the headset would have full access to all of the information the technician had available at the time.

In order to combat this potential risk, I have a couple solutions that I would like to recommend. My first recommendation would be to install capabilities on the headset that can recognize when the device has been removed. Once the device realizes that it has been removed, it would automatically log the user out so any information currently being accessed would remain confidential. My next solution would be to set the headsets up so that they log out whenever they are disconnected from bluetooth. This way, in the event of a lost or stolen device, all confidential information will be safe so long as the technician either turns their bluetooth off or leaves the bluetooth range. While this solution may seem simple, I believe that it would serve as an excellent fail-safe when implemented along with my other recommendation.

With the emergence of social engineering trends, cyber security professionals are being put into a position where they have to be creative when it comes to combating certain techniques. Trends like shoulder surfing and phishing scams are what led to the popularity of multi-factor authentication. Multi-factor authentication is a process that increases security by asking a user to verify their identity more than once during a login attempt (McKeown, 2020). This is normally done by sending an email or text message to a predetermined email address or phone number whenever a login attempt is noticed. Even if a user’s login information is stolen, if multi-factor authentication is in place, an unauthorized login attempt will be stopped and the user will be alerted of the attempt.

Data Protection Strategy

While the headset is secure against many social engineering techniques, no device that is connected to the internet can be completely secure on its own. Without some form of digital security, this new technology would easily succumb to a multitude of cybersecurity failures. One major suggestion would be the use of a virtual private network, or VPN (Janssen, 2021). The VPN will act as a sort of tunnel for all incoming and outgoing traffic that passes through it. When the user of the VPN sends data to the internet, the VPN will encrypt the data and pass it on to the VPN server. The server will then decrypt the data and pass it on to its intended recipient. Likewise, when the user receives data, the data is first encrypted by the VPN server. That information is then decrypted by the VPN software on the user’s device upon arrival. Through this method of encryption and decryption, all confidential data is protected and secure against any potential criminal actors that may attempt to connect to the device.

Of course, even virtual private networks have their risks and disadvantages. Greenfield (2020) outlines 5 specific drawbacks that enterprises should be aware of when using a VPN. The most important drawback from a security perspective is the lack of granular security. This is to say that VPNs often give even low-level employees access to networks that should only be available to network administrators. This problem opens the network up to data breaches and malware, because granting administrative privileges to an employee that doesn’t have the training or knowledge to handle those privileges can lead to that individual making damaging changes to the network.

System Protection

In the modern age, it is almost impossible to run a business without having some form of online presence. For this reason, the network of a corporation can be one of its most valuable assets. Without network protection technologies, a business can be destroyed by a cyber attack if the supposed attacker has enough malicious intent. Network protection technology comes in a number of different forms, and each technology serves its own purpose in its own way (Cisco, 2021). Each of these technologies, however, share the same goal of protecting a network from potential harm. Whether you are using a VPN to encrypt and decrypt network traffic or anti-virus/anti-malware software to keep your network healthy, network protection technology serves to protect data from corruption and theft.

Due to the online nature of the headset, network protection seems to be the most reasonable form of protection. The amount of confidential data that our field technicians will be handling via the optical screen in the headset warrants ensuring that the data remains confidential.

References

Business Tech Weekly. (2021). *What is shoulder surfing?* BusinessTechWeekly.com. https://www.businesstechweekly.com/cybersecurity/password-security/what-is-shoulder-surfing/.

Cisco. (2021, June 28). *What is network security?* Cisco. https://www.cisco.com/c/en/us/products/security/what-is-network-security.html.

Greenfield, D. (2020). *The disadvantages of VPNs for enterprises*. Cato Networks SASE Cloud Platform. https://www.catonetworks.com/blog/the-disadvantages-of-vpns-for-enterprises/.

Janssen, D. (2021, August 3). *VPN explained: How does VPN work and Why would you use it?* VPNoverview.com. https://vpnoverview.com/vpn-information/what-is-a-vpn/.

McKeown, E. (2020, September 3). *What is multi-factor Authentication (MFA) and how it WORKS*. PingIdentity. https://www.pingidentity.com/en/company/blog/posts/2017/what-is-multi-factor-authentication-mfa.html.