**CYB-250**

**Short Response: Breach Analysis**

**Candace Ralston**

**2/1/2023**

The audience that I am using for the reporting the breach that was seen during the audit is the senior management. I would be telling them that there was a breach that was identified during a routine audit. The breach calls into question the safeguards that the company has in place (snhu.edu). I have to inform them that the safeguards need to be replaced or updated so this breach doesn’t happen.

First we need to find out what caused the breach and how it happened. I talked with the CIRT team and they found out that a port was mistakenly left open (snhu.edu). A client machine was communicating with another client machine on an isolated network and the port that they were using was left open (snhu.edu). This happened after the configuration files was moved three weeks prior. So, this means that the network was open to the attack. I would explain to management that basically what happened is that one of the clients computers was communicating with another on the network. This opened a back door that was left opened and no one knew that it was left open. Then someone else found this back door and decided to take advantage of it.

We do have a way to prevent this from happening that is already in the network. It is called subcontrol 12.2 or the Scan for Unauthorized Connections Across Trusted Network Boundaries (snhu.edu). This only specifies that we should scan for this type of thing monthly, I am saying that we should update the scans to be run on a daily basis. This would take time and resources to do but it would stop these types of breaches from happening. We need to update the policy in this manner to keep the network more secure. It would also mean changes to the company but if it is not done more breaches like this will happen and next time it might not get seen until something like a Denial of Service (DDoS) attack could happen. This is where the hackers aim to over whelm the website and the online services with more traffic than the server can handle. This is why it is important to update or get new security devises and software.

The other best subcontrol that should also be used would be the 1.4 device (media.snhu.edu). This would maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. With this inventory it shall include all hardware assets, whether it be connected to the organization’s network or not. With this subcontrol we would be able to maintain all the devices and keep them up-to-date on all security and other updates. Another subcontrol would be the 2.7 application where it utilizes application whitelisting (media.snhu.edu). This utilizes application whitelisting on technologies on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets. What this means is that any software that can be dangerous can be blocked before it can do harm. With these subcontrols we would have a better chance of making sure breaches don’t happen.

On top of the other security measures, it has been also proposed that an RSA encryption as be implemented. The data is encrypted by using what’s called a public key, which is then decrypted by using a private key. This method encrypts the secret DES key so that it can be used over the network, but it will encrypts and decrypts the actual message using the faster DES algorithm. This will work well with the Virtual Private Network (VPN) that we already have. Other forms of VPN that we can use are remote access, which connects a device outside to the corporate office. Another one would be a site-to-site, which connects the corporate office to branch offices over the Internet (cisco.com).

**References**

[Articulate Word Output (snhu.edu)](https://learn.snhu.edu/content/enforced/1252377-CYB-250-T3405-OL-TRAD-UG.23EW3/course_documents/CYB%20250%20Module%20Five%20Short%20Response%20Text%20Version.pdf)

[cis\_controls\_v7.pdf (snhu.edu)](https://snhu-media.snhu.edu/files/course_repository/undergraduate/cyb/cyb250/cis_controls_v7.pdf)

[What Is a VPN? - Virtual Private Network - Cisco](https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html#~how-a-vpn-works)