Network Security Report

Prepared by: Isabelle Jaber

Date: July 29th, 2024

Table of Contents:

ATTACK SURFACE ANALYSIS

Endpoints and Devices

The current network architecture comprises cloud resources, Wi-Fi access points, point-of-sale (POS) terminals, servers, front desk endpoint terminals, servers, and x-ray technology. All of the devices should be properly patched and updated. All patches and updates to the Electronic Health Records (EHR) System, dental imaging system, and front desk endpoints, occur monthly. This can be confirmed with logs, and tracking the release of updates from the manufacturers.

Network Layer

The external IP addresses are 139.60.168.191 for the SoHo location, 139.177.192.141 for the Midtown location, and 139.48.0.109 for the Park Slope location. The internal IP address range for the organization's assets is 192.168.0.0/24. As of now, it is unknown as to how many open ports there are on the IP addresses. Running an nmap scan on the network should reveal the open ports and other exposed network services.

Web Applications

The EHR System, dental imaging system, front desk endpoints, cybersecurity technologies, and the Family Smiles Dentistry website are all public-facing applications.

These applications use many technologies. Amazon Web Service (Amazon-Linux) provides a security-focused, stable, high-performance execution environment to develop and run cloud applications. It is used by Family Smiles Dentistry as an Electronic Health Records (EHR) System. Cassandra is a database engine with fault tolerance, linear scalability, and consistency. It is capable of handling a large amount of data across multiple servers. It also handles the data in the Family Smiles Dentistry EHR System. Alpine secures the data in Family Smiles Dentistry's EHR System (source). Spark integrates the database with large-scale data processing tools. Ubuntu is an operating system that provides an interface between the user and the computer hardware.

User Accounts and Authentication

The EHR system utilizes 1 shared account (with full privileges) stored in the company's 1Password account. An Office 365 account is used to log in to front desk endpoints. It is unclear whether weak or default passwords are used at this time. With regular updates can come the resetting of passwords to defaults. There is no indication at this time that multi-factor authentication (MFA) mechanisms are implemented to secure user accounts.

Data Exposure

Sensitive Personally Identifiable Information (SPII) including medical data and credit card information are stored, processed, and transmitted by Family Smiles Densitry's systems. While the data is encrypted at rest, there is no data encryption in transit. This is crucial to reduce the risk of packet sniffing attacks. This type of attack is when the data packets that are in transit can be viewed or even altered before they get to their destination. This can lead to unauthorized personnel gaining patients' SPII. The access controls employed by Family Smiles Dentistry are also insufficient to protect their data. It is unclear whether they use the same Office365 account to log into the front desk endpoints, or if each staff member has their own accounts, but, if the former is the case, this poses an extreme security risk. This means there is minimal accountability for actions taken on a system because there is no way for the system to know who was performing the actions that occurred on the endpoint. Even if they all have their separate accounts, the fact that they don't use MFA makes the accounts susceptible to shoulder surfing techniques. Additionally, they seem to be using 1 shared account (with full privileges) stored in the company's 1password account, to gain access to their EHR System. For reasons previously stated this does not keep the data safe from attackers, particularly because it allows the user full privileges to all the data.

Cloud Services

There are cloud services used by the Family Smiles Dentistry system. They use an Amazon Web Services (AWS) EC2 cloud server to run custom Python scripts for archiving dental imaging data. They also use AWS S3 (Amazon Simple Storage Service) to back up patient images. Their Security Information and Event Management (SIEM) tool, Wazuh, also scans cloud workloads. The AWS cloud services employed by Family Smiles Dentistry use the SaaS cloud service model.

Patch Management

It appears that Family Smiles Dentistry only has a patch management system setup for the EHR System and the Dental Imaging System. This process is conducted by the front desk staff. The installation of these patches and updates occurs once a month and is done outside of business hours to avoid any disruptions to normal business operations. The monthly patch management duties are assigned to members of staff on a round-robin basis.

PROPOSED NETWORK ARCHITECTURE

Adding switches and firewalls will increase network segmentation. Network segmentation on this scale could be enhanced by installing separate switches for the terminals and the servers. Installing a firewall after the router and then between the switches will also assist in network segmentation. Installing an Intrusion Protection System in addition to the firewalls will protect the egress/ingress points.

Creating individual user accounts for access to the EHR System and to the front desk endpoints, and enabling MFA on these accounts will further increase the data's security. Also using secure network protocols to encrypt the data in transit will keep the data safe from packet sniffing.

Besides these technical defenses, utilizing physical security measures. These would include locks for server rooms and security cameras that would protect the physical assets of Family Smiles Dentistry.