Attack Surface Analysis Report

Table of Contents

Introduction:

Family Smiles is a dental clinic in New York City with clinics in SoHo, Midtown, and Park Slope. They focus on providing compassionate care that is accessable and convenient for its patients. While they have implemented some cyber security measures, they have not yet fully implemented a complete attack surface analysis. This report will provide a summary of the attack surface of the company and determine some recommendations for improving the security posture of the company.

Endpoints and Devices:

- Windows workstations
- Point of sale systems
- On-site Ubuntu server
- Digital x-ray machines
- Routers
- Switches
- Firewalls
- Wi-Fi access points

Network Layer:

- Internal IP Range: 192.168.0.0/24
- External IPs:
    - SoHo: 139.60.168.191,

    - Midtown: 139.177.192.141,
    - Park Slope: 139.48.0.109
- The EHR system might be exposed on port 443 for backing up to the cloud service via HTTPS.

Web Applications:

- Client portal for appointment scheduling and patient information.
- A patient portal for viewing medical records.
- These applications are assumed and not explicitly described in the brief.

User Accounts and Authentication:

- The EHR system uses a single shared admin account stored in the company 1password vault.
- Front desk workstations use Office 365 account for authentication.
- Using Office 365 account could lead to password reuse and weak passwords. Relies on each employee to practice good cyber hygiene.
- No multi-factor authentication is mentioned.

Data Exposure:

- EHR system stores patient medical records and patient information.
- Patient dental images are stored in S3 buckets and integrated with the EHR system.
    - This could present a security risk if the imaging devices are compromised or this connection exploited.
- The data is encrypted on rest and transmitted to the cloud via HTTPS utilizing HTTP post and get requests.
    - Another security risk is the exposure of the EHR system to the internet.

Cloud Services:

- Automated backups
- Disaster recovery plan for restoring service
- A remote server for archiving dental imaging with Python
- Security information and event Management (Wazuh)
- Endpoint detection and response (Wazuh)
- S3 bucket for backups of patient images
    - Recent images stored in hot storage while older images resided in cold storage.
- Encrypted backups of the EHR
- The cloud services are provided as a SaaS

Patch Management:

- Patching is only mentioned for the EHR system and Dental imaging system this only happens on a monthly basis. Additionally the policy of rotating responsibility could make it difficult confirm patches were properly applied.
- This has the potential to lead to a security risk within the patching period and the distributed responsibility and manual nature of their process increase the risk of human error.
- The use of a SaaS for all cloud services also introduces more shared responsibility and widens the attack surface.

Recommendations:

- When giving security recommendations, it is important to consider the relative risks and the business impact. Therefor the simplest and most cost effective methods should be explored first. The segmentation of the offices resources into smaller groups and assigning responsibilities to each group should be considered. Importantly insuring that patients only connect to a guest network and not the internal network could be a good first step. Using Ethernet over WiFi wherever possible especially for handling sensitive information could reduce attacker ability to intercept the information. Additionally, ensure that employees are trained to use proper security hygiene, strong passwords and multi-factor authentication, and are aware of the risks of Phishing attacks.