BrainStation®

Cybersecurity Bootcamp Unit 2 Project

Table of Contents

Case Study

Disclaimer

All entities and events in this case study are purely hypothetical. Details of the case study are inspired by real-world events.

Company Profile

This medical clinic is a renowned dental healthcare provider dedicated to delivering exceptional and compassionate dental services to families within the local community. Operating with a commitment to oral health and patient well-being, the clinic has established itself as a trusted name in dental care, and operates in New York City with locations in SoHo and Midtown in Manhattan, Park Slope in Brooklyn, ensuring accessibility and convenience for patients seeking dental care.

Family Smiles Dentistry Technology Architecture

1. Network Infrastructure:

- A secure and scalable network infrastructure forms the backbone of the dental practice's technology. It includes routers, switches, firewalls, and Wi-Fi access points.
- Components:
  - Enterprise-grade routers and switches
  - Internal Private IP addresses use the 192.168.0.0/24 range
  - External Public IP for the offices addresses are:
    - SoHo: 139.60.168.191
    - Midtown: 139.177.192.141
    - Park Slope: 139.48.0.109
  - Secure Wi-Fi access points with WPA2 encryption

2. Electronic Health Records (EHR) System:

- The EHR system centralizes patient records, treatment plans, and appointments in a secure digital format.
- Components:
    - EHR platform is accessed by staff on premises.
    - Integration with cloud-based billing systems
    - Hosted on Ubuntu based systems on premise
    - Regularly syncs with cloud based backup systems hosted by the SaaS vendor (based on AWS) using HTTPS
        - An HTTP POST request is used to upload data to the cloud based backup system
        - An HTTP GET request is used to download and update local data from the cloud based backup system
    - The data on this system is considered critical. The application encrypts data at rest.
- Patch and Update Management:
    - Regular patching and updates on the system are done manually once a month by front desk staff. A calendar reminder is shared with all front desk staff, and the task is assigned on a round robin basis.
    - Devices are scheduled for updates during non-operational hours to minimize disruptions.

3. Dental Imaging System:

- Advanced dental imaging technology for capturing and managing digital radiography and images.
- Components:
    - Digital X-ray sensors and imaging devices
    - PACS (Picture Archiving and Communication System) for image storage and retrieval
    - Backup of patient images to Amazon s3 bucket.
    - Integration with EHR for streamlined patient care
- Patch and Update Management:
    - Regular patching and updates on the system are done manually once a month by front desk staff. A calendar reminder is shared with all front desk staff, and the task is assigned on a round robin basis.

    - Devices are scheduled for updates during non-operational hours to minimize disruptions.

4. Front Desk Endpoints:

- Dedicated endpoints at the front desk for streamlined patient check-ins, appointments, and administrative tasks.
- Components:
    - Windows desktop computers with secure access to practice management software
    - Point-of-sale (POS) terminals for handling payments
    - Streamlined iIntegration with EHR for real-time appointment updates to the cloud

5. Cybersecurity Technologies:

- Technologies to safeguard the dental practice against cyber threats and protect patient data.
- Components:
    - Cloud based/Cloud managed SIEM and EDR capabilities with Wazuh
        - EDR installed on Front Desk Endpoints as well as EHR servers
        - Endpoint agent also performs weekly vulnerability scans after hours on monday
    - Office 365 account is used for login to front desk endpoints.
    - EHR system utilizes 1 shared account (with full privileges) stored in the company's 1password account.

6. Cloud-Based Systems:

- Cloud-based backup solutions to ensure data resilience and quick recovery in case of data loss or system failure.
- Components:
    - Regular automated backups of EHR data on SaaS cloud based platform
    - Encrypted data storage on SaaS cloud based platform
    - Disaster recovery plan for rapid system restoration
    - Amazon EC2 server to run custom python scripts for archiving dental imaging data

- Script on the server ensures that each patient has their most recent image stored in hot-storage (ie. S3 Standard) and all older images are stored in cold-storage (ie. S3 Glacier)