Surgical Dental Clinic

Daniel Messemer – Dkarlos Garcia - Kevin Botana - Jesse Rodriguez - Tavaris Hooks

About Us

This project focuses on enhancing the cybersecurity framework of a small dental clinic that employs five staff members including a dentist. The clinic provides specialized services such as tooth extractions, bone grafting, 3D imaging, anesthesia, and electronic health record (EHR) management. As a healthcare facility, the clinic must comply with the Health Insurance Portability and Accountability Act (HIPAA) to safeguard patient information.

Problem Statement

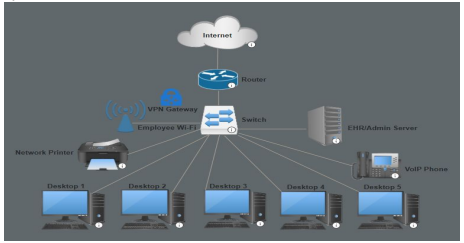
Problem: A cyberattack jeopardized private information and damaged consumer confidence in the dental clinic.

Solution: Employ cutting-edge security measures, create a solid cybersecurity plan, and conduct a comprehensive security evaluation.

Implementation:

- Evaluate the safety of the clinic's network, identifying any weak spots.
- Implement stringent security policies & solutions to ensure compliance with HIPAA and other regulations.
- Train staff to be cyber-aware and ensure ongoing security updates.

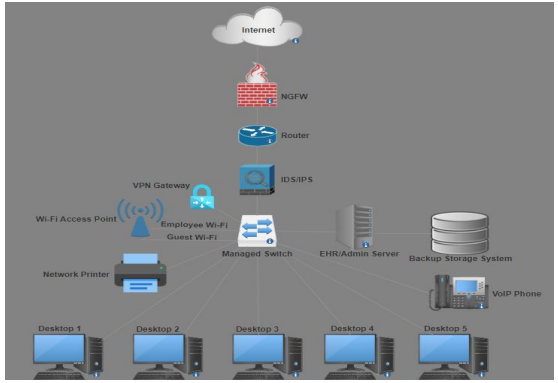
Network Topology Before Security Assessment:



Purpose

The project aims to enhance the Surgical Dental Clinic's cybersecurity posture by identifying and mitigating vulnerabilities, implementing proactive security measures, and ensuring compliance with HIPAA regulations and cybersecurity standards. This effort is intended to strengthen patient trust and protect sensitive healthcare data from potential threats.

Security Enhancements: Network Topology



Deliveries by Professional Services

Project Start	Deliveries	
Asset Identification	Access Control & Password Policies	Enhanced Endpoint Security
Threat Assessment	Enhanced Network Security	Backup & Recovery Plan
Risk Assessment	Employee Training	Policy For Updating Software
	Data Privacy Policies	Implementation of IDS/IPS

Results

- **Access Controls:** Strong role-based access controls (RBAC) were implemented to ensure only authorized personnel can access sensitive patient data and medical records.
- **Network Segmentation:** Implemented network segmentation to isolate critical medical devices and systems from general administrative networks, reducing the attack surface.
- **EDR & IDS/IPS:** Deployed Endpoint Detection and Response (EDR) alongside Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to continuously monitor for suspicious activities, detect potential threats in real-time, and enhance endpoint security by identifying, investigating, and mitigating cyber threats.
- **Identity and Authentication Management:** Multi-factor authentication (MFA) was enforced for all staff accessing sensitive clinical systems to enhance user authentication security.
- **HIPAA Compliance:** Ensured adherence to HIPAA regulations for protecting patient data and ensuring privacy in all digital communications and data storage.
- **Increased Staff Awareness of Cyber Threats**: Staff receive cybersecurity training to recognize and respond to common threats like phishing and social engineering. This improved awareness reduces human error and strengthens the clinic's security posture

Contact Information

Daniel Messemer
Daniel.Messemer001@mymdc.net
Dkarlos Garcia
dkarlos.garcia001@mymdc.net
Kevin Botana
kevin.botana001@mymdc.net
Jesse Rodriguez
jesse.rodriguez008@mymdc.net
Tavaris Hooks
tavaris.hooks001@mymdc.net