CUSTOMER SUCCESS: HEALTHCARE

With medical centers facing an increased risk of cyberattacks, a large hospital system entrusted Compucom, Cisco®, and Stratejm to dramatically bolster their cybersecurity

Overview

This hospital system is a teaching hospital and the largest health service provider for its area. In recent years, it made strategic moves to transform its health care delivery, improve patient-care efficiency, optimize and make its health information system available externally, and integrate its multiple hospitals into one system.

Challenges and Business Impacts

After a malware incident at the hospital, Compucom and the customer's IT team performed a review of their security posture. They concluded the current system lacked the capabilities to prevent the increasingly sophisticated cyberattacks facing medical facilities. The following action priorities were identified:

- Create an incident response plan with a review and tabletop exercise (a session with a facilitator where team members discuss their roles and responses to an emergency)
- Build a business continuity plan with a review and tabletop exercise
- Drive continuous Active Directory security enhancement through flaws discovery and mitigation
- Source a tool to determine weak user passwords and prevent password spraying attacks

The customer needed a third party to manage the implementation of a more sophisticated and robust solution, as there were not enough available resources on their internal IT team.

According to the customer, security threats to their IT infrastructure greatly impact the delivery of many critical healthcare services, potentially compromising the availability and accuracy of the information used for patients' medical diagnoses and treatment plans.

Solutions

Compucom took on oversight, handling compliance and governance of the contract. Our action plan included introducing a comprehensive set of tools and services to improve cybersecurity capabilities and reduce vulnerabilities in the hospital's system. We worked closely with Cisco, who supplied the infrastructure, and Stratejm, who was contracted to provide managed security services. Our customer obtained some government funding for this cybersecurity project.

First, we moved quickly to protect end users by rolling out the cloud-delivered Cisco Umbrella suite. Umbrella provided the protection and visibility necessary to assess the current threat landscape that could potentially impact users.

Second, we focused on securing the medical center's email system, a major breach vector. Cisco Secure Email was deployed to handle threats such as phishing attacks, business email compromise, and malicious content.

Third, to introduce zero-trust capability with multi-factor authentication (MFA), we implemented Cisco Duo. This seamlessly rolled out two-factor authentication (2FA) to users, shielding the hospital system from compromised credentials attacks. MFA was part of the overall plan to protect remote access, ensure device trust, and consolidate access with single sign-on.

The final piece in the solution was to complement the updated security infrastructure with robust security-operations-center (SOC) services. SOC uses people, processes, and technology to constantly monitor an organization's network — preventing, detecting, analyzing, and rapidly responding to cybersecurity incidents while continuously improving the organization's security posture. SOC teams specialize in the increasingly complicated and challenging task of staying ahead of bad actors to prevent critical attacks.

The following are some of the capabilities Stratejm's Managed Security Services provided to our customer:

- **Security information and event management:** collection and monitoring of log data
- **Threat intelligence:** monitoring chatter across dark web, and other sources, for emerging threats particular to healthcare and our customer
- **Monthly reports:** an operations report, covering the key metrics and trends coming from the SOC results, and a vulnerability report based on vulnerability scans of internal device reporting to the customer's external IP address
- **Cyber Intelligence Center:** 24/7/365 SOC service, with analysts available to assist with incident handling and response

Delivering Value

Our customer's executive director for digital services described how the planned actions helped meet the medical center's cybersecurity challenges:

- **The incident response plan with review and tabletop exercise:** "In case of any cyber incident, this plan will guide our response and documentation process for quick mitigation, recovery and preventing further occurrence"
- **The business continuity plan with review and tabletop exercise:** This plan covers the prevention and recovery from potential threats to the hospital system. It ensures the "IT infrastructure is protected and able to function quickly in the event of a disaster"
- **The tool for determining weak user passwords and preventing password spraying attacks:** This was essential to put in place, as "any compromised user attack could lead to installation of malicious software or exposure of patient information"

The executive director went on to explain how the hospital system is operating now:

- Cisco solutions are used for email filtering (Cisco Email Security gateway), web filtering (Cisco Umbrella), and online meeting and video conferencing (Cisco Webex®)
- A user awareness program has been created which includes a phishing email simulation
- Using Stratejm as their managed security service provider, the medical center now has Security Information and Event Management (SIEM) for real-time, 24/7 threat monitoring, detection, and response; the executive director added that this service provides information required for incident investigations

With the solution provided by Compucom and Cisco, and the Stratejm service to help guide our customer in the future, the hospital system will now be proactive, aware, and able to get ahead of vulnerabilities.

compucom®

cisco Partner
Gold Integrator
Master Collaboration Specialized
Master Security Specialized

Stratejm