CASE STUDY

Hospital Campus

Cybersecurity

> “Strengthening Physical Security Through Awareness Training”

Engagement Objective

The primary objective was to determine the hospital's susceptibility to unauthorized access through social engineering tactics and physical penetration.

The CIO requested an assessment of staff awareness and response to such threats, with a focus on the labor and delivery area.

Telesystem
IT's About Trust

About the Customer

A hospital engaged in a physical penetration testing exercise to evaluate the effectiveness of its security measures, particularly in sensitive areas such as labor and delivery. The Chief Information Officer (CIO) sought to assess vulnerabilities in the physical security infrastructure and the readiness of staff to identify and mitigate social engineering threats.

Penetration Testing Approach

The pen testing team conducted open-source intelligence gathering and reconnaissance to identify potential entry points and exploit vulnerabilities. During the assessment, a significant event emerged: a celebration honoring a nurse's 15 years of service, involving a breakfast gathering in the restricted area. This presented an opportune moment for a social engineering attempt.

Penetration Testing Execution

Taking advantage of the scheduled event, the pen tester arrived with six dozen Krispy Kreme Donuts and positioned themselves outside the restricted area. As nurses arrived for shift change, the tester offered the donuts, claiming they were for the celebration. Exploiting the inherent trust and hospitality of the staff, the tester was granted access without proper verification. Once inside, the tester mingled with the staff, partaking in the breakfast celebration, and even took selfies with the unsuspecting employees as evidence of the breach.

Recommendations and Implementation

The penetration testing exercise highlighted a critical gap in the hospital's security posture: while significant investments had been made in physical barriers and access controls, staff awareness and vigilance were lacking. The primary recommendation was to implement a comprehensive Security Awareness Training platform.

Key Elements of the Training Platform

1. **Continuous Micro-learning Modules:** Bite-sized, targeted training modules were developed to educate staff on various security threats, including social engineering tactics like piggybacking.
2. **Phishing Simulations:** Regular phishing simulations were conducted to familiarize staff with common email-based threats and teach them to recognize and report suspicious activity.
3. **Physical Security Tests:** Periodic physical security tests were conducted, simulating scenarios where unauthorized individuals attempted to gain access to restricted areas without proper authorization.

Outcome

By embracing a proactive approach to security awareness, the hospital witnessed immediate improvements in staff readiness to identify and respond to security threats. The combination of micro-learning, phishing simulations, and physical tests instilled a culture of security consciousness among employees, reducing the risk of unauthorized access and potential breaches.

Conclusion

The hospital's experience underscores the importance of integrating security awareness training into broader security strategies. While physical barriers and access controls are essential components of security infrastructure, they must be complemented by well-informed and vigilant staff to effectively mitigate social engineering threats and safeguard sensitive areas.