Penetration Testing Including Medical Devices

The Device Problem

Medical technology is constantly updating and working together to transmit information over your networks, allowing you to share information across many platforms and make your work life easier. Many medical devices have the ability to transmit vital health information from a patient's body to medical professionals - some of which can even be controlled remotely. If any of these devices are hooked to your networks, they could create an entryway for an attacker to access your systems, and even harm a patient in the process.

These devices present a great resource for making healthcare faster and more accurate, but it's important to ensure they don't introduce an additional threat to your organization or your patients. Any device that connects to your network can be exploited in order to obtain records and other sensitive company information. Attackers are targeting health systems left and right because of the valuable information they hold, and you want to make sure you're not a target - through medical devices or otherwise.

Secure Your Network

Every company has vulnerabilities, but for healthcare, information security is even more important because of the amount of records that are sent internally and externally every day. Just like your routers and printers, it's incredibly important to change all default passwords and configurations on medical devices that are connected to your networks.

Our Penetration Testing Including Medical Devices is an internal penetration test that focuses on what an attacker could compromise through your network, even through medical devices. This includes protected health information (PHI) and non-public personal information (NPPI). Attackers could gain access to your internal network through malware, employees, or medical devices, and our analysts will attempt to exploit vulnerabilities in your network through all of these channels and more.

This Penetration Test Will Include:

- **Determining weaknesses of internal security measures**
- **Manual testing of discovered vulnerabilities**
- **Utilizing tools and techniques used by real-world attackers**
- **Comprehensive report with actionable recommendations for remediation**

Frequently Asked Questions

What is the difference between vulnerability scanning and penetration testing?
Vulnerability Scanning is an automated method that identifies vulnerabilities that may exist on an organization's network. Penetration testing is by nature more accurate than vulnerability scanning since it actually confirms that a suspected weakness is exploitable.

Will this hurt my network?
This is extremely unlikely. We very rarely have any reported problems. We do not attempt any denial of service attacks.

How do you connect to our network remotely?
We connect through the TraceCSO Vulnerability Scanner.

What kinds of questions are asked in the scoping call?
We ask for target IP addresses and exclusions, account lockout policies so that we can mitigate the risk of locking out domain users during testing, times you want scans to run, and confirm the time we will be testing.