Case Study

In-depth external and internal penetration test reveals security gaps

Client

Top-tier regional healthcare system

Headquartered in Cincinnati, this regional healthcare system (RHS) is comprised of hospitals, physicians, and specialist offices, and serves the community through quality care and cutting edge research.

Challenge	OnX Canada solution	Results
• RHS holds massive amounts of personal information and needed to ensure it was doing everything possible to protect it. • Web-facing servers and applications security risks were unknown. • Public Internet in non-restricted areas was not separate from the corporate network. • End-user security knowledge was unknown.	• Security engineers designed a multi-phase penetration test. • OnX consultants performed reconnaissance to test the external-facing network segment. • OnX placed its own custom-built PC in an end-user network segment on the RHS's LAN to test the corporate network security. • To test publicly available network connectivity, a OnX consultant posed as a patient visiting a facility, and connected to an open network port.	• RHS revamped their security strategy, executing on the recommendations provided by OnX. • Vulnerabilities were prioritized by severity, priority, and difficulty, and each was documented. • Mitigation strategies and remediation recommendations were also developed for each vulnerability. • Additional defenses and controls were planned and implemented.

Challenge

The RHS is responsible for protecting several categories of sensitive data, including its patients' medical records, financial information, and employee personal data. In a modern threat landscape where each of these is highly sought by attackers, understanding their network's weaknesses and addressing them is a high-priority mission.

From the Internet, some servers and web applications are available, allowing any user to communicate with services, and authenticated users to access restricted features of the applications. Web applications have become common targets for attackers—as a method to reach the organization's LAN from the Internet—so the RHS needed to understand the risk exposure of external-facing systems.

The RHS also operates facilities where the public can access guest wireless Internet. Some of these facilities have open network jacks in unrestricted locations. The RHS was concerned that a local attacker may use some of this available connectivity to steal data or plant malware on internal systems.

Finally, knowing that most high-profile data breaches begin with a phishing e-mail, the RHS considered an attack from a legitimate end-user workstation a serious risk. What could an attacker do if a workstation was compromised?

OnX Canada solution

Working with the RHS's security team, OnX security consultants designed a multi-phase penetration test. The goal of the test was to simulate real attacks, using tools, methodologies, and targets that actual attackers would use, and was performed in three distinct phases.

To test the external-facing network segment, OnX consultants performed reconnaissance and identified vulnerabilities in Internet-facing servers and applications. Several were targeted for exploitation–attempts to obtain unauthorized access, collect network information and system configuration, and pivot to internal machines.

To test the internal network, OnX placed its own custom-built PC in an end-user network segment on the RHS's LAN. Consultants were able to discover and steal privileged credentials, using them to move from machine to machine, searching for data stores with medical records and financial information, and finding ways to move that data out through the RHS's Internet connection.

To test publicly available network connectivity, a OnX consultant posed as a patient visiting a facility. This allowed the tester to establish a foothold on the internal LAN from which additional simulated attacks were conducted, again locating and exfiltrating sensitive data.

After completing all testing, the findings from the assessment were compiled. OnX consultants reviewed all vulnerabilities discovered and exploited, as well as all access and sensitive data that was obtained. Vulnerabilities were prioritized by severity, priority, and difficulty, and each was documented. Mitigation strategies and remediation recommendations were also developed for each vulnerability. All of this material was gathered and placed in a findings report, which also included an executive and technical summary.

The findings were presented to the RHS's security and IT teams. Each vulnerability and recommendation was outlined by the OnX consultant team. The client used the findings to prioritize future security projects, with plans to improve some processes and procedures, as well as to deploy additional security controls and defenses in key areas of the network.

Results

The RHS has revamped its security strategy to include the recommendations from the security assessment. Additional controls and defenses were procured and are planned for deployment in the coming year. Software updates and configuration changes were applied to address some of the vulnerabilities discovered. The RHS considers their data substantially safer after addressing the findings from the penetration test.