SecureWorks

TESTING IN-STORE DEVICES FOR NETWORK CYBERSECURITY VULNERABILITIES

Concerns about store visitors using display models to compromise its networks leads to a SecureWorks engagement

Industry: Telecommunications | **Country:** United States

BUSINESS NEED

A rural wireless carrier wanted to assess the risk of the mobile devices displayed in its retail stores being used to gain access to its networks.

SOLUTION

The client signed up for a focused, real-world attempt to crack its network security from inside its stores using the mobile devices displayed for sale, with expert help from SecureWorks Security & Risk Consulting Team.

BENEFITS

- Validated the wireless cybersecurity of retail stores
- Raised awareness of a specific, potential threat vector
- Provided extra evidence of PCI compliance

PRODUCTS | SecureWorks Advanced Penetration Testing

WHEN MILLIONS OF U.S. CONSUMERS VISIT THE STORES OF THEIR LOCAL WIRELESS TELECOMMUNICATIONS PROVIDERS EACH DAY, THEY PICK UP THE VARIOUS SMARTPHONES AND TABLETS ON DISPLAY TO EVALUATE THEIR WEIGHT, FEATURES AND FINISH.

Many also try them out, calling out to their own current phones or surfing the web. Could hackers use those mobile devices to break into a wireless carrier's networks, too?

That's the question one rural wireless carrier wanted answered. For help, it called in SecureWorks Security & Risk Consulting Team, based on the sterling reputation SecureWorks had earned with its parent corporation.

Given that the wireless carrier needed to test a specific attack vector, SecureWorks recommended Advanced Penetration Testing, a service offering from the SecureWorks Security & Risk Consulting (SRC) portfolio. Advanced Penetration Testing uses an approach that's tailored to the client's requirements utilizing sophisticated techniques in its comprehensive effort to break through a company's cyberdefenses.

TRYING TO BREACH CLIENT DEFENSES

Each Advanced Penetration Test is conducted by SecureWorks technical testing team, who are among the security industry's top testers. They use proprietary tactics and global cybersecurity intelligence from the SecureWorks Counter Threat Unit (CTU) to do their jobs. For this particular test, the wireless carrier selected a representative store and required the work to be done after hours.

The SecureWorks team performed the Advanced Penetration Test by applying a range of advanced attack protocols, using state-of-the-art hacking tools to seek access to the wireless carrier's internal networks. In the store selected for the test, the SecureWorks team used a variety of mobile devices on display, both smartphones and tablets that feature iOS and Android operating systems.

The results of the testing effort showed that the wireless carrier's network cyberdefenses could protect its internal networks from an in-store attack initiated by a store visitor using a display device. This validation of its protection from this particular attack vector gave the company assurance that the risk of an in-store hack is virtually nil.

At the same time, the testing team provided it with additional evidence for auditors that its efforts to comply with the Payment Card Industry (PCI) data security standards of major credit card issuers exceed what the auditors would typically see at other companies.

OPENING DOORS TO NEW OPPORTUNITIES

This engagement added to the growing reputation of SecureWorks with the wireless carrier's corporate parent, a large multinational holding company. In fact, SecureWorks was invited twice by the parent's executive management team to take part in its quarterly business reviews and address the issue of increasingly sophisticated cybersecurity threats.

These presentations and their accompanying discussions have opened up opportunities for SecureWorks to help the parent company and its subsidiaries to ensure that their cyberdefenses are effective and up to date:

- From the SecureWorks SRC services portfolio, the executive team is interested in additional penetration testing, PCI gap analysis, web application testing and a retainer-based incident response arrangement.
- From the SecureWorks Managed Services portfolio, the executives are considering vulnerability management and supplemental security monitoring.

What's more, because the parent company partly drives growth via acquisitions, its executives have learned about SecureWorks Targeted Threat Intelligence services. These services will evaluate the overall security posture of acquisition candidates and also seek out specific vulnerabilities, so the executives will know in advance what cybersecurity risks a newly acquired company could bring with it.