Cisco Red Team Exercise

Cisco instituted a unique and comprehensive security overview of this financial institution's operations, illustrating potential weaknesses.

Snapshot

Customer Profile

- U.S.-based financial institution
- Retail and commercial banking services

Solution

- Complete Red Team exercise
- Included both physical and digital realms of institution's operations, offering it a unique and comprehensive security overview

Key Takeaways

- Successful physical penetration allowed for dropping custom malware on internal devices
- A lack of security training allowed for successfully phished data from executives and malicious files installed on their computers

Security Challenge

There were many challenges in the path of this large financial institution, including confidential information on most devices, falling under well-defined categories such as intellectual property, personally identifiable information (PII) or the requirements of the Payment Card Industry Data Security Standard (PCI DSS).

Many functions in this organization perform sensitive actions using this data and are potentially vulnerable to attacks. These attacks range anywhere from identity theft to industrial espionage, from brokering sensitive information to manipulating fiscal transactions.

Attackers have dozens of ways to capitalize on these vulnerabilities for personal gain. Weaknesses range anywhere from lacking physical defense on computing systems to vulnerable web applications whose databases can be jeopardized. Attackers have a multitude of attack surfaces to choose from and the sheer enormity of banking organizations and their overall attack surface make them the holy grail for both attackers to compromise and security experts to defend.

Cisco Solution

Cisco performed a complete Red Team exercise on a U.S.-based financial institution to assess its digital and physical assets. During the exercise Cisco was charged with performing physical security assessments of numerous facilities deemed sensitive by the bank, as well as numerous branches and personnel residences.

Physical assessment involved attempting to physically infiltrate facilities and gain access to internal devices and networks, as well as breaching wireless networks in place in these facilities or the residences of senior executives. After access was gained, Cisco attempted to deliver custom malware on employees' physical devices.

The exercise also included an assessment of overall physical security countermeasures. This included assessing guard behavior and adherence to protocol and evaluating security camera coverage, as well as approach vectors to mission-critical assets.

Outcomes

The exercise raised a number of flags regarding repetition of bad practices in the environments tested. While not all bad practices represent exploitable vulnerabilities, the continued use of poor security practices was a root cause of the wide array of results provided in the penetration testing. It was determined during the assessment that the cost for a hacker to break in was $200,000. After implementing Cisco recommendations, the cost to the attacker more than tripled, acting as a great deterrent for attackers.

The independent vulnerabilities discovered during this security assessment were cause for concern and lead to several root causes, including a lack of adherence to security policies. From the ability to defeat the human factor to the numerous significant flaws found in proprietary technology and assets, these flaws left the audited institution vulnerable to attack through any of the attack vectors mapped at the beginning of this exercise.

Cisco then provided recommendations for both immediate remediation and ongoing prevention with best practice security policies and continues to provide this support on an ongoing basis.

Learn more about Cisco Red Team Exercise or other Cisco Security Services.