Cisco Security Red Team Exercise

The Cisco Red Team exercise demonstrated the weak points of this global insurer's network, preventing potentially devastating attacks

Snapshot

Customer Profile

- European financial services company
- Fortune 500 Company
- One of the largest insurance providers in the world

Solution

- Black box external assessment
- Black box internal assessment
- White box applications penetration testing (APT) assessment

Key Takeaways

- Demonstrated potentially devastating vulnerabilities
- Infiltrated organizations network over the Internet, successfully deploying custom malware
- Obtained administrative control of Citrix management server, allowing remote control of all organization thin clients

Security Challenge

An international insurance company was primarily concerned about potential vulnerabilities in its network and the devastating consequences of a breach.

This insurance company's chief information officer (CIO) was trying to answer three primary questions when the company engaged Cisco to facilitate a Red Team exercise:

- How safe is my house?: Need to determine the overall security posture of the organization.
- How easily can someone break in?: Determine if the organization is using the right measures to protect its network.
- Is there a thief in my house?: Determine if the organization has the capabilities to detect malicious activities on its network.

Cisco Solution

Cisco performed a complete Red Team exercise on this insurer, to answer the three questions raised by the organization's CIO.

Cisco Red Team exercises are goal-oriented, rather than scope-oriented, security assessments. The scope often is the organization itself, rather than any set of handpicked assets, reflecting real-world attacks and behavior patterns.

As such, the exercise is defined by its goals. The goals and objectives of these exercises are often be defined as compromise of personally identifiable information (PII) or payment card information (PCI) as defined by the applicable client's market vertical and technical viability, such as access to a sensitive data source or ongoing activity such as eavesdropping on a channel that may allow sensitive data to leak.

Outcomes

The organization was pleased with the outcome of the exercise and the information they learned as a result. The outcome of the exercise presented few vulnerable areas on its network.

The Cisco team penetrated the company's network at multiple entry points and obtained access that potentially compromised the entire corporate IT infrastructure. Showing where these vulnerabilities are proved invaluable, given that real-world attackers can do irreparable damage.

The insurance company and Cisco have now formed a strategic partnership for the future. This partnership includes, but is not limited to, periodic Red Team exercises as part of the Cisco Security Posture Assessments Service, which includes security design assessments.

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