CASE STUDY

Red Team Reveals Security Voids

online
business systems

Online was engaged by a large, international organization that had an extensive and ongoing penetration testing program to perform a red team exercise. Our client was interested in exploring how secure their networks were using real-world tactics.Their penetration testing program was primarily aimed at protecting external and internal networks and applications, and they had never been tested using the Red Team approach.

SECURITY MATURITY

Our client had a mature security program in place and had implemented many cybersecurity measures to safeguard their networks and valuable assets. Along with routine penetration tests, the organization also had its staff participate in regular phishing training exercises and was promoting a strong security awareness program.

THE CHALLENGE

While the organization's security program was robust, they also understood that their penetration testing activities were constrained by various limitations to the dates and times each test could be conducted, and additional limitations around the scope of the tests to specific networks and applications. These constraints limited the ability of the testing to identify weaknesses that may have been present.

THE SOLUTION

Prior to performing the red team testing, several tactics were considered to ensure the testing effort addressed the appropriate challenges.

ONLINE WORKED WITH THE CLIENT TO DEVELOP A ROBUST FOUR-PHASED RED TEAM PLAN THAT INCLUDED:

- Foot Printing & Reconnaissance
- Network & Application Penetration Testing
- Social Engineering & Physical Attacks
- Reporting & Closure

ATTACKER BASED THINKING

ONLINE'S RED TEAM WAS PROVIDED WITH EXTENSIVE LATITUDE TO PERFORM TESTS OVER A YEAR-LONG PERIOD. THIS INCLUDED ATTACKS AGAINST ANY OF THE IN-SCOPE NETWORKS AND APPLICATIONS, SOCIAL ENGINEERING ATTACKS AND PHYSICAL SITE INTRUSIONS.

In order to be successful, only a small number of people within the organization were made aware of the Red Team attack strategy; with limited visibility, users were not put on the defensive.

The Red Team targeted the client's headquarters, which was a large facility employing a third-party, subcontracted, physical Security Team.

THE EXERCISE EXPOSED BOTH STRENGTHS AND WEAKNESSES IN THEIR SECURITY PROGRAM.

THE RESULTS

The organization learned that all of the network and application security controls that they had put in place, based on penetration testing activities, were very effective. However, while the users had been trained on phishing attacks, more training was required, as credential stealing attacks successfully exploited many of their employees.

In addition, the organization's IT Security Team confirmed that their implementation of multi-factor authentication helped mitigate much of the risk of the successful credential gathering phishing attacks. What the organization was less aware of was the weaknesses identified in their physical security.

The Red Team was able to bypass security and get into the facility using several different methods and found many opportunities to connect rogue devices to their network. The Online Red Teamers found office layouts and other incredibly useful information while inside the network.

Gaining after-hours access to the physical security office, the Red Teamers were able to then access and print their own security badges, giving them full access to most of the facility. The team determined that the organization did not properly limit external internet access from the internal network. Therefore, the devices placed on the network were able to communicate outbound and provide ongoing access to the organization's internal network.

Online's Red Team used this position on the internal network to gain full network compromise. Valuable real-world threats and vulnerabilities were exposed through this process.

Online's final report provided recommendations to remediate identified vulnerabilities and allowed the organization to gain valuable insight to improve their security so that they can build stronger defense strategies and reduce the number of hidden-in-plain site weaknesses.

While no networks were harmed during this planned attack, this engagement proved to be very informative to the client's internal IT Security Team, as well as the Executive Team.

NEXT STEPS

To learn more about how Online Business Systems can help your business, visit **obsglobal.com**

Results. Guaranteed.

Founded in 1986, Online Business Systems is North America's leading Digital Transformation and Cybersecurity consultancy. We help enterprise Clients by designing improved business processes enabled with secure information systems. Our unsurpassed delivery, our people, and the Online culture of loyalty, trust and commitment to mutual success set us apart.