Shorebreak Security, 8635 Holiday Springs Road, Melbourne FL 32940,
info@shorebreaksecurity.com

Social Engineering Assessment Case Study

Background
Shorebreak Security was contracted to conduct an email based social engineering assessment for a Federal government science laboratory with 3,500 employees. Employees at this laboratory are continually under attack from nation-state threat actors and receive more than the average amount of security awareness training.

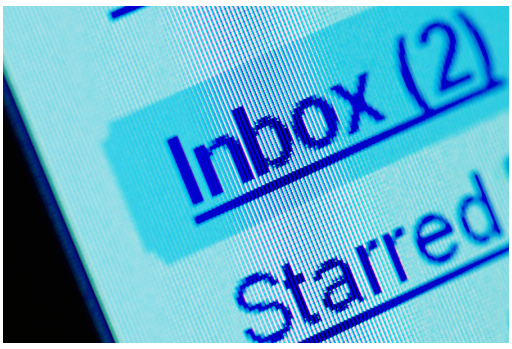
The Information Systems Security Officer (ISSO) wanted to test the effectiveness of the user awareness training and knew that there is no better test than a real-world test.

Intelligence Gathering

The first phase of the assessment was a time-consuming, but necessary step in conducting an intelligent assessment. Over a period of days, we mapped the organization's entire Internet presence and mirrored every website available – hundreds of them. As part of this task, over 2,000 email addresses were collected and presented to the ISSO for review. In many case, we were able to identify not only email addresses, but full names and positions as well. Identifying system administrators was particularly easy.

At the same time, we started to develop several potential attack scenarios based on the exposure we were seeing. A self-service password reset website was identified as being an ideal target, as it provided employees with the ability to unlock and change Windows Active Directory passwords via the Internet.

Test 1 – A "No-fail" Test



The first email phishing test was sent to approximately 400 users. It was a test that no one should have failed. It had all the warning signs of a phishing email and the customer expected to have a very low click rate. As it turned out, however, many more users "clicked" on the malicious email than we expected, and those users were targeted for more training.

Test 2 – Domain Compromise

The purpose of the second test was to take another subset of employees and conduct a more sophisticated test, with the expected outcome being higher click rate.

To prepare this test, Shorebreak registered a new domain name that appeared to be associated with the target organization, and made an exact copy of the self-service password reset website. We re-created the backend web application so it would function, but instead of changing the user's password, it would simply capture it.

We then sent emails purporting to be from IT Security, telling the users that their password had been identified as weak and to "click here" to change it. When the employee clicked the link, they were taken to our own version of their site – it looked identical and the domain name appeared legitimate.

Many users took the bait and entered their username and current password on our website, allowing us to capture their domain credentials. If an employee was successfully "phished", we immediately redirected them to a training page to instruct them on how to spot attacks such as the one they had just felled victim to.

Armed with domain credentials and a method to enter the network remotely (VPN), an attacker could have quickly gained access to the internal network.

Test 3 – Testing the "Smart People"

Up to this point, testing had not included Information Technology staff, such as system administrators, network engineers, developers, and security staff.

We would now conduct a similar test as above, but we would target the IT folks, who really should know better. After all, they should KNOW which domains the lab uses.

While the click-through rates were much lower, all it took was one user with elevated privileges to give us privileges on the internal network.

In Summary

This test provided the ISSO and lab management with actionable information they immediately use to improve the employee's security awareness, decrease their exposure to Internet threats, and implement technical controls to prevent an attack like this from happening in the future.

About Shorebreak Security

We are a veteran-owned small business providing exceptionally high-quality, high-value Information Security consulting services.

We specialize in conducting a variety of relevant, real-world Information Security tests that show you where your weaknesses are. We translate Information Technology risk into organizational risk, and empower you to make informed decisions

Contact Us:

Shorebreak Security, 8635 Holiday Springs Road, Melbourne FL 32940
info@shorebreaksecurity.com - 1-888-838-7311