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

Lifeguard Works: A Case Study on Customer “X”

Background

Shorebreak Security completed a comprehensive internal and external penetration test in August of 2013 on Customer “X”, a very successful, privately owned Information Technology company.

In February of 2014 Customer “X” signed up for Shorebreak Security’s Lifeguard service and Shorebreak Security started testing the network daily.

The following is a timeline of major events and lessons learned stemming from the first eight months of Lifeguard service.

February 2014: Incomplete Remediation

Despite having had a comprehensive test four months earlier, our engineers discovered the existence of a new, externally accessible, root-level (administrative access) vulnerability. This vulnerability was identified during manual penetration testing, and would not have been identified at all had we relied on vulnerability scanning alone. Our test team validated the vulnerability by exploitation, and gained root access to the server.

The customer was notified via text message and email right away.

Customer X’s IT staff remediated the finding and the Lifeguard dashboard automatically notified us that the system had been fixed. Verification testing, however, showed that the fix was only partially effective, and that the vulnerability was still exploitable. The customer conducted a second round of remediation, and upon verification we were able to successfully “close” the finding in Lifeguard. Despite the initially incomplete remediation, this entire cycle was still completed in less than 24 hours.

March 2014: Manual Testing uncovers “0-day”

Within just two weeks of the first critical finding, manual testing identified a previously unknown vulnerability (“zero day’) in a software vendor’s authentication system within a web application. The vulnerability could be exploited to gain root-level (administrative) access to the underlying operating system.

Customer X remediated the vulnerability with external security controls within 24 hours. We immediately conducted testing to verify the fix, and the vulnerability was successfully closed. The Shorebreak Team then drafted a security advisory and sent it to the vendor of the vulnerable software, so that a patch could be developed.

April 2014: Reaction to OpenSSL "Heartbleed"

The OpenSSL "Heartbleed" vulnerability was made public in April of 2013. Because Lifeguard scans were constantly cataloging hosts, ports, services and banners, our team was able to immediately identify vulnerable hosts. Within hours, Customer X was notified and could begin remediation efforts.

Validation testing showed that Customer X's remediation was incomplete. In this case, the vendor-supplied patches had been applied but the systems were not rebooted, leaving the systems vulnerable. Customer X was notified that the vulnerability was still present and a second round of remediation and verification testing was conducted and completed.

Customer's X's exposure to the Heartbleed vulnerability was less than 48 hours and remediation was complete before most vulnerability scanner vendors had published new signatures to check for the vulnerability.

September 2014: Reaction to the "ShellShock" vulnerability

The critical GNU Bash "shell shock" vulnerability was published in September of 2014, and we contacted Customer X to advise them on the issue and proceeded to conduct testing to identify vulnerable systems. Within 24 hours, Customer X had been reassured that their exposure to this vulnerability has been minimized.

October 2014: New Apps, New vulnerabilities

Two additional critical findings were identified as the network configuration changed and new vulnerabilities were made public.

In one case, manual testing discovered that a new web application had been deployed with a manufacturer default admin password. In another, an "SQL injection" vulnerability was identified and exploited, resulting the ability to bypass the authentication system of the web application and become a valid user.

Both vulnerabilities were reported and quickly rectified.

Observations

On average, one "critical" finding was discovered each month. Had the customer waited until their next annual penetration test to identify these vulnerabilities, criminal hackers or other adversaries could have easily compromised network.

In almost every case, manual testing was key in identifying the vulnerability.

In many cases, the customer remediation effort was insufficient in addressing the vulnerability. Without Lifeguard, the customer would have believed that the vulnerability was remediated, but in reality would have remained exposed.

Why Lifeguard Works:

1) In almost every case, critical vulnerabilities were identified and verified through **manual testing**, not by automated scanners.

2) In about 50% of the cases, the customer's **remediation efforts failed** verification testing and needed a second round of fixes before the vulnerability could be verified as completely fixed. Immediate validation "follow-up" testing by Shorebreak Security was key in ensuring that vulnerabilities were no longer exploitable.

3) In all cases, the exposure time from vulnerability identification to verification of remediation took **less than 48 hours** - in most cases less than 24 hours.

4) Network configuration and vulnerabilities are both dynamic variables that change daily and **continuously create new vulnerable conditions**. The key to minimizing risk is continuous monitoring - the ability to quickly identify, remediate and validate vulnerabilities.

5) The test team's ability to communicate with the customer before, during, and after remediation was crucial in ensuring each vulnerability was properly

remediated. Shorebreak Security became a trusted **partner in all phases of Risk mitigation.**

6) In eight months of service, Lifeguard's metrics showed Customer X's management and technical staff a quantifiable return on investment (ROI). The data show a **steady decline of Risk** across the network as vulnerabilities were fixed, and that exposure times from identification to remediation were decreased. Security and Risk exposure became a data point that could be used to identify weakness and show improvements.

7) Our customer's technical staff no longer had to spend time to run vulnerability scanners and analyze results – they could concentrate on their primary duties and rely on Shorebreak Security engineers to do this tedious, but very important work.

8) Our customer's management was indicated that they confident that they had an accurate, up-to-date risk assessment, and as risk changes, they would be notified and able to respond appropriately.

9) Risk – as measured by vulnerabilities, impact and exposure – was decreased!

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