VIGILANT

SUCCESS STORY

Client:
MID-SIZED TECH COMPANY

Solution:
PENETRATION TESTING

Vigilant Penetration Testing Reveals Findings that Prevent Malicious Actors from Stealing Data

Vigilant's Pen Testing effectively identifies weaknesses with remediation that keeps threat actors from holding data for ransom.

Investigation | Vulnerability Identification | Recommendations & Remediation

BUSINESS CHALLENGE

Like larger organizations, small to midsized companies are fending off attacks and compromise, but usually with less resources. To test their security environment, this midsized technology firm contracted Vigilant to conduct a two-week internal network penetration test. The goal was to gauge the response of their internal teams to an active threat and identify point in time findings such as end-of-life systems, outdated components, and missing patches. To simulate a real-world attack, the internal team was not made aware of the testing.

VIGILANT SOLUTION

This "assumed breach model" was chosen to enable the testers more time to focus on risks to the company. One of Vigilant's encrypted internal penetration implant devices was placed on the network to create a secure tunnel back to the Vigilant environment to ensure that all data remained safe and secure. Then the Vigilant offensive security team exploited a number of common attack vectors to conduct recon and gather information. The results: many of the client's defenses did not detect the testers and several other findings were found.

REMEDIATION OUTCOME

Since several findings were discovered, Vigilant researched and advised upgrades to specific versions of applications needed in addition to a patching program to prevent these types of attacks from being successful in the future. Vigilant also assisted with implementing mitigating controls on a critical system that was end-of-life so a multi-month upgrade could be planned and executed properly.

Why Vigilant Penetration Testing?

Unlike most competitors, Vigilant's knowledgeable experts understand that simply stating "upgrade to fix this issue" is not a remediation plan. At times, mitigating controls need to be put in place that allow business continuity to remain during a period of testing/tooling for a proper upgrade. We live in a world where the risk of attack is not an "if" but rather a "when." Vigilant truly cares about protecting your information. Our process is unmatched, and our prioritized recommended courses of action are specifically designed to reduce your attack surface quickly.

*Note: for security reasons, Vigilant never reveals the identity of our clients.

www.vigilantnow.com | 855-238-4445 | sales@vigilantnow.com