HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

ALERT

Issued 7/12/18

Pentesters Probe Two Dozen .orgs and ALL Failed

Positive Technologies, a security company, conducted 22 infiltration attempts between April and December 2017 for corporate customers and various industries who had hired Positive to test out their security systems. What the researchers found, unfortunately, was that getting in to every single one of these companies was all too easy. Despite being the most-publicized malware infection in years, a vulnerability to the WannaCry nasty was found in nearly a third (31%) of the companies. Additionally, 60% of the machines tested were found to have not patched MS17-010, a remote code execution bug that had been addressed in March 2017, months before the tests were performed. That single bug caused the vulnerability rate from the tests to double from the previous year. In one case, pentesters found a public-facing system that was vulnerable to CVE-1999-0532, a bug that is now more than 18 years old. Network security was not much better. Pentesters were able to get into the internal LAN of targets 68% of the time, and that 75% of companies allowed wi-fi networks to access the company intranet. 40% of companies had a dictionary password (vulnerable to brute-forcing) on their wireless network. None of the companies tested were able to stop an insider attack: every single one of them allowed an internal account to take full control over the infrastructure. On top of that, 26% of employees sent phishing emails in the tests followed the dodgy links and half of those people were convinced to submit data into a fake authentication page. There's also a mid-year report from ZDI based on its own bug-hunting numbers. That report found a 33% increase in bug reports while SCADA bugs (30% of all advisories), Microsoft browser flaws, and virtual machine bugs all surged in popularity.