PROVIDENCE BUSINESS NEWS
PBN
pbn.com
YOUR SOURCE FOR BUSINESS NEWS IN SOUTHERN NEW ENGLAND | MAY 12, 2023

GUEST COLUMN | PETER NELSON

Test your defenses

EVERY ORGANIZATION using information technology has some form of support, everything from a managed service provider down to "someone from accounting." This approach not only keeps things running day to day, it also reasonably assumes that security is managed for the network, the users and the data.

While many tools are available to quickly secure the major entry points into a network, there is a tendency to adopt a simple "set it and forget it" approach. Due to the dynamic nature of modern-day network environments and threats, this approach no longer works.

That's why regular vulnerability assessments and penetration testing safely check defenses and identify potential entry points into a network and data; basically, it's like a real-world hacker trying to get deep inside the network, collecting information and reporting the findings back to the staff.

Vulnerability assessments and penetration testing are two separate processes working in tandem to identify and test both known vulnerabilities and safely exploit lesser-known ones. The vulnerability assessment scans the network against a list of publicly documented security vulnerabilities and reports findings. Typically, this assessment scan finds the major security gaps.

Next, the penetration test is where the security team actively attempts to exploit all documented and undocumented vulnerabilities from both outside and inside the network.

The scans produce valuable reports for staff or outsourced IT teams with both the documented liabilities and specific remediation recommendations. Running these scans does not make a network safer; it's closing the security gaps that provides the real value.

Cyber insurance carriers are also interested in the reports because performing regular (at least annually) tests and assessments expose the carriers to less risk. We even speculate that this process helps reduce the cost of coverage. We expect to see cyber insurance carriers mandating regular testing as a prerequisite for renewing or obtaining a cybersecurity policy.

While these tests have been used by large, enterprise-level organizations for years and deliver a clear return on investment, the price tag has become more affordable for small and midsize organizations. And just in time: as larger firms have tightened up their defenses, attacks on smaller businesses have increased dramatically. According to a January 2023 report by Fundera, there was a 424% increase in new cyber breaches at small and midsize businesses last year.

What's more, the costs of a breach, even for a 15-person company, can be fatal to an organization. There's a disruption in the company's mission, resulting lost sales and customer confidence, increased IT costs to recover data and prevent future hacks, and potential fines and fees from regulatory or state agencies.

We expect to see **cyber insurance carriers mandating** regular testing.

For example, a 30-person Rhode Island firm recently suffered a loss after a ransomware attack that included a $35,000 payment to the hackers followed by a $230,000 fine paid to the commonwealth of Massachusetts for divulging personal identifiable information of several Massachusetts residents. Then there's the reputation hit and the cost associated with being without critical data for several weeks.

If a company is addressing all the best practices – business continuity planning, user training, cybersecurity, vendor management, proactive 24/7 monitoring – with a managed service provider or in-house staff, that business is on the right track. But with the addition of vulnerability assessments and penetration testing, the company has a sophisticated and sound security strategy. It's likely only a matter of time before insurance carriers or government agencies require such tests be conducted. ■

Peter Nelson has been the vice president of engineering for NetCenergy LLC, an outsourced information technology provider based in Cranston, since its founding in 2003.