Constant threat

New cyberthreats make network testing more important than ever

INTERVIEWED BY ADAM BURROUGHS

GREGORY J. SKODA, JR., CISA
Principal
Skoda Minotti

(440) 605-7176
gskodajr@skodaminotti.com

WEBSITE: For more information about protecting your company's network, visit www.skodaminotti.com/risk.

Insights Accounting & Consulting is brought to you by **Skoda Minotti**

There are many threats that can compromise a company's computer network. Many businesses, however, don't fully understand what can happen when networks aren't configured properly, or are outdated.

"Prudent business owners invest in services to provide better assurance to their customers that they're taking steps to protect stakeholder data," says Gregory J. Skoda, Jr., CISA, principal at Skoda Minotti. "Without certain preventative and detective systems in place, someone can easily gain access to your network. It will only get more important to take steps to protect your business as attacks become more prevalent."

Smart Business spoke with Skoda about protecting company computer networks.

What tests can be conducted to measure the strength of a network's security?

There are two common tests: a vulnerability assessment and a penetration test.

Vulnerability assessments use software to scan computer networks to identify system issues. Examples of this could be old systems, unpatched software, default manufacturer credentials or passwords that could allow an outsider easy access to a network.

A penetration test is a controlled attempt to exploit the weaknesses found in the vulnerability assessment. These tests could be attempts to crack passwords and use default login credentials to compromise a network. This can help discover how severe a vulnerability issue could be. There are also times when a vulnerability assessment shows there are potential problems, but the penetration test shows it's actually a false positive.

How often should tests be conducted?

Depending on the type of organization and nature of the business, vulnerability tests could be conducted multiple times per day. Businesses that host websites are running assessments constantly, but most businesses would be fine running quarterly checks. Penetration tests are usually done annually.

It's advisable for companies that have made technology infrastructure or network changes to perform these scans during, or immediately after, such an event to ensure there are no holes in the security protocols.

Why should companies conduct these tests?

One of the important reasons to conduct these tests is to identify what systems are connected to a network. With wireless capability and myriad device connections that can be tied to a company's network, it's important to know who or what is requesting access to your systems.

Companies lose an element of control when mobile devices or laptops connect to their network, and that could lead to a catastrophe. Testing ensures all systems are up to date and reaffirms that security measures are actually in place and functioning. They can also validate that the procedures your internal IT department or external IT consultant has performed are working. Companies may also need to show that their security measures are in compliance with applicable regulatory standards and customer requirements.

Conducting regular network assessments can provide assurance to customers or other stakeholders that your systems are secure. That sentiment can mean more if those tests are conducted by an independent third party. It can help put customers at ease if they know that proper steps are being taken to protect their information.

What should companies look for in a provider?

Hire a provider with the right experience, skills and tools to properly perform the testing. Look for an independent, third-party IT auditing expert that will work in partnership with your team.

You will also want to find a provider that is a Certified Information Systems Auditor, Global Information Assurance Certification Certified Penetration Tester, Certified Information Systems Security Professional or is comparably certified, and ask which tools and methodologies are being used. Review the provider's references and case studies.

New exploits and hacks appear daily that can be used to gain access to a company's network. It's important to regularly inspect the strength of your systems to ensure your network is secure against new threats. ●