WESTERN NEW YORK
THE DAILY RECORD
YOUR TRUSTED SOURCE FOR LEGAL AND REAL ESTATE NEWS
NYDAILYRECORD.COM
NOVEMBER 29, 2021

Commentary: Six steps toward building a stronger security profile in 2022

By SCOTT ROTHSCHILD
Daily Record Columnist

These days, there's a lot of emphasis on the implications of data breaches, ransomware attacks, and other system compromises from bad actors on the world stage. We read about the "parade of horribles," which can ensue after an event, and it would be easy to lay down and acquiesce to the eventuality that "our company will be hit at some point." But we shouldn't because there are several steps you can take to help protect your business. The objective of this article is to explore some of the ways in which we can mitigate risk and enable "early detection" on any gaps or areas of opportunity within the IT Infrastructure. Here are a few suggestions from me and the team at Avalon Cyber:

Step 1 – Set Up Multifactor Authentication and a Password Manager TODAY!

"If you're not using multifactor authentication (MFA) on your accounts today," says Kyle Cavalieri, president of Avalon Cyber, "stop what you're doing, and set it up now!" He explains that using a username and password to access personal or professional accounts is simply not enough. Adversaries are harvesting credentials all the time and the password you're using to access multiple sites has probably already been collected. But is remembering passwords a huge pain too? Then we recommend getting a password manager, like LastPass, installed on your computer and your smartphone. Once you have that set up, you don't have to remember different passwords because they will all be stored within this secure database. Don't feel like making up your own passwords? Most password managers allow you to generate a completely random and secure password to be used on the site you are trying to authenticate into. The best part is that when you go to try to access the site again in the future, the password manager recognizes the site and can even allow you to auto-populate the username and password to log in with. Not only should this make the user experience more streamlined, it's also a heck of a lot more secure!

Step 2 – Vulnerability Assessments

Engaging a professional cybersecurity services organization to conduct internal and/or external vulnerability scans will help you identify risks in your company's environment. This would be an independent review, working in conjunction with your IT team or managed services provider, to create a plan that addresses weaknesses in your network. When you engage an outfit to perform this service, you should expect to receive a comprehensive scan of all network assets, as well as a detailed report of critical findings and suggested remediation steps. Your cyber partner will also provide an executive debriefing of their findings after the assessment.

Step 3 – Penetration Testing

During a penetration test, cybersecurity professionals attempt to exploit critical systems to access your sensitive data. By safely simulating the activity of a cybercriminal targeting your network, you'll find out if your currently deployed security resources are valid and whether your employees are following your security policies. An industry-standard penetration testing service targets anything with a live IP address, including servers, desktops, laptops, firewalls, web servers, and web applications, and is followed up with a detailed report. At the conclusion, just as after a vulnerability assessment, a final presentation/executive debriefing of findings, including a Q&A session, should happen.

Step 4 – Managed Detection and Response

Antivirus solutions and securing just the perimeter of your network are no longer enough to protect your IT environment. You need to monitor your endpoints at all times and be aware of any lateral network activity taking place. That's why you should seek out a professional cyber services provider who can deliver managed detection and response (MDR): a 24/7/365 service which uses lightweight agents (software that identifies bad behavior) to detect and respond to threats inside and outside your network. This endpoint monitoring solution screens malicious behavior at the endpoint level, which then allows your provider to alert you to potential threats, and finally, shut down those threats ASAP.

Step 5 – Incident Response (IR)

In these wild times, many companies find it prudent to have a trusted cybersecurity team on retainer to ensure an instant response should they need to activate them in the case of an event. If you ever experience a breach, your vendor should be able to provide actionable threat intelligence and threat hunting services to find and fill gaps in your network. Next, they will determine whether any of your data was affected. A professional cyber team will have extensive experience in digital forensics and know where to find critical electronic evidence, and concurrently, preserve and analyze it. Some cybersecurity companies also offer data breach review and data breach notification services to assist you with alerting your clients about the breach, if required by state and national regulations.

Step 6 – Implement a Security Awareness Program

Did you know that 90 percent of cyberattacks come through phishing emails? All you need is one employee to click a malicious link and you could have a cyberbreach. That's why so many cyber companies offer programs that allow your IT team to launch simulated phishing attacks. By running comprehensive security awareness training campaigns, you help educate your employees and stakeholders and reduce the possibility of a phishing-related cyber incident.

Although we've all heard the saying that goes, "It's not if, it's when" an information security breach will happen, there are plenty of ways for us to mitigate and minimize the risks involved. The "pay now or pay later" eventuality can work in a company's favor if they implement the right planning, policies, and partnerships. A lot of diseases which used to be untreatable can now be remediated with a proactive approach. The same can be said for the inherent threats we're seeing in the daily cyberattack headlines. A little bit of planning and strategy can make a lot of difference for your organization in the end. Here's to much success and a strong defense in 2022!

Scott Rothschild is an Account Executive at Avalon Legal who has been consulting with law firms and corporations on document management, workflow and eDiscovery since 2003.