Success Story

Large North American Retail Chain Relies on Rapid7 Nexpose® and Metasploit® to Achieve Compliance, Minimize Risk, and Mitigate Threats

How does a multi-billion dollar retailer do security? According to the company's Information Security Manager, Steve, it starts with compliance – but by no means does it end there.

Steve brings more than a decade of network security experience to the job, where he is tasked with protecting hundreds of sites and store locations, as well as complying with SOX, PCI and HIPAA regulations.

Compliance Doesn't Equal Security

The retailer in question uses Rapid7 Nexpose and Rapid7 Metasploit Pro to secure their environment. Like many organizations in this industry, compliance is the primary driver for having a strong vulnerability management program in place: new PCI DSS requirements for penetration testing were what spurred their initial Rapid7 purchase. Up until that point, the security team had reviewed machines manually to see what patches were missing and what other vulnerabilities needed to be remediated. "We got to a point where doing it manually was out of the question, given the time frame," Steve recalls. "Even a team triple our size couldn't have gotten it done."

> "It's a seamless integration [between Nexpose and Metasploit,] which saves me countless hours and allows me to focus on my highest risks."

That's not to say that Steve considers the organization secure as long as they're compliant – history has shown that compliant companies can still fall victim to cyberattacks. "Compliance is certainly a key driver for our vulnerability management program, but just because I can pass a test doesn't mean I'm secure. We need to take things a step further in order to truly secure the network."

Both Nexpose and Metasploit can help complete the PCI-required vulnerability scans and penetration tests, but it was the combination of both Nexpose and Metasploit together that caught Steve's eye. The two products, working in tandem, provide the capabilities he and his team need to go beyond baseline compliance assessments and get actionable security information – discovering assets and threats, assessing the organization's security posture, and helping patch or implement mitigating controls. "You get more bang for your buck with both of them" Steve concurs, "It's what ultimately made me decide to go with Rapid7."

“Now remediation is completed in a matter of weeks, versus 2-3 months.”

A “Smarter” Product

Since being deployed, Steve says that Nexpose and Metasploit have more than proven their value. The deep integration between the two solutions gives a simpler workflow and more effective risk prioritization, enabling him to spend more time addressing real threats. “The saving grace is that you can have Nexpose vulnerabilities automatically imported into Metasploit to validate exploitability. It’s a seamless integration which saves me countless hours and allows me to focus on my highest risks.”

Despite the fact that retailers are strongly dedicated to protecting customer information and thwarting cyberthreats, the industry has nevertheless spawned some of the most high-profile data breaches in recent years. But Steve doesn’t let himself worry about what would happen if his organization makes headlines for all the wrong reasons. Instead, he capitalizes on the fact that there is now more awareness of retail security issues. “It gives you a leg up when you’re talking to your management team,” he says.

He gives an example: “When Nexpose checks to see if there are vulnerabilities in an OS, it doesn’t just look at known exploits for that operating system.” In this he’s referring to the fact that Nexpose uses an expert system to achieve better results in vulnerability scanning to find assets and vulnerabilities that other solutions often cannot. “Nexpose goes far beyond what you get with other vulnerability management tools,” Steve says. “For example, if it’s running SSH, it will check what version and also tell me whether it can easily be accessed with specific passwords or usernames.”

From Months to Days

In addition to helping with Steve’s peace of mind, Rapid7 has also been a time saver. “Just to maintain the security of all our retail transaction servers and to get everything patched would have taken 2 to 3 months with our old, manual approach,” he says. “Not only do you have to update operating systems, you also have to patch applications and make sure the surrounding environment isn’t vulnerable – not to mention making sure that administrators haven’t dropped anything new onto the machine. It’s a very complicated change control process involving a whole series of checks.

“Now, after Nexpose scans, a remediation report is automatically created for the administrator of the machine. And now remediation is completed in a matter of weeks, versus 2-3 months.”

Support – Whenever You Need It

Anytime Steve has a question, he has multiple avenues for getting a response. “The community surrounding Rapid7 is great,” he says. “There are always answers to questions, you can go to as many tutorials/webinars as you like – that’s information you’re just not going to get at the water cooler. I like digging into the details of what others have done – so many members of the community have taken exceptional amounts of time to provide step-by-step details of a particular project or experience. That’s incredibly helpful.”

Apart from the Rapid7 Community site, Steve also has the option to contact Rapid7 support: “Support is quite knowledgeable and extremely responsive. They’re professional, prompt – what more can I say?”