Rapid7 Metasploit Changes the Security Mindset at AutomationDirect

AutomationDirect.com is a leading supplier of industrial automation equipment and associated components to manufacturers around the world. Based in Cumming, Georgia, AutomationDirect goes beyond low pricing to earn customer loyalty, delivering award-winning customer support, objective product evaluations, and partnerships with reliable systems integrators.

AutomationDirect itself uses sophisticated automation solutions to pack and ship its orders for greatest accuracy and efficiency, but it also treats its people "like billion-dollar assets," says Tim Hohmann, founder and company captain. And because AutomationDirect does most of its business online, it must comply with Payment Card Industry Data Security Standard (PCI DSS).

Client
AutomationDirect

Industry
Automation Equipment Supplier

Website
www.automationdirect.com

Challenge: Raising Threat Awareness

"We're a proactive company. We don't like to be reactive," says Tim Lawrence, IT security analyst at AutomationDirect. After an enlightening, perhaps frightening, visit to the Black Hat convention in July 2010, Lawrence devised a sensible, long-term security strategy to stay ahead of the latest threats, both internal and inadvertent, and external and deliberate.

Being a proactive organization.Lawrence wanted to change the security mindset of the AutomationDirect IT staff. "Administrators are notorious for just getting something up and running," he says, "They don't think security. They just think, 'I'm going to get this up, get the customer happy, and move on to my next target.' The strategy works great for making the customer happy but doesn't go too far in securing an environment. AutomationDirect refers to this situation as the forgotten server in a closet with the mop bucket on top of it and we're trying to make sure that we don't leave any lying around."

Lawrence already used some freeware tools, including the freeware version of Metasploit Framework, but he wanted commercial-grade vulnerability and penetration testing solutions to anticipate and thwart would-be hackers and to eliminate internal oversights that create inadvertent vulnerabilities.

Case Study Highlights

Challenge

While AutomationDirect was not under any immediate known security threat, IT security needed to espouse the cause of overall security best practices to the entire IT staff to head off any possible worst-case scenario.

Solution

AutomationDirect chose to implement Nexpose Enterprise Edition for vulnerability scanning and Metasploit Pro for penetration testing. Together, they comprise a complete solution for risk assessment and remediation across the data center, networks, and Web servers.

Solution: Rapid7 Metasploit Pro

AutomationDirect chose to implement a complete Rapid7 solution that includes Nexpose Enterprise Edition for vulnerability scanning and Metasploit Pro for penetration testing. Together, they comprise a complete solution for risk assessment and remediation across the data center, networks, and Web servers.

> *"Metasploit has become my de facto tool that I use for everything. I use it every day."*
>
> **Tim Lawrence**
> IT Security Analyst
> AutomationDirect.com

Metasploit Pro has the world's largest public database of quality-assured exploits that Lawrence uses to emulate realistic network attacks on specific targets in the AutomationDirect environment. It assesses the security of Web applications, network and endpoint systems, and email users. It has an easy-to-use interface that allows him to automate tasks and leverage multi-level attacks, so he can complete penetration test assignments faster than he could with the freeware version. It includes support for Web application exploits, managing client-side campaigns against end users, VPN pivoting, and team collaboration.

"Metasploit has become my de facto tool that I use for everything," says Lawrence. But he knows that the nature of Metasploit is to penetrate targets, so he is careful when defining the scope of his exploits. "There's always a chance that you may bring a target down. I've had other products crash a machine, but I've not had an issue with Metasploit." Lawrence also uses Nexpose and Metasploit Pro in tandem, taking advantage of data-sharing capabilities between the two products.

After using Metasploit to break into a Web server, Lawrence runs the Nexpose vulnerability scanner through the compromised server. He uses VPN pivoting to discover an exploitable vulnerability in a database that hosts confidential customer data and employee information. He can leverage this information to conduct social engineering in the form of a targeted phishing campaign to open new attack vectors on the internal network. "People are always going to be your weakest link. It is common nature for people to click on things."

Like Nexpose, Metasploit Pro generates customizable executive and audit reports. Says Lawrence, "The exploitation modules that are in Metasploit Pro are great. It saves me from having to document so much by hand and saves me a lot of man-hours."

Results: Changing the Mindset

Lawrence says the Metasploit reports have changed the mindset of the server administrators he works with. "As soon as I drop a piece of paper on them that shows how I've gotten into a machine, and that from there I was able to get on other machines, it totally changes their posture on what needs to be done," he says. Now server administrators ask for risk assessments and remediation recommendations before putting new servers online.

Although Lawrence reports no major issues with the product, he appreciates how quickly the Rapid7 support team handled some minor key management issues. "I love the product," he says. "It was very easy to get up and running. Every enhancement that Rapid7 comes out with gets used immediately. It's a sound product. It works. I wish I could say that about some of the other products I use."

The Rapid7 Professional Services team also provides AutomationDirect with quarterly PCI Compliance Testing. An auditor who drove six hours to visit AutomationDirect stayed only an hour, satisfied that Lawrence's team is following compliance protocols.

"It's hard to put a value on security," says Lawrence. "One compromise will cost you way more than this product. If you can secure one target from being compromised, it's going to pay for itself once. The value of what you get for the money is exponential."