

“With Nexpose, I can lock down exactly what’s being scanned so that entry-level staff can use it safely, thus allowing senior staff to concentrate on high level security activities.”

Brian Kollmansberger
Lead Security Analyst

Rapid7 Nexpose Supports Compliance at a large regulated utility

As a regulated public utility company that provides electric and natural gas services to more than 1.4 million customers throughout the North-Central United States, the organization’s 8500 employees are committed to safety and integrity throughout their operations and business practices. In addition to corporate business applications such as email, the production IT environment uses a Supervisory Control and Data Acquisition (SCADA) system that gathers data from sensors\control relays placed throughout the generation and transmission infrastructure into central data centers that manage and control operations.

Challenge: Regulatory compliance in a sensitive environment

As a large regulated utility company, this organization participates in and adheres to the North American Electric Reliability Corporation (NERC)’s Cyber Information Protection (CIP) standards certified by the Federal Energy Regulatory Commission. The NERC CIP develops and enforces reliability standards; assesses adequacy; monitors the bulk power system; and educates, trains and certifies industry personnel. The NERC CIP reliability standards define the reliability requirements for planning and operating the North American bulk power system. They must also comply with a variety of environmental and financial regulations.

As part of its regulatory compliance efforts, the organization needed a vulnerability assessment tool to identify and remediate potential security issues throughout its SCADA environment and corporate applications.

“We wanted to do this proactively and regulatory requirements helped us to build a business case for it,” says Brian Kollmansberger, lead security analyst.

Finding the right tool to suit our needs was a long process, says Kollmansberger. “Very few companies have solutions that work in a SCADA environment. It has unique protocol stacks that are sensitive.”

Open-source applications lacked the flexibility and required considerable resources for development and ongoing maintenance. The organization needed to avoid crashes within the SCADA system and another tool that they had purchased proved unsatisfactory because it relied upon an offsite management system that did not provide detailed scan logs.

Solution: Rapid7 Nexpose Enterprise Edition

After an 18-month exhaustive multi-product review period, Kollmansberger and his team now use Rapid7 Nexpose Enterprise Edition to perform vulnerability assessments of all their corporate applications and SCADA environment. Nexpose Enterprise is Rapid7's flagship vulnerability assessment and remediation software solution. It can be configured to automatically scan for more than 14,000 vulnerabilities and perform more than 54,500 checks across Web applications, databases, networks, server operating systems, and other software products. It locates and identifies threats, assesses and ranks their risk to the environment, and offers step-by-step remediation plans. It has a range of templates to track vulnerabilities specific to various compliance standards and regulations. It supports remote scanning and offers an API for integration with other IT management systems.

Nexpose generates reports that provide constituents with extensive information about their security postures, using SANS guidelines to rank vulnerabilities by criticality and suggest step-by-step remediation plans.

"We have spent considerable resources and time trying to deploy Open-Source and purchased products with limited success," says Kollmansberger. "Comparatively the deployment of Nexpose was very easy and very flexible, especially with the SCADA scan template. Unlike other systems that do different types of OS fingerprinting or application fingerprinting, with Nexpose I have the control to minimize that. In general the SCADA scan template caused no issues whatsoever."

Kollmansberger likes the visibility that Nexpose offers, particularly the highly granular ability to configure scans. The detailed logs enable him to determine what type of scan may cause a SCADA device to crash and tune the scan to exclude specific protocols or services on individual devices. "I can do full vulnerability scans that I couldn't do with other products," he says.

To support compliance requirements, he worked with Rapid7 Professional Services to build custom scanning templates and format reports that sort information by IP address, rather than by port or service. Nexpose also enables Kollmansberger to generate reports targeted for the interests of each constituent. For example, the internal auditing and compliance teams need information presented differently than the network, Web server, and corporate application administrators, who need different information than the SCADA administrators.

Results: Secure and Compliant

Comparing Nexpose to the other vulnerability assessment tools that his organization has used, Kollmansberger says, "I've had extremely good reviews from everyone that has used it." The remediation steps help server administrators and networking



teams within the Web environment to quickly resolve critical issues and perform patches and updates.

Nexpose reduces the time required to harden new devices before they come online. The security team also uses Nexpose to perform ad-hoc scans after any changes to the SCADA environment, supporting compliance requirements.

Next Steps

Now that Kollmansberger has fine-tuned Nexpose scan templates, he is confident that scans will not cause system crashes, especially within the sensitive SCADA environment. Because Nexpose is easy to use, the organization is able to reduce the workload of senior staff by delegating to each business unit or other security personal the responsibility for scheduling and running scans according to individual needs, with Kollmansberger's team assessing the results.

"I'm very pleased with the product," he says. "With Nexpose, I can lock down exactly what's being scanned so that entry-level staff or business units can use it safely, thus allowing senior staff to concentrate on high level security activities."

About Rapid7

Rapid7 is the leading provider of unified vulnerability management and penetration testing solutions, delivering actionable intelligence about an organization's entire IT environment. Rapid7 offers the only integrated threat management solution that enables organizations to implement and maintain best practices and optimize their network security, Web application security and database security strategies.

Recognized as the fastest growing vulnerability management company in the U.S. by Inc. Magazine, Rapid7 helps leading organizations such as Liz Claiborne, the United States Postal Service, Carnegie Mellon University and Red Bull to mitigate risk and maintain compliance for regulations such as PCI, HIPAA, FISMA, SOX and NERC. Rapid7 also manages the Metasploit Project, the leading open-source penetration testing platform with the world's largest database of public, tested exploits. To obtain a free download of Nexpose or Metasploit, please visit <http://www.rapid7.com/resources/free-downloads.jsp>.

For more information, visit www.rapid7.com.