IT Asset Management

Executive Summary

- The National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of Standards and Technology (NIST), developed an example solution that financial services companies can use for a more secure and efficient way of monitoring and managing their many IT hardware and software assets.

- The security characteristics in our IT asset management platform are derived from the best practices of standards organizations, including the Payment Card Industry Data Security Standard (PCI DSS).

- The NCCoE's approach uses open source and commercially available products that can be included alongside current products in your existing infrastructure. It provides a centralized, comprehensive view of networked hardware and software across an enterprise, reducing vulnerabilities and response time to security alerts, and increasing resilience.

- The example solution is packaged as a "How To" guide that demonstrates implementation of standards-based cybersecurity technologies in the real world. The guide helps organizations gain efficiencies in asset management, while saving them research and proof of concept costs.

THE CHALLENGE

Large financial services organizations employ tens or hundreds of thousands of individuals. At this scale, the technology base required to ensure smooth business operations (including computers, mobile devices, operating systems, applications, data, and network resources) is massive. To effectively manage, use, and secure each of those assets, you need to know their locations and functions. While physical assets can be labeled with bar codes and tracked in a database, this approach does not answer questions such as "What operating systems are our laptops running?" and "Which devices are vulnerable to the latest threat?"

Computer security professionals in the financial services sector told us they are challenged by the vast diversity of hardware and software they attempt to track, and by a lack of centralized control: A large financial services organization can include subsidiaries, branches, third-party partners, contractors, as well as temporary workers and guests. This complexity makes it difficult to assess vulnerabilities or to respond quickly to threats, and accurately assess risk in the first place (by pinpointing the most valuable assets).

THE SOLUTION

The NIST Cybersecurity *IT Asset Management Practice Guide* is a proof-of-concept solution demonstrating commercially available technologies that can be implemented to track the location and configuration of networked devices and software across an enterprise. Our example solution spans traditional physical asset tracking, IT asset information, physical security, and vulnerability and compliance information. Users can now query one system and gain insight into their entire IT asset portfolio.

The guide:

- maps security characteristics to guidance and best practices from NIST and other standards organizations including the PCI DSS

- provides

  - a detailed example solution with capabilities that address security controls

  - instructions for implementers and security engineers, including examples of all the necessary components for installation, configuration, and integration

- is modular and uses products that are readily available and interoperable with your existing IT infrastructure and investments

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee regulatory compliance. Your organization's information security experts should identify the standards-based products that will best integrate with your existing tools and IT infrastructure. Your company can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

Our example solution has the following benefits:

- enables faster responses to security alerts by revealing the location, configuration, and owner of a device

- increases cybersecurity resilience: you can focus attention on the most valuable assets

- provides detailed system information to auditors

- determines how many software licenses are actually used in relation to how many have been paid for

- reduces help desk response times: staff will know what is installed and the latest pertinent errors and alerts

- reduces the attack surface of each device by ensuring that software is correctly patched

SHARE YOUR FEEDBACK

You can get a copy of the guide at http://nccoe.nist.gov and help us improve it by submitting your feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

- email financial_nccoe@nist.gov

- participate in our forums at https://nccoe.nist.gov/forums/financial-services

To learn more, you can contact us at financial_nccoe@nist.gov to arrange a demonstration of this reference solution.

TECHNOLOGY PARTNERS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution.

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based example solutions using commercially available technologies. As the U.S. national lab for cybersecurity, the NCCoE seeks problems that are applicable to whole sectors, or across sectors. The center's work results in publicly available NIST Cybersecurity Practice Guides that provide modular, open, end-to-end reference designs.

LEARN MORE

Visit http://nccoe.nist.gov

ARRANGE A DEMONSTRATION

nccoe@nist.gov

240-314-6800