CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Reducing Security Costs with Standard Configurations: U.S. Government Initiatives

Key Message: Information security costs can be significantly reduced by enforcing standard configurations for widely deployed systems.

Executive Summary

Based on the success of a U.S. Air Force initiative to use standard configurations for all Microsoft Windows XP and Vista systems, the U.S. Office of Management and Budget has mandated that all federal agencies move in this direction. The intent is to reduce vulnerabilities when installing a new system and to streamline the patching process during system operation and maintenance. All organizations and business leaders can benefit from this experience when managing their own IT infrastructures.

In this podcast, Clint Kreitner, president and CEO of The Center for Internet Security, describes these initiatives and the role of his organization in defining the standard configurations that have served as the basis. The configuration definitions are publicly available to all organizations.

PART 1: INITIATIVE BACKGROUND AND HISTORY

U.S. Office of Management and Budget Policy Mandate

By February 2008, all federal agencies will be required to use standard security configurations for all Microsoft Windows XP and Vista systems.

Moreover, as of June 2007, all acquired applications that run on government systems need to certify they are fully functional when running on a system with these standard configurations.

How did this come about?

- Vulnerability reduction is one of the key principles in the U.S. National Strategy to Secure Cyberspace
- Based on studies conducted by the National Security Agency (NSA) and MITRE, systems configured using the CIS benchmarks eliminated upward of 90% of the vulnerabilities that existed in Windows systems as configured out-of-the-box by the vendor
- In the 2004/2005 timeframe, John Gilligan, CIO for the U.S. Air Force, decided to use the leverage of Air Force procurement of Windows systems to require that Microsoft and its OEMs configure delivered systems in accordance with CIS benchmarks.

The Air Force now has 99%+ of its Windows XP Service Pack 2 systems configured in accordance with a single configuration standard.

The Air Force experience set the stage for the OMB mandate and action.

Establishing the Configurations

How were the standard configuration definitions established?

First by a group of users and security experts, both public and private sector, assembled by CIS. Based on this work, CIS established the Gold Standard for Windows 2000 in 2002. Vendors (Microsoft, Cisco, Hewlett-Packard, Sun) then joined this process.

The U.S. National Institute of Standards and Technology (NIST) is the owner of the standard configuration definitions used by the U.S. government. They are maintained in the National Vulnerability Database, which is a work in progress.

PART 2: CHALLENGES AND TIPS FOR IMPLEMENTING STANDARD CONFIGURATIONS

Create a Standard Image

The Air Force bundles the standard configurations with the most commonly used applications: Microsoft Office, Internet Explorer, plus a few others that everyone uses.

Make sure there is a process in place to ensure that all applications are fully functional when running on the standard configuration.

Expect and Deal with Pushback

Recognize that system administrators will often feel their prerogative and freedoms are being taken away and will believe their configurations are superior to the standard.

This initiative therefore requires a strong and resolute will at the leadership level.

Centralize the Patch Process

The Air Force expects to save approximately $200 million over time as a result of using standard software configurations for which patches can be tested and applied globally as a centralized (versus decentralized, individual-user) activity.

Enforce a Universal Comply-to-Connect Policy

In the future, any system that accesses the Air Force network will be tested for compliance with the standard configuration prior to being connected. Access by non-compliant systems will be denied.

Provide Incentives

As one example, the Air Force offers discounted laptops to military and civilian personnel to use as home systems. These have the standard configuration in case they are used to access an Air Force network remotely.

Learn from the Experience of Others

OMB is using the Air Force experience and lessons learned as its model.

PART 3: HAVING THE COLLECTIVE WILL TO MAKE IT STICK

Governance and Policy

Governance and policy actions are required to ensure standard configurations are adopted and enforced as a cultural norm.

Committed, Resolute, Knowledgeable Leaders and Champions

Karen Evans, the Administrator of the Office of Electronic Government and Information Technology at OMB, was a system administrator during her career and understands the issues arising when systems are improperly configured.

She is driving the OMB action based on the Air Force experience and model.

Ken Heitkamp, Air Force Associate CIO for Lifecycle Management for Warfighting Integration, drives the Air Force effort. He points to the resolute nature of the Air Force generals and colonels when dealing with pushback.

Leaders and users need to understand that some personal freedoms are sacrificed when connected to organizational networks and the Internet, given the high degree of interconnectivity and interdependence.

Address Cultural Differences

A military culture is certainly different from a federal government agency, which in turn is different from an academic institution or a commercial concern. Leaders need to determine what will work for their organization and culture.

Regardless, leadership will and governance structure are key.

Make Cost/Benefit Arguments

Using cost/benefit arguments like Southwest Airlines' decision to fly only one model of airplane (737) can help. Based on this decision, Southwest has a single standard for aircraft configuration, parts, inventories, and maintenance skills.

Standard configurations can provide significant operational and economic benefits.

Resources

The Center for Internet Security benchmarks and tools

Evans, Karen. "Ensuring New Acquisitions Include Common Security Configurations." Office of Management and Budget, Executive Office of the President, June 2007.

"Guidance for Securing Microsoft Windows XP Systems for IT Professionals." National Institute of Standards and Technology, Computer Security Resource Center, November 2005.

"Guidance for Securing Microsoft Windows Vista." National Institute of Standards and Technology, Computer Security Resource Center, March 2007.

Johnson, Clay. "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems." Office of Management and Budget, Executive Office of the President, March 2007.

Miller, Jason. "OMB finalizes acquisition language for standard desktop configuration." FCW.com, June 5, 2007.

Yasin, Rutrell. "The long road toward standard configuration." GCN.com, April 2, 2007.

Yasin, Rutrell. "OMB to help agencies with standardized desktop configuration." FCW.com, May 24, 2007.