WHITE PAPER

beyondtrust®

Beyond Traditional Security

Computer Security and Compliance in the Federal Government

Table of Contents

The Federal Information Security Management Act of 2002 requires federal agencies to report on the state of their information security. The United States Office of Management and Budget released a reporting tool called CyberScope in 2009 to assist these agencies in meeting FISMA reporting requirements. CyberScope attempts to correct previous deficiencies and streamline the FISMA reporting process. BeyondTrust offers products that allow organizations to comply with these requirements.

Overview

Continuous monitoring is a process that detects compliance issues with an organization's IS environment. The United States Department of State performs continuous monitoring on its network of 40,000 computers and 5,000 routers, which support 285 posts throughout the world. It uses the Risk Scoring Program to monitor an information system and assess its security in ten categories. The system receives a score between one and ten in each category, with one representing the highest level of security and ten representing the lowest level of security. The RSP uses these ten scores to assign a single letter grade to the IT professionals responsible for that system, with "F-" being the worst grade and "A" being the best grade. This assessment is performed at least once every two days.

The continuous-monitoring model of the RSP provides IT professionals with their degree of risk, and it also encourages a sense of competition with their peers. The State Department reports that its RSP has reduced the risk of its domestic systems by 83 percent and that of its foreign systems by 84 percent since 2008. The OMB has also implemented a security dashboard to complement CyberScope's automated reporting capability. This dashboard helps to ensure that CyberScope submits its reports in a timely manner.

CyberScope uses the Internet to collect reports on IT security from federal agencies. This represents a fundamental change in the IT reporting method, which agencies previously performed on paper. Cyberscope currently has about 600 agency staff members who access this system through a standard interface by logging in with a personal identity verification and personal identity number. Users then enter live data and transmit it in a standard format to the OMB. The OMB then compiles this information and generates reports which it transmits to other agencies according FISMA requirements.

An information assurance vulnerability alert is a notification of a vulnerability that exists in an operating system or application software. The United States Cyber Command analyzes vulnerabilities on hosts that reside on the Global Information Grid and determines if the Department of Defense needs to issue an IAVA. This practice allows components of the DOD to take the appropriate action to minimize the security threat posed by these vulnerabilities.

The DOD uses three severity categories to classify a weakness in an information system. These categories include CAT I, CAT II and CAT III, with CAT I being the most severe and CAT III being the least severe. Certifying authorities or their designated representatives assign a DOD severity category to a system weakness after considering all mitigating factors.

Requirements

FISMA requires federal agencies to perform the following activities on a recurring basis:

- Report IS data each month
- Answer security questions
- Attend accountability sessions and interviews

DATA FEEDS

The security management tools of each federal agency automatically collect IS data for that agency. These agencies must load specific elements from this data into CyberScope on a monthly basis as of Sept. 2011, whereas the previous requirement called for annual reporting. The monthly reporting metrics for fiscal year 2010 and FY 2011 were identical, but the Chief Information Officer Council's Continuous Monitoring Working Group will collaborate with agencies over time to further develop reporting requirements. The Department of Homeland Security will provide agencies with revisions to the reporting requirements and they will also be published in CyberScope in sufficient time for the agencies to adopt them. Changes to the data feed schema will also be published in CyberScope prior to their use. The CyberScope information page will provide the answers to common questions on the monthly data feeds.

SECURITY QUESTIONS

Agencies must also provide CyberScope with the answers to a set of IS questions. The primary goals of these questions are to determine the security capabilities of the agencies' information systems and assess their effectiveness.

ACCOUNTABILITY SESSIONS AND INTERVIEWS

The DHS implemented a schedule of accountability sessions and interviews for federal agencies known as CyberStat in Jan. 2011. It allows IS security experts in the DHS to assist selected agencies in developing action plans to improve their security. CyberScope and other sources provide data for CyberStat, allowing agencies to achieve greater accountability over their security practices. CyberStat sessions will allow the DHS to respond quickly in assisting agencies with addressing security risks. The specific objectives of CyberStat include the following:

- Identify areas of security that require additional focus
- Assist agencies in meeting FISMA requirements
- Recognize agencies that meet these standards.

The participants in CyberStat sessions include representatives from the DHS, National Security Staff and the OMB. They examine the agency's IS data to identify security risks and produce an action that allows the agency to improve its performance. The information obtained from the CyberStat process also provides a general assessment of the federal government's security posture, which may contribute towards future policy decisions. An agency that doesn't receive a CyberStat review may still be subject to interviews from government IS specialists. The purpose of these interviews will be to identify specific security threats that are unique to that agency.

Benefits

The primary benefit of compliance with FISMA requirements is to protect information from unauthorized access, including the disclosure, use, modification and destruction of that data. FISMA strengthens IS security by assigning specific responsibilities to each agency involved in this process such as the OMB and the National Institute of Standards and Technology. This policy requires the head of each agency to implement procedures that will reduce IS security risks to an acceptable level in a cost-effective manner. The specific goal of FISMA for FY 2011 was to create an enterprise for the federal government that can protect information by using technological innovations.

Agencies should use existing processes that perform continuous monitoring to collect data that they will report to CyberScope. The implementation of a new process typically requires additional resources, which are better used for mission-critical activities. The increase in reporting frequency allows IS specialists to make security decisions more quickly and with more current information.

The security authorization required by FISMA allows agencies to assess the effectiveness of its security controls. This

includes a determination that these controls have been implemented correctly, are functioning as required, and are producing the desired result. The security authorization process also requires continuous monitoring as specified by NIST SP 800-53, Revision 3 and NIST SP 800-37, Revision 1. These documents also describe the controls that are needed to protect the information system. OMB requires CIOs to provide a quantitative assessment of their organization's security authorization process, while Inspectors General must provide a qualitative assessment of this process.

Solutions

BeyondTrust's products support directives used to comply with FISMA requirements such as FDCC, SCAP and DIACAP. Our products are designed to meet the needs of many government agencies, which often have complex, heterogeneous infrastructures. BeyondTrust provides the following solutions for meeting federal security requirements:

- Retina CS Threat Management Console
- Retina Insight
- PowerBroker Servers for Linux & Unix
- PowerBroker for Windows

The key benefits of our products include the ability to identify the actions that will produce the greatest reduction in an agency's security risk. They also perform automatic reporting on compliance efforts and policy management. The key capabilities of BeyondTrust's products include a comprehensive assessment of an agency's vulnerabilities, and our products also have modules that perform integrated patch management.

RETINA CS THREAT MANAGEMENT CONSOLE

Retina CS is a platform that simplifies the challenge of complying with Cyberscope requirements. It provides threat awareness in real time, allowing you to assess the level of each threat and adjust your security strategy accordingly. Retina CS also allows you to deploy secure servers without compromising user productivity by implementing the concept of least privilege.

RETINA INSIGHT THREAT INTELLIGENCE MODULE

Retina Insight reduces security risks by continuously monitoring your information systems. It generates built-in reports on trends in vulnerabilities and compliance that include analytical views and drilldowns. Retina Insight also provides a single library for these reports that saves space while still allowing you to meet your Cyberscope reporting requirements.

POWERBROKER SERVERS FOR LINUX & UNIX

PowerBroker Servers for Linux & Unix provides easy control over root-level access, allowing you to increase collaboration between users without compromising your security. It complies with Cyberscope requirements by logging information on the system environment and automatically centralizing those logs when you have more than one server. PowerBroker Servers also automates workflows for log reviews and generates reports that are ready for an audit.

POWERBROKER FOR WINDOWS

PowerBroker for Windows uses Group Policy and Active Directory to eliminate the need for users to have administrator privileges. This solution provides complete control over the programs that a user is able to run, which provides protection from all types of malware. PowerBroker allows you to meet Cyberscope requirements by improving the security posture of your information systems without impacting your users.

beyondtrust®
Beyond Traditional Security

About BeyondTrust

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) and vulnerability management solutions for dynamic IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world's 10 largest banks, seven of the world's 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities. The company is privately held, and headquartered in Carlsbad, California. For more information, visit **beyondtrust.com**.

CONTACT INFO

NORTH AMERICAN SALES
1.800.234.9072
sales@beyondtrust.com

EMEA SALES
Tel: + 44 (0) 8704 586224
emeainfo@beyondtrust.com

CORPORATE HEADQUARTERS
550 West C Street, Suite 1650
San Diego, CA 92101
1.800.234.9072

CONNECT WITH US
Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com