Federal Agency Security Practices (FASP)
VA Central Incident Response Capability (VA-CIRC)
Submitted by:
Department of Veterans Affairs'
Office of Cyber and Information Security (OCIS)

Background

"*For those who have borne the battle, for their widows, and their orphans*". In 1865, Abraham Lincoln expressed this founding idea, which has become the guiding principle of the Department of Veterans Affairs. Toward that end, VA has become the nation's largest health care and cemetery services provider and the provider and guarantor of significant other financial benefits and services for 25.5 million living veterans. With 225,000 employees managing services and benefits of over $60 billion annually, its information infrastructure connects with veterans and partners nationwide and represents an important piece of the nation's critical infrastructure.

The VA Office of Information and Technology (OI&T) is a critical enabling component for this important responsibility. The mission of the Office of Cyber and Information Security (OCIS) within OI&T is two-fold:

- To provide information security services to veterans and their beneficiaries that protect their private information and enable the timely, uninterrupted and trusted nature of those services, and
- To provide assurances that cost-effective information security controls are in place to protect automated information systems from financial fraud, waste and abuse.

To oversee the confidentiality, integrity, availability and accountability for use of the health and benefit information processed on its information systems, it is essential to closely monitor threats to, and vulnerabilities of, VA's complex information enterprise. Expert guidance must also be provided to field elements concerning the prioritization of mitigation actions and, when necessary, how to implement those mitigation actions. Response, recovery and reporting responsibilities for actual cyber security incidents are also essential for the reliable operation of VA networks and compliance with Federal regulatory requirements. This Federal Agency Security Practices (FASP) write-up sets out the pathway followed by OCIS to create a VA Critical Incident Response Capability (VA CIRC).

Problem

Management of cyber security for VA's extensive and geographically distributed information assets is complicated by the fact that the systems and information technology staff supporting individual VA lines of business are not yet fully integrated under a standard architecture or organizational structure. The historical problems of decentralized architecture and cyber security management have resulted in a technically and organizationally diverse information enterprise that as a consequence is vulnerable to risks promoted by miscommunication and slow response to events. Coupled with the threats of rapidly spreading malicious code and the ever-present potential for compromise by individuals with malicious intent, this creates conditions that require immediate and coordinated security management throughout VA.

The lack of an enterprise-wide and comprehensive incident response capability contributed to a persistent weakness in the Department's security posture, permitting a serious risk to the organization's critical IT systems, the privacy of the veterans' and other sensitive information, and VA's ability to perform its mission.

Solution

Over a period of months, OCIS created the appropriate contract vehicle for the VA environment with service level agreements and appropriate other requirements. These included the following:

- Monitoring and reporting on the cyber security posture of the Department;
- Coordinating externally with other government incident response centers such as the Department of Homeland Security's Federal Computer Incident Response Center (FedCIRC);
- Performing threat and vulnerability analysis and providing warnings of anticipated exploitation attempts;
- Assisting in vulnerability scanning and penetration testing;
- Providing cyber security deficiency remediation guidance, such as necessary patches for software;
- Developing concepts of operations and other related policies, procedures and guidelines relating to cyber security incidents;
- Performing analysis of cyber security events;
- Maintaining detailed logs and databases of VA cyber security incidents and response;
- Performing the full range of function across the spectrum of activities relating to incident management and response, which generally includes detection, pre-emption, prevention, reaction, response and recovery; and
- Providing state-of-the-practice incident handling and response capabilities for the VA enterprise.

The VA-CIRC was awarded to a conglomerate of small and large business industry partners, the VA Security Team (VAST). The VA CIRC is in part collocated with the VA network monitoring team in a Network and Security Operation Center (NSOC), which facilitates the timely resolution of network performance and security-related issues.

As the first anniversary of this contract award approaches, the VA CIRC has become the national focal point to monitor, manage, report, and remediate all cyber security incidents having enterprise-wide implications and to operate the anti-virus signature file push capability by utilizing VA's Network and Security Operations Centers (NSOC). The VA CIRC also monitors and manages host-based and network-based intrusion detection sensors and firewalls at all VA network interconnection points. When attacks are detected, the VA-CIRC cyber security team isolates the problem, develops and implements a fix, and tracks the source of the attack so that action can be taken, and manages the Department-wide recovery effort when required.

Process

OCIS provides the funding, management staff, and authority for VA CIRC to manage monitoring and resolution of cyber security incidents and threats to the VA enterprise. A VA CIRC Charter identifies the management structures to ensure changes and issues affecting project completion are properly controlled. A Project Control Board (PCB) consists of a Project Manager and supporting functional team leaders. An Executive Steering Committee (ESC) furnishes executive direction to the PCB.

Major Milestones

- Establish an overall VA-CIRC implementation plan and schedule.
- Begin research and implementation plan for advanced technology testing and integration with VA's infrastructure.
- Complete VA-CIRC associated "defense-in-depth" technology acquisitions.
- Establish "defense-in-depth" at all 17 VA national Internet gateways.
- Complete VA-CIRC presence at field NSOC.
- Acquire and implement redundant VA-CIRC presence at additional NSOCs.
- Integrate and implement advanced technology monitoring technologies.
- Implement penetration testing and scanning support.
- Operate and support all VA national Internet gateways
- Operate VA-CIRC as an integrated VA IT utility.

Contacts

Bruce A. Brody, CISM, CISSP
Associate Deputy Assistant Secretary for Cyber and Information Security
Department of Veterans Affairs
202-273-8007
bruce.brody@mail.va.gov

Pedro Cadenas, Jr.
Deputy ADAS for Cyber and Information Security
Department of Veterans Affairs
202-273-8431
pedro.cadenas@mail.va.gov

Michael S. Arant, CISSP
Cyber Security Liaison
Department of Veterans Affairs
michael.arant@mail.va.gov