November 2014

INFORMATION SECURITY

VA Needs to Address Identified Vulnerabilities

GAO Highlights

Highlights of GAO-15-117, a report to the Chairman, Committee on Veterans' Affairs, House of Representatives

Why GAO Did This Study

In carrying out its mission to ensure the health, welfare, and dignity of the nation's veterans, VA relies extensively on information technology systems that collect, process, and store veterans' sensitive information. Without adequate safeguards, these systems and information are vulnerable to a wide array of cyber-based threats. Moreover, VA has faced long-standing challenges in adequately securing its systems and information, and reports of recent incidents have highlighted the serious impact of inadequate information security on the confidentiality, integrity, and availability of veterans' personal information.

GAO was asked to review VA's efforts to address information security vulnerabilities. The objective for this work was to determine the extent to which selected, previously identified vulnerabilities continued to exist on VA computer systems. To do this, GAO reviewed VA actions taken to address previously identified vulnerabilities, including a significant network intrusion, vulnerabilities in two key web-based applications, and security weaknesses on devices connected to VA's network. GAO also reviewed the results of VA security testing; interviewed relevant officials and staff; and reviewed policies, procedures, and other documentation.

What GAO Recommends

GAO is making eight recommendations to VA to address identified weaknesses in incident response, web applications, and patch management. In commenting on a draft of this report, VA stated that it concurred with GAO's recommendations.

View GAO-15-117. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

While the Department of Veterans Affairs (VA) has taken actions to mitigate previously identified vulnerabilities, it has not fully addressed these weaknesses. For example, VA took actions to contain and eradicate a significant incident detected in 2012 involving a network intrusion, but these actions were not fully effective:

- The department's Network and Security Operations Center (NSOC) analyzed the incident and documented actions taken in response. However, VA could not produce a report of its forensic analysis of the incident or the digital evidence collected during this analysis to show that the response had been effective. VA's procedures do not require all evidence related to security incidents to be kept for at least 3 years, as called for by federal guidance. As a result, VA cannot demonstrate the effectiveness of its incident response and may be hindered in assisting in related law enforcement activities.
- VA has not addressed an underlying vulnerability that allowed the incident to occur. Specifically, the department has taken some steps to limit access to the affected system, but, at the time of GAO's review, VA had not fully implemented a solution for correcting the associated weakness. Without fully addressing the weakness or applying compensating controls, increased risk exists that such an incident could recur.
- Further, VA's policies did not provide the NSOC with sufficient authority to access activity logs on VA's networks, hindering its ability to determine if incidents have been adequately addressed. In an April 2014 report, GAO recommended that VA revise its incident response policies to ensure the incident response team had adequate authority, and VA concurred.

Further, VA's actions to address vulnerabilities identified in two key web applications were insufficient. The NSOC identified vulnerabilities in these applications through testing conducted as part of the system authorization process, but VA did not develop plans of action and milestones for correcting the vulnerabilities, resulting in less assurance that these weaknesses would be corrected in a timely and effective manner.

Finally, vulnerabilities identified in VA's workstations (e.g., laptop computers) had not been corrected. Specifically, 10 critical software patches had been available for periods ranging from 4 to 31 months without being applied to workstations, even though VA policy requires critical patches to be applied within 30 days. There were multiple occurrences of each missing patch, ranging from about 9,200 to 286,700, and each patch was to address an average of 30 security vulnerabilities. VA decided not to apply 3 of the 10 patches until it could test their impact on its applications; however, it did not document compensating controls or plans to migrate to systems that support up-to-date security features. While the department has established an organization to improve its vulnerability remediation, it has yet to identify specific actions and milestones for carrying out related responsibilities. Until VA fully addresses previously identified security weaknesses, its information is at heightened risk of unauthorized access, modification, and disclosure and its systems at risk of disruption.