Treasury Inspector General for Tax Administration
Office of Audit

WHILE CONTROLS HAVE BEEN IMPLEMENTED TO ADDRESS MALWARE, CONTINUED ATTENTION IS NEEDED TO ADDRESS THIS GROWING THREAT

Issued on March 10, 2009

Highlights

Highlights of Report Number: 2009-20-045 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Malware refers to a computer program that is inserted into a computer system with the intent of compromising the confidentiality, integrity, or availability of an organization's data, applications, or operating systems. Without ongoing attention to the preventive and response controls to address malware, Internal Revenue Service (IRS) computers and the sensitive taxpayer data stored on them are at risk of compromise that could ultimately result in theft of taxpayer identities and fraud.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of our statutory requirements to annually review the adequacy and security of IRS information technology. The overall objective of this review was to determine whether adequate security controls are present to prevent and respond to malware attacks.

WHAT TIGTA FOUND

The IRS' preventive and response controls to address malware are generally effective; however, continued attention should be given to limiting some practices that increase the risk of malware incidents and increasing employee awareness of their responsibilities for preventing malware incidents. TIGTA found that virus scans for servers are not automated and must be manually initiated by the system administrators. TIGTA's analysis of antivirus scans determined that 89 percent of the servers were usually scanned weekly. The remaining servers were scanned less frequently or not at all.

To limit the risk of malware infection, system administrators are prohibited from using their administrator accounts to access the Internet unless authorized by the Chief Information Officer. In a 1-week period in February 2008, TIGTA identified 63 administrator accounts that successfully accessed Internet web sites a total of 820 times without authorization. The IRS did not conduct sufficient monitoring to ensure that administrator accounts are sufficiently controlled to prevent compromise by malware-infected sites.

Also, employees are not routinely contacted when their system activity results in a successful malware incident or when their actions violate IRS policy. TIGTA believes that notifying users of their specific activities that resulted in malware infections would serve to better educate users about the malware threat, and that IRS management has a responsibility to notify employees and their managers when their actions violate IRS policies.

In addition, the IRS mandatory annual security awareness training does not include the use of personal portable devices and removable media as common ways in which users can infect systems with malicious code. Of the 661 malware incidents reported in 2007, 69 (10 percent) were caused by users inserting removable media or connecting external or portable hard drives to their systems.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer 1) schedule automatic scans of antivirus software on servers, 2) regularly remind administrators not to use their administrator accounts to access the Internet and monitor Internet activity to determine whether administrators are complying with this control, 3) notify employees and their managers when their activity results in a successful malicious code incident, particularly when the activity is a violation of IRS policy, and 4) update the IRS security awareness training to include the risk of introducing malware when using portable and removable media.

In their response to the report, IRS officials agreed with the recommendations and plan to take appropriate corrective actions. The IRS plans to schedule automated antivirus scans on servers, regularly monitor servers to ensure antivirus scans are executed weekly, ensure administrators are regularly reminded of Internet access restrictions, and continually monitor for Internet access by administrator accounts and report violations for followup actions. In addition, the IRS plans to ensure employees and their managers are notified regarding applicable cyber incidents, and convert to the Department of the Treasury mandated information systems security awareness training course that addresses the use of portable and removable media as common ways that users can introduce malicious code to the network and potential effects.

READ THE FULL REPORT

To view the report, including the scope, methodology, and full IRS response, go to:

http://www.treas.gov/tigta/auditreports/2009reports/200920045fr.pdf.

Email Address: inquiries@tigta.treas.gov
Web Site: http://www.tigta.gov
Phone Number: 202-622-6500