Treasury Inspector General for Tax Administration

INADEQUATE SECURITY CONTROLS OVER ROUTERS AND SWITCHES JEOPARDIZE SENSITIVE TAXPAYER INFORMATION

Issued on March 26, 2008

Highlights

Highlights of Report Number: 2008-20-071 to the Internal Revenue Service Chief Information Officer

IMPACT ON TAXPAYERS

Access controls for Internal Revenue Service (IRS) routers were not adequate, and reviews to monitor security configuration changes were not conducted to identify inappropriate use. A disgruntled employee, contractor, or hacker could reconfigure routers and switches to disrupt computer operations and steal taxpayer information.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether controls were sufficient to detect and deter unauthorized use of IRS routers and switches, two key components used to direct network traffic. Because the IRS sends sensitive taxpayer and administrative information across its networks, routers on the networks must have sufficient security controls to deter and detect unauthorized use.

WHAT TIGTA FOUND

The IRS uses the Terminal Access Controller Access Control System (TACACS+) to administer and configure routers and switches. At the time of our review, the IRS had authorized 374 accounts for employees and contractors on the TACACS+ that could be used to access routers and switches to perform system administration duties. Of these, 141 (38 percent) did not have proper authorization to access the TACACS+. Authorizations for 86 of the 141 employee and contractor accounts had been provided on some prior date, but the authorizations had expired at the time of our review. TIGTA is particularly concerned that 27 of the 55 employees and contractors had accessed the routers and switches to change security configurations.

To authenticate users, the TACACS+ uses a security application that requires users to enter an account name and password. System administrators had circumvented this control by setting up 34 unauthorized accounts that appear to be shared-user accounts. In addition, audit trail log reviews were not being conducted by the Cybersecurity office, and only a limited percentage of the audit trails for the IRS routers and switches were being reviewed. The review of audit trails is necessary to detect potential security events such as hacking attempts, virus or worm infections, and attempts to change or alter information. Also, system administrators were not following IRS procedures that require an authoritative, IRS-wide time server for the purpose of synchronizing the system clocks of IRS systems.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer clarify responsibilities for reconciling user accounts on the TACACS+, improve the testing of authentication controls on the TACACS+, ensure that the TACACS+ is configured to prevent employees and contractors from gaining access to the routers and switches if they have not used the system within 90 calendar days, eliminate unnecessary shared accounts, and ensure that each account is properly authorized. In addition, the Chief Information Officer should ensure that the Enterprise Networks organization provides the audit trails for the TACACS+, routers, and switches to the Cybersecurity office for periodic reviews; audit trail information is filtered for effective analysis; and all routers and switches are configured to the same time zone.

In their response to the report, IRS officials stated they agreed with six of the recommendations and plan to evaluate implementation of the seventh. The IRS plans to begin monthly reconciliation of the TACACS+ user accounts, implement testing of the authentication controls on the TACACS+, ensure that employee user accounts are locked after 45 calendar days of inactivity and removed after 90 calendar days of inactivity, and ensure that no unauthorized or unnecessary shared accounts exist on the TACACS+. In addition, the IRS plans to continue to filter audit log information, and the Enterprise Networks organization plans to ensure that the Cybersecurity office has access to all audit trail information for review and analysis. The IRS plans to evaluate the TIGTA recommendation to configure all routers and switches to the same time zone to determine whether this approach is an appropriate enterprise solution. TIGTA will follow up on the adequacy of these corrective actions in future audits.

READ THE FULL REPORT

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

http://www.treas.gov/tigta/auditreports/2008reports/200820071fr.pdf.