Evaluation Report

OIG-CA-09-005

INFORMATION TECHNOLOGY: Network Security at the Alcohol and Tobacco Tax and Trade Bureau Could Be Improved

December 18, 2008

Office of Inspector General

Department of the Treasury

Contents

Abbreviations

CIO	Chief Information Officer
FDCC	Federal Desktop Core Configuration
NFR	notification of findings and recommendations
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication
TCIO	Treasury Chief Information Officer
TD P	Treasury Directive Publication
TTB	Alcohol and Tobacco Tax and Trade Bureau

December 18, 2008

John J. Manfreda
Administrator
Alcohol and Tobacco Tax and Trade Bureau

The purpose of our evaluation was to assess the network security of the Alcohol and Tobacco Tax and Trade Bureau (TTB). Our overall objective was to determine whether sufficient protections exist to prevent intrusions into TTB's network and systems. To accomplish this objective, we used specialized software to detect and exploit vulnerabilities in TTB's systems. In addition, we performed social engineering tests to gauge user awareness of security threats and examined compliance with requirements to implement the National Institute of Standards and Technology (NIST) Federal Desktop Core Configuration (FDCC).[1] We performed our fieldwork from January through July 2008. Appendix 1 contains a detailed description of our objective, scope, and methodology.

Results in Brief

We found that TTB had established adequate security controls to prevent remote exploitation and compromise of workstations, servers, and infrastructure devices. However, we identified areas of improvements where TTB should take additional steps to improve the security controls over its network and systems. For example, we reported high-severity security vulnerabilities on some TTB systems resulting from ineffective security configurations, such as unnecessary or insecure services running on systems.[2] In addition,

[1] Office of Management and Budget Memorandum (OMB) M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems" (Mar. 22, 2007), required agencies to implement common security configurations developed by NIST for Windows Vista and XP operating systems by February 1, 2008.

[2] International Business Machines Internet Security Systems, a company that provides security products and services designed to protect organizations against Internet threats, defines high-severity

we found the use of default passwords, granting of excessive database privileges, failure of some systems to display required warning banners, missing patches, and unsupported or obsolete software versions. Furthermore, we found that several systems did not have the required FDCC settings. We also determined that TTB could improve user awareness of workstation security, and network shared-drive access.

Our three overall findings with respect to TTB network security are as follows:

1. Several TTB network systems did not meet security configuration requirements.
2. Unlocked workstations pose security risks.
3. Access restrictions were inadequately established for a shared network drive.

Upon completion of our fieldwork, we provided three notifications of findings and recommendations (NFR), which included 18 recommendations, to the Chief Information Officer (CIO) of TTB. The CIO concurred with our findings and recommendations and provided plans for corrective actions. Due to the sensitivity of the recommendations, we are summarizing them as follows for this report:

1. Reconfigure some system services with more secure options.
2. Correct password security measure in TTB systems that do not conform to Treasury and NIST policies.
3. Ensure that the principle of least privilege is enforced and applied to the identified TTB systems, which have not already enforced it.
4. Apply the latest service packs and security updates for the identified systems and applications, which have not been updated.
5. Continue to implement security configurations required by Treasury, NIST, and OMB policies.
6. Continue to improve user awareness of the need to lock unattended workstations.

vulnerabilities as allowing immediate remote or local access, or immediate execution of code or commands, with unauthorized privileges.

7. Ensure that appropriate access restrictions are established for the identified shared network drive.

A crosswalk will be provided to the CIO with this report, which links the 7 recommendations listed above to the 18 recommendations provided in the NFRs.

Background

TTB is the newest Treasury bureau and employs more than 600 people. It is responsible for collecting more than $14 billion a year in federal alcohol, tobacco, firearms, and ammunition excise taxes, as well as the permit systems and regulations established for those industries under the authority of the Internal Revenue Code and the Federal Alcohol Administration Act.

Because TTB's network computers are connected with each other, other bureaus' networks, and the Internet, it is important that proper configurations and controls be in place to ensure that only authorized users are granted access. Unauthorized access to TTB's network could provide an intruder with the opportunity to compromise the confidentiality, integrity, and availability of sensitive information. Once inside, unauthorized users could extract, delete, or modify sensitive data; discover user names and passwords; and launch denial-of-service attacks. Undetected, such activities could hinder TTB's mission and undermine public faith in TTB's ability to safeguard the tax information it collects.

Findings and Recommendations

Finding 1 Several TTB Network Systems Did Not Meet Security Configuration Requirements

We found that several TTB network systems were configured ineffectively and did not meet the security configuration requirements set forth by NIST; Treasury Directive Publication (TD P) 85-01, "Treasury Information Technology Security Program" (Nov. 3, 2006); OMB; and/or TCIO. We identified high-severity

vulnerabilities that resulted from systems running unnecessary or insecure service. In addition, we found vulnerabilities resulted from ineffective configurations as follows:

- Default passwords in use on network devices
- Excessive permissions and privileges granted on database external procedure services, jobs, users, and groups
- Database servers with inadequate limits on the number of failed logins
- Failure of some systems to display the warning banner
- Failure of systems to meet some FDCC settings
- Publicly accessible TTB system running with local administrative privileges and lacking FDCC settings

NIST SP 800-53 recommends that organizations configure information systems to provide only essential capabilities and specifically prohibits or restricts the use of the functions, ports, protocols, and/or services as defined by the agency. In addition, TD P 85-01 requires that bureaus change all default vendor- or factory-set administrator accounts and passwords before installation or use. NIST 800-53 also recommends that the information system enforce the most restrictive set of rights/ privileges or accesses needed by users or processes acting on behalf of users. Similarly, OMB Circular No. A-130, "Security of Federal Automated Information Resources," appendix III, requires that controls include least privilege to restrict a user's access or type of access to the minimum necessary. TD P 85-01 requires that patches be tested and installed on a timeline in accordance with the criticality of the patches. OMB 07-11 requires implementation of FDCC on all systems running Windows XP operating system.

Unnecessary or insecure services could result in a larger potential attack surface, more potential entry points, information disclosure, or additional overhead to maintain unneeded functionality. Additionally, insufficient access controls allow attackers to gain more knowledge about the remote host or to change the configuration of the remote system to disrupt the agency's mission. When a warning banner is missing, the boundary of systems is not clearly delineated, thereby encouraging or

consenting to unauthorized access. Furthermore, failure to apply up-to-date patches or to update obsolete software versions would make TTB's systems susceptible to network virus infection and hacker attacks. Finally, failure of systems to meet some FDCC settings could also result in reduced confidentiality, integrity, and availability of information.

Recommendations

We recommend that the Administrator

1. reconfigure some system services with more secure options;
2. correct password security measure in TTB systems that do not conform to Treasury and NIST policies;
3. ensure that the principle of least privilege is enforced and applied to the identified TTB systems which have not already enforced it;
4. apply the latest service packs and security updates for the identified systems and applications which have not been updated;
5. continue to implement security configurations required by Treasury, NIST, and OMB policies.

Finding 2 Unlocked Workstations Pose Security Risks

Unlocked workstations pose a security risk to user credentials and information. Even though TTB implemented automatic lockout through domain policy, we found that not all users manually locked their workstations when leaving them unattended. As a result, the systems could be accessed by anyone using the user credentials during the unattended period. During our social engineering test, we were able to insert our Universal Serial Bus drive into three unattended workstations and load our specially coded program onto the system. From our penetration test laptop, we had full remote control of the workstations with the user's access level. With this access, we could view user activities and capture sensitive information, including the active directory listing that contained TTB's network resource information. Attacks performed from this point on would appear to have originated from the user.

TD P 85-01, control S-WS.1, requires that unattended workstations be disabled for use by anyone other than authorized individuals (such disabling would typically require logging off, locking, password-protecting, or other means). In addition, TTB Memorandum 0 7250.1, "Alcohol and Tobacco Tax and Trade Bureau Automated Information Systems Security Program Policy," section 6.5.11, "Users and Employees," requires users to ensure that adequate protection is maintained on their workstation, including not sharing their passwords with any other person and logging out, locking, or enabling a password-protected screen saver before leaving their workstation.

Malicious individuals with physical access to unlocked systems could run programs, uncover sensitive information, or perform other activities on the system. Such activities would appear to have originated from the authorized user.

Recommendation

We recommend that the Administrator

6. continue to improve user awareness of the need to lock unattended workstations.

Finding 3 Access Restrictions Were Inadequately Established for a Shared Network Drive

We determined that access restrictions were inadequately established for a shared network drive. After gaining access to unattended workstations, as mentioned in finding 2, we discovered that TTB users have open access to the shared network drive, which contains potentially sensitive information. We were able to open any of the files or folders we attempted to access on this drive. Specifically, we were able to access program code for one of TTB's applications, legal documents and forms with customer information, personally identifiable information, and partial social security numbers. We were informed that TTB established this network drive to allow sharing or transferring of information

between users in different work groups. However, we found that neither users nor TTB network administrators established adequate security permissions to allow or deny user or group access to individual files and folders.

NIST SP 800-53 requires that information systems be enforced with the most restrictive set of rights, privileges, or accesses needed by users to perform specified tasks. In addition, TTB Memorandum 0 7250.1, "Alcohol and Tobacco Tax and Trade Bureau Automated Information Systems Security Program Policy," requires TTB administrators to enforce compliance with executive, legislative, and technical requirements to ensure that only appropriate personnel with a "need to know" are granted access to sensitive information. Also, TTB requires implementation of logical access controls to provide protection from unauthorized access, alteration, loss, disclosure, and availability of information. Additionally, section 522a of title 5, United States Code, requires that agencies implement comprehensive privacy and data protection procedures. These procedures govern the agency's collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to agency employees and the public.[3]

The lack of access control on the shared network drive could allow TTB users and attackers unrestricted access to a wide variety of sensitive information, including personally identifiable information. Storage of such unauthorized information could result in noncompliance with federal privacy requirements. Unprotected sensitive data could also result in significant data breaches, causing harm to the agency's image and reputation. Also, the availability of application code on the shared network drive could provide useful information to attackers.

[3] Section 522a of title 5, United States Code, Records maintained on individuals.

Recommendation

We recommend that the Administrator

7. ensure that appropriate access restrictions are established for the identified shared network drive.

Management Response

As noted in appendix 2, TTB management agreed with our findings and recommendations and has either implemented or will be implementing the recommendations by July 2009.

OIG Response

We agree that the formal steps TTB has proposed are responsive to the intent of our findings and recommendations.

* * * * * *

I would like to extend my appreciation to the TTB CIO and TTB staff for the cooperation and courtesies extended to my staff during the evaluation. If you have any questions, please contact me at (202) 927-5171 or Abdirahman Salah, IT Specialist, Office of Information Technology Audits, at (202) 927-5763. Major contributors to this report are listed in appendix 3.

/s/

Tram J. Dang, Director
Office of Information Technology Audits

The overall objective of this evaluation was to determine whether sufficient protections exist to prevent intrusions into the Alcohol and Tobacco Tax and Trade Bureau (TTB) network, systems, or computer equipment. This evaluation was included in the Office of Inspector General Annual Plan for 2008. In addition, the results of this evaluation may be used to support our work undertaken in accordance with the requirements of the Federal Information Security Management Act. We performed our fieldwork at TTB locations and the Treasury Office of Inspector General in Washington, D.C., from January through July 2008. We conducted our evaluation in accordance with the President's Council on Integrity and Efficiency's Quality Standards for Inspections.

We performed most logical tests from within TTB's network and from the Internet.[4] We did not prioritize or rank the security vulnerabilities detected by the tools used, nor did we evaluate the remedies for the vulnerabilities identified. In conducting our review, we used specialized software to conduct the vulnerability scanning and penetration testing. We also performed social engineering tests to evaluate user awareness and responsibility in protecting information and information systems.

Upon completion of our tests, we provided TTB management with reports generated by our tools and evidence of findings. The reports provided details on specific vulnerabilities detected and exploited and the suggested actions needed to address them. We also provided TTB management with notifications of findings and recommendations so that corrective actions could be implemented immediately.

[4] Logical tests are tests that exploit vulnerabilities in the computer's software.

Department Of The Treasury
Alcohol And Tobacco Tax And Trade Bureau
Washington, DC 20220

December 18, 2008

MEMORANDUM FOR: Tram J. Dang
Director, Office of Information Technology Audit, OIG

FROM: Robert J. Hughes
Chief Information Officer, Alcohol and Tobacco Tax and Trade Bureau

SUBJECT: Draft Report "INFORMATION TECHNOLOGY: Network Security at the Alcohol and Tobacco Tax and Trade Bureau Could Be Improved"

I appreciate the opportunity to review and comment on the subject report.

TTB is committed to information security, and we believe that we have a program in place that is significantly better than adequate. The effectiveness of our program is regularly demonstrated by the results of independent penetration tests and external program reviews. We understand that any security program can be improved, and we appreciate the efforts of OIG to help further strengthen our program. We concur with the three findings and their associated recommendations, and we immediately began addressing those findings as soon as we were informed of them. This memorandum outlines how TTB is addressing the findings and their associated recommendations.

Finding 1: *Several TTB network systems did not meet security configuration* requirements.
Recommendation 1: *Reconfigure some system services with more secure options.*
Recommendation 2*: Correct password security measure in TTB systems that do not conform to Treasury and NIST policies.*
Recommendation 3*: Ensure that the principle of least privilege is enforced and applied to the identified TTB systems, which have not already enforced it.*
Recommendation 4*: Apply the latest service packs and security updates for the identified systems and applications, which have not been updated.*
Recommendation 5*: Continue to implement security configurations required by Treasury, NIST, and OMB policies.*

TTB concurs with Finding 1 and the associated recommendations. TTB has already remediated or is currently remediating all findings where device settings can actually be modified and will be finished by July 2009. Out of a population of over 1500 devices (printers, storage arrays, servers), 52% of which were scanned, the OIG identified 43 as needing configuration changes. Of those 43 devices, 26 were non-production machines and 17 were production machines. TTB has updated or is updating the settings for all machines which were identified as needing updates. However, 10 production devices remain configured as-is due to the limitations of specific hardware (such as printers) and TTB's business need to use these services. TTB accepts the minimal risk that these devices present. Although we concur with the OIG's technical discoveries, we do not agree with the characterization of these items. The items identified by the OIG as "high-severity" are not considered formal vulnerabilities according to the Common Vulnerabilities and Exposures (CVE) database sponsored by the National Cyber Security Division of the Department of Homeland Security. All attempts at remote exploitation by the OIG to gain system access and exploit the TTB infrastructure failed, including tests conducted using the testing tools IBM ISS, AppDetective, Core Impact, and MetaSploit.

Finding 2: *Unlocked workstations pose security risks.*
Recommendation 6*: Continue to improve user awareness of the need to lock unattended workstations.*

TTB concurs with Finding 2 and the associated recommendation. TTB has a comprehensive security awareness program, and we will continue to conduct required annual security and privacy training for all employees. We conduct specialized training for supervisors with IT responsibilities, display various security awareness posters in TTB offices monthly, send regular security awareness broadcast emails, and conduct internal social engineering tests to heighten security awareness within the Bureau. We recognize that even the best trained employees can forget to lock their computers. To mitigate the impact of leaving an unlocked computer unattended and accessible, TTB computers are set to automatically lock the desktops after 10 minutes of inactivity. Additionally, we intend to investigate HSPD-12 logical access implementations that could further minimize risks associated with unlocked, unattended workstations.

Finding 3: *Access restrictions were inadequately established for a shared network drive.*
***Recommendation 7**: Ensure that appropriate access restrictions are established for the identified shared network drive.*

TTB concurs with Finding 3 and the associated recommendation. TTB has implemented access controls for all folders and data on the identified common network share.

Appendix 3
Major Contributors

Office of Information Technology Audits

Tram J. Dang, Director
Abdirahman M. Salah, IT Specialist (Lead)
Gerald J. Steere, IT Specialist
Jane Lee, IT Specialist
Larissa Klimpel, IT Specialist
Rafael J. Cumba, Referencer

Appendix 4
Report Distribution

Alcohol and Tobacco Tax and Trade Bureau

Chief Information Officer

Department of the Treasury

Office of Accounting and Internal Control
Office of Strategic Planning and Performance Management
Office of the Chief Information Officer

Office of Management and Budget

Office of Inspector General Budget Examiner