Report in Brief

JUNE 13, 2019

Background

The Department of Commerce and its bureaus are required to follow federal laws to secure information technology (IT) systems through the cost-effective use of managerial, operational and technical controls.

This responsibility applies to all IT systems, including U.S. Patent and Trademark Office (USPTO) systems. The agency heavily relies on IT infrastructure to support its mission–critical systems and applications.

One critical component of USPTO IT infrastructure is Active Directory, which maintains a logical structure, known as a domain, for USPTO to manage all network resources within the domain.

Due to the nature of its role, Active Directory holds sensitive information such as users' credentials and network topologies, making it a prime target for cyberattacks. USPTO must ensure adequate security of its Active Directory to avoid complete compromise of its network.

Why We Did This Review

Our audit objective was to determine whether USPTO has adequately managed its Active Directory to protect mission critical systems and data.

Our review focused on fundamental security practices of Active Directory management and security control implementations of the servers hosting Active Directory.

UNITED STATES PATENT AND TRADEMARK OFFICE

Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk

OIG-19-014-A

WHAT WE FOUND

We found that USPTO (1) inadequately managed its Active Directory, and (2) poorly protected its critical IT assets hosting Active Directory. These deficiencies put the USPTO's ability to accomplish its mission at significant risk. Regarding USPTO inadequately managing its Active Directory, we found that:

1. inadequate configuration of Active Directory allowed excessive access permissions;
2. user credentials were not securely stored in Active Directory;
3. weak passwords were used; and
4. a security best practice was not followed to enforce multi-factor authentication.

Regarding USPTO poorly protecting its critical IT assets hosting Active Directory, we found that:

1. vulnerability scanning practices were inadequate to identify and remediate vulnerabilities;
2. no baseline existed for authorized ports and services; and
3. critical vulnerabilities were not remediated in a timely manner.

USPTO immediately began to take action during our audit to remediate some of the security deficiencies. However, we remain concerned with USPTO's commitment to prioritizing improvement of its security posture. We identified, in finding 2, the same security practice deficiencies that we identified and reported 2 years ago, specifically relating to vulnerability scanning and port management.

WHAT WE RECOMMEND

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office direct the Chief Information Officer to take the following actions:

1. Immediately (1) reevaluate the current Active Directory configuration based on users' roles and responsibilities, (2) reorganize Active Directory user groups based on job functions, and (3) remove any unneeded privileges.
2. Eliminate weak credential encryption to the maximum extent possible. For those applications that currently do not support strong encryption, implement additional compensating controls to protect credentials.
3. Ensure that all passwords meet the standards set by Department and USPTO policies or implement additional compensating controls to protect them. Furthermore, consider incorporating a password policy that emphasizes password length, a primary factor in characterizing password strength recommended by NIST guidelines.
4. Ensure PIV card technology compatibility with on-going and future system development for USPTO next-generation applications, and switch PIV enforcement to a per-user basis, when technically feasible.
5. Finalize the vulnerability-scanning SOP and ensure it includes requirements to verify scanning tools are updated prior to scans and credentialed scanning is performed on physical and virtual machines.
6. Apply the principle of least functionality by developing an authorized open port baseline for system operation, enforce it, and establish an approval procedure for open port requests that deviate from the baseline.
7. Work with USPTO contracting officers to ensure effective government oversight of contractors performing vulnerability assessment scans.
8. Streamline the patch management change-review policies and procedures to allow for timely vulnerability remediation.