Hewlett Packard Enterprise

Business white paper

Gain accountability with government-wide software security control procedures

Software-based cyber-attacks target civilian federal agencies

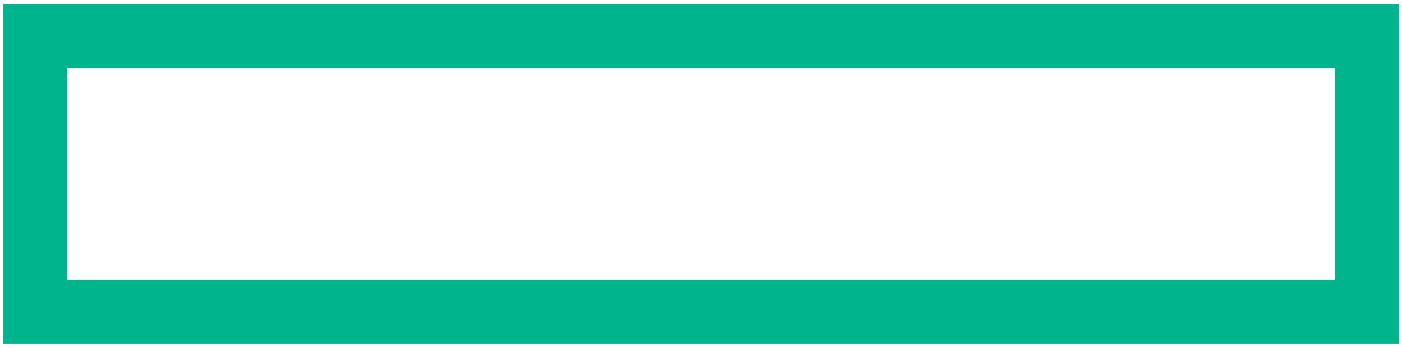

Table of contents

Executive summary

The U.S. civilian government agencies remain highly vulnerable to software-based cyber-attacks, especially when compared to the Department of Defense (DoD) and many private sector firms that employ robust software security and validation procedures. This weakness has resulted in a series of major breaches of federal organizations in 2015 affecting millions of government employees and citizens.[1]

State and non-state intelligence and criminal organizations focus on and exploit weaknesses in software programs to bypass civilian agency network defenses. Federal organizations face three key issues regarding software security: unknown vulnerabilities, software-related breaches, and gaps in software security assurance (SSA).

Known and unknown threats: What you don't know will hurt you
IT vulnerabilities fall into two general categories: known and unknown. Known weaknesses are flaws that information technology (IT) application security experts are aware of. Software-based vulnerabilities fall into this category and are hosted by the U.S. government in the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). These types of issues can be solved or mitigated with continuous diagnostics and mitigation (CDM), patching, and intrusion detection and prevention systems.

Only the attacker knows about the unknown software vulnerabilities, often referred to as "zero-day" attacks. Taking advantage of these software flaws, attackers can circumvent network defenses. Software security analysis, remediation, and application defense technologies are key tools for mitigating zero-day vulnerabilities.

Software-related breaches: Exploiting weaknesses in the system
A significant number of network breaches occur through the software layer. One common method used to breach federal agency networks is via targeted attacks combining both social and technical engineering to access IT systems. After access is gained, attackers carefully scout the network for data and systems to steal or control. Once systems are controlled, attackers then begin to steal and damage the data.

Another type of attack is the "front door" variety conducted with techniques such as SQL injection or cross-site scripting. These attacks are used to bypass access controls and pull data from poorly designed websites with database back ends. Such vulnerabilities are easily detected and repaired, but they continue to remain the top weaknesses of civilian agencies.

[1] Hacking of Government Computers Exposed 21.5 Million People, Julie Hirschfeld Davis, The New York Times, July 2015 **nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0**

Gaps in software security assurance: A backdoor for attackers
Civilian agency IT defenses are weakest at the software layer. SSA programs offer the fastest time to value for IT security investments. Software security improvements can be implemented more quickly via IT development and operations than other types of IT infrastructure defense. But this is not happening in the civilian government due to tight budgets and a focus on perimeter defense.

Programs such as the Department of Homeland Security's (DHS) CDM and EINSTEIN focus on traditional IT security management and perimeter defense. Both application security programs do not adequately address unknown or zero-day software vulnerabilities.

A call to action
This paper recommends that civilian government agencies adopt robust software security and validation controls based on DoD efforts such as the Defense Information Systems Agency's Security Technical Implementation Guide (DISA STIG).

In addition, to avoid a patchwork approach to adoption, it is suggested that a government-wide mandate is necessary to bring all agencies into compliance. Such a mandate would be overseen by the DHS and would build on requirements contained in NIST's 800-53 Revision 4—"Security and Privacy Controls for Federal Information Systems and Organizations." The statutory mandate should be based on commercial best practices and modeled on the SSA policies currently being implemented throughout the DoD.

Introduction: Civilian agencies remain vulnerable

The U.S. civilian government's software security policies, practices, and application security testing capabilities lag significantly behind the DoD and private sector. This paper suggests that without a statutory mandate federal agencies will remain highly vulnerable to software-based cyber-attacks.

The case for standardized IT security practices is well established in the federal government. Efforts such as the DHS's CDM and EINSTEIN programs, and recent revisions to NIST's 800-53 special publication on security and privacy controls indicate a continuing need for strong, broadly applied software security standards, and application security testing capabilities. However, these measures focus on traditional perimeter domains of network defense and configuration management. They have not kept pace with the sophistication and rapacity of the nation's cyber adversaries who are focusing their attacks on government network software.

Legislative efforts such as Government Information Security Reform Act and the Federal Information Security Management Act address the need for civilian agencies to include security in their IT planning and practices. However, this legislation does not call for a unified set of SSA practices across all ".gov" organizations. The civilian government will benefit from statutory mandates requiring a disciplined approach to SSA for effective response to current cybersecurity threats. Only the DoD has issued the technical guidance and policies[2] needed to secure its mission-critical systems from software-based vulnerabilities.

Recent, large-scale cyber-attacks on the U.S. federal government[3] have been carried out through software-based vulnerabilities. Although the DHS recognizes the need for safer software, its major security initiatives such as CDM and EINSTEIN mainly focus on network and perimeter defense, and only address a small segment of civilian government's SSA requirements.

It is recommended that the DHS oversee the implementation of a software security mandate for all federal agencies operating in the ".gov" domain. Building on the requirements contained in NIST 800-53 Revision 4, this statutory mandate should be based on commercial best practices and modeled on the SSA policies currently being implemented throughout the DoD.

[2] The DISA first drafted the Application Security and Development STIG in 2006. The current version is now used throughout the DoD and U.S. Intelligence Community. It requires automated source code analysis and deployed testing when applicable

[3] The Year of the Breach: 10 Federal Agency Data Breaches in 2014, Jack Moore and Nextgov Staff, Nextgov, December 2014 **nextgov.com/cybersecurity/2014/12/year-breach-10-federal-agency-data-breaches-2014/102066/**

Known and unknown vulnerabilities: What you don't know will hurt you

IT security vulnerabilities fall into two general categories, known and unknown. In the case of known weaknesses, the IT security community is aware of the vulnerability. For civilian agencies, these vulnerabilities can be removed or mitigated through a combination of strong configuration management controls such as the DHS CDM program and intrusion detection and prevention systems such as EINSTEIN.

Unknown weaknesses, often referred to as "zero-day" issues, are undiscovered coding errors. These vulnerabilities are mainly found in the software layer, either by system owners scanning their software for vulnerabilities, or by adversaries scouting for back doors into an organization's networks. However, efforts by agency application security do not focus on the software layer. Spending for network and server defense is 23 times more than spending on software security, although more than 80 percent of current breaches come through the software layer.[4]

The MITRE Corporation maintains two different taxonomies tracking software and IT security issues—Common Weaknesses Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE). The CWE is a list of software security weaknesses that can potentially result in vulnerabilities while the CVE is a dictionary of publically known vulnerabilities specific to combinations of known hardware, software, and configuration management. In 1999, the initial draft of CVE contained 663 vulnerabilities.[5] It has since grown to more than 71,000 entries, with more than 600 entries in January 2016 alone.[6]

Relying on the CVE and the NVD alone is inadequate as they only reflect publically known application security weaknesses in common, widely used software packages. The NVD does not list vulnerabilities in government-created software, and weaknesses in open source or commercial software are not always discovered in a timely manner or announced to end-user organizations. While commercial software is typically found on every government desktop, the actual business of government is performed on custom applications uniquely created for the missions of each agency or department. Software breaches constantly occur despite the wide awareness and active management of the CVE dictionary, highlighting the need for additional software analysis for new security flaws.

[4] Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves, Joesph Feiman, Gartner, Inc. (Research Note G00269825), September 2014

[5] Common Vulnerabilities and Exposures (PowerPoint slides retrieved from **cve.mitre.org/docs/docs-1999/CVE-Press-09-29-99.ppt** in January 2016.), The MITRE Corporation, September 1999

[6] Browse vulnerabilities by date, CVE Details, January 2016 **cvedetails.com/browse-by-date.php** retrieved

Software-related breaches: Exploiting weaknesses in the system

Federal governments' IT systems are the target of persistent attacks by criminal and state actors seeking to either disrupt operations or extract sensitive data.

One way networks are breached is through targeted attacks that blend social and technical engineering to gain access to IT systems. This may include the insertion of malware into a network to maintain access. A breach is often followed by reconnaissance of an organization's networks, systems, and data. This is followed by hidden control of those systems and the exfiltration of data.

Another form of attack is via the "front door," and involves techniques such as SQL injection and cross-site scripting to access and pull data directly from poorly designed websites with database back ends. Although these types of vulnerabilities are easily detected and fixed in software applications, they continue to remain the most common software vulnerability.[7]

In a detailed post-incident analysis of the Heartland Payment Systems breach, considered one of the largest known financial breaches, Federal Reserve Board analyst Julia Cheney wrote, "the method used to compromise Heartland's network was ultimately determined to be SQL injection. Code written eight years ago for a Web form allowed access to Heartland's corporate network. This code had a vulnerability that was not identified through annual internal and external audits of Heartland's systems or through continuous internal system monitoring procedures, and provided a means to extend the compromise from the corporate network to the separate payment processing network. Although the vulnerability existed for several years, SQL injection didn't occur until late 2007."[8] In this case, the breach was conducted as a front-door attack.

In recent years, the number of breaches of federal IT systems has increased dramatically, with major incidents occurring at agencies such as the Department of Interior,[9] the Department of Energy,[10] and the Office of Personnel Management. Many agencies have also been serially re-breached. The use of known, published vulnerability lists alone cannot adequately provide for the security of public sector agencies. It is time federal agencies proactively assess their own software for vulnerabilities, either via mandate or via technical requirements.

[7] "OWASP Top 10—2013; The 10 Most Critical Web Application Security Risks," The Open Web Application Security Project, 2013

[8] "Heartland Payment Systems: Lessons Learned from a Data Breach," Julia Cheney, January 2010

[9] "Interior Networks hacked 19 times by foreign attackers," Federal Times, November 2015 **federaltimes.com/story/government/cybersecurity/2015/11/25/interior-19-hacks/76378710/**

[10] "Attackers Hacked Department of Energy 159 times in 4 years," Computer World, September 2015 **computerworld.com/article/2983749/cybercrime-hacking/attackers-hacked-department-of-energy-159-times-in-4-years.html**

Gaps in software security assurance: A backdoor for attackers

More than 80 percent of current IT security spending is on perimeter defense, protecting the network and access to it. In the past, penetrating IT infrastructure was technically simple and primarily a brute force operation to access unprotected endpoints.[11] Intrusion detection and prevention systems have blocked this route to network access. However, attacks now target the software layer, carefully interweaving social engineering with exploits of software vulnerabilities to gain access to IT resources and data.

An SSA program offers the fastest time to value for IT security investments. Software security improvements can be implemented faster through IT development and operations than other types of IT infrastructure protection. But this is not occurring in the civilian government due to funding constraints and due to the misprioritization of available funds on network controls and configuration management. Today, the government spends a majority of application security dollars in the operation stage, which, according to the NIST is 30 times more expensive than designing security in from the beginning.[12]

DHS's CDM program is an example of this unbalanced spending as it focuses on traditional IT and IT security management. Although it will increase the baseline security posture of agency IT infrastructures, it will have little impact on the ability to find and remove unknown and zero-day software vulnerabilities. Likewise, DHS's EINSTEIN program supports network defense and monitoring for civilian agencies but focuses on traditional perimeter enforcement. EINSTEIN does not adequately address the risk of unknown software vulnerabilities. This paper recommends that agency security spending focus on mitigating software-based threats.

Another issue is how software is sourced. Contemporary software is often sourced in different ways, including custom development through systems integrators, software from commercial software vendors, and free open source software (FOSS). While meeting agency software needs through sourcing allows increased agility to meet mission needs, it complicates the enforcement of uniform software security standards and procedures. Although the risks of open source software have long been understood, the risks of non-validated commercial software and firmware are just becoming apparent. Additionally, all sources are commonly combined to meet specific application needs. Assessing one for software vulnerabilities without determining the other continues to expose an organization's systems to software vulnerabilities. All sources of software—custom, commercial, and FOSS—must be included in any SSA program.

It is suggested that policies be initiated mandating the use of multiple automated security testing tools, where appropriate, to ensure weaknesses in the software running the business of government are found and eradicated. This is the approach taken by the DoD through DISA STIG. It provides an off-the-shelf set of software security compliance controls and mandates the type of testing necessary to validate these controls. If a new policy is not a preferred approach, then the DISA STIG for software should be considered for implementation across all federal civilian agencies as an adjunct to FISMA 800-53.

[11] This was the era of large-scale credit card fraud, facilitated through organized criminal markets for stolen card numbers and personal information, and by emerging e-marketplaces used to unload fraudulently acquired goods. During this time, the FBI's Cyber Division emerged and disrupted these criminal enterprises, apprehending many of the criminals operating them, both domestic and foreign

[12] **sans.org/reading-room/whitepapers/analyst/application-security-tools-management-support-funding-34985**

Call to action

To avoid adopting security policies in a patchwork fashion, this paper recommends that a government-wide mandate is necessary to bring all agencies into compliance. Such a mandate would be overseen by the DHS and would build on requirements contained in NIST's 800-53 Revision 4—"Security and Privacy Controls for Federal Information Systems and Organizations." The statutory mandate should be based on commercial best practices and modeled on the SSA policies currently being implemented throughout the DoD.

Learn more at
hpe.com/software/fortify

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

© Copyright 2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

4AA6-5610ENN, May 2016