(Lack of) **Patch Management** Highlighted in US Congress

▸ by Kevin L. Jackson

According to the former Equifax CEO's testimony to Congress, one of the primary causes of this now infamous data breach was the company's failure to patch a critical vulnerability in the open source Apache Struts Web application framework. Equifax also waited a week to scan its network for apps that remained vulnerable.[1] Would you like to appear at the next Congressional hearing on patch management?

Patch management is the process of identifying, acquiring, installing, and verifying patches for products and systems. Patches not only correct security and functionality problems in software and firmware, but they also introduce new, and sometimes mandatory, capabilities into the organization's IT environment. It is so useful, the CERT® Coordination Center (CERT®/CC) claims that **95 percent of all network intrusions are avoidable** by using proper patch management to keep systems up-to-date.

This nightmare true story and compelling endorsement from CERT®/CC, however, masks the ugly operational patch management implementation complexities. Key enterprise challenges include:

- **Timing, prioritization, and testing of patches** often present conflicting requirements. Competitive prioritization of IT resources, business imperative, and budget limitations often leave patching tasks on the back burner
- **Technical mechanisms and requirements** for applying patches may also conflict and may include:
  - **Software that updates itself** with little or no enterprise input
  - **Use of a centralized management tool**
  - **Third-party patch management applications**
  - **Negative or unknown interactions** with network access control, health check functions, and other similar technologies
  - **User-nitiated manual software updates**
  - **User-initiated patches or version upgrades**
- **Typical enterprise heterogeneous environment** that includes:
  - **Unmanaged or user managed hosts**
  - **Non-standard IT components** that require vendor patching or cannot be patched
  - **Enterprise-owned** assets that typically operate on non-enterprise networks
  - **Smartphones, tablets,** and other mobile devices
  - **Patching** of rehydrating virtual machines
  - **Firmware updates**

Piling up on these purely operational tasks are the change management steps associated with:

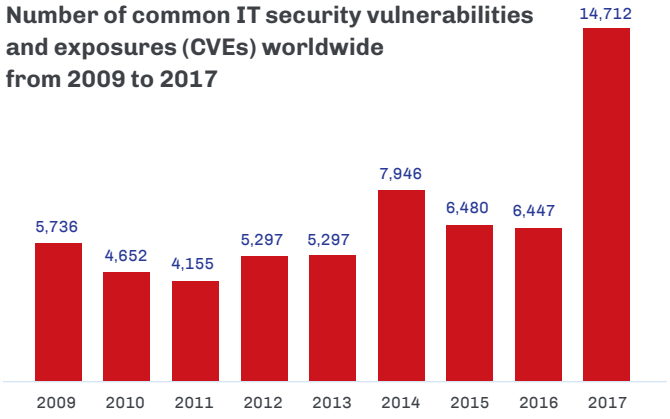
- **Maintaining current knowledge** of available patches
- **Deciding what patches** are appropriate for particular systems

bmc IDG

- **Ensuring proper installation** of patches
- **Testing systems** after installation
- **Documenting all procedures** and any specific configurations

This challenge can also be significantly exacerbated in an IT environment that blends legacy, outsourced and cloud service provider resources. Environment heterogeneity and the sheer volume of patches released is why any patching strategy that primarily relies solely on manual implementation is untenable.

Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2017



Sources: Forrester Research; cvedetails.com © Statista 2018

According to the SANS Institute, meeting the patch management challenge requires the creation of a patch management methodology and the automation of that methodology.[2] The methodology itself should include:

- **A detailed inventory** of all hardware, operating systems, and applications that exist in the network and the creation of the process to keep the inventory up-to-date
- **A process to identify vulnerabilities** in hardware, operating systems, and applications
- **Risk assessment** and buy-in from management and business owners
- **A detailed procedure for testing patches** before deployment
- **A detailed process for deploying patches** and service packs, as well as a process for verification of deployment

As for the automation component, it should deliver an automated, comprehensive server lifecycle approach that can provision and configure software, update patches and

Former Equifax Chair and CEO Richard Smith testified before the Senate Banking Committee

implement configurations that can improve security and compliance across physical, virtual and cloud servers.

It should also encompass a policy-based approach with support for all major operating systems on physical servers and leading virtualization and cloud platforms. An ability to automate continuous compliance checks and remediate any security or regulatory shortcoming is also paramount. If appropriately implemented, IT Staff should be able to manage patching via a web interface. Having this feature increases server to admin ratio, enhances operational productivity, accelerates audit timelines and reduces incident response latency.

A leading solution in this space is **BladeLogicServer Automation by BMC**. It was specifically designed to address the dual enterprise requirements of (1) ensuring compliance with rules and regulations and (2) software patching to reduce security vulnerabilities. In the market for over 10 years, it is a comprehensive server lifecycle automation solution that helps organizations provision and configure software, update patches and configurations to improve security and compliance across physical, virtual and cloud servers. Advanced capabilities include script automation, compliance tracking and the ability to stage and test patches before committing them. The latter feature is used to copy patch bundles to the targeted servers before maintenance windows open.The full-function suite integrates with change management systems to facilitate change record creation. Vulnerability management and remediation are automated by importing vulnerability management scan data from vendors like Qualys, Tenable and Rapid 7, and mapping the vulnerabilities back to underlying patches in BladeLogic.

Secure IT operations start with the identification and prioritization of critical vulnerabilities paired with the capability to deliver multi-tier remediation. These reinforcing goals are why an advance patch automation solution is a "must-have" for today's modern enterprise.

Kevin Jackson is Founder & CEO of GovCloud Network, a consultancy specializing in information technology solutions that meet critical government operational requirements. Follow him on Twitter @Kevin_Jackson

1 https://arstechnica.com/information-technology/2017/10/a-series-of-delays-and-major-errors-led-to-massive-equifax-breach/

2 https://www.sans.org/reading-room/whitepapers/sysadmin/meeting-challenges-automated-patch-management-1468