SECURITYWEEK NETWORK: Information Security News | Newsletters | Cybercrime News Security Experts: WRITE FOR US

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Free Subscription | White Papers | Webcasts | Events | Contact Us

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Infrastructure Management & Strategy

Trends & Data Black Hat

Home › Compliance

A Compliance with a Complex Problem

By Terry Cutler on Feb 16, 2011

Like Buzz Tweet 15 0 Digg Share 6 RSS

In an interview earlier this year, Kristin Lovejoy, Vice President of Security Strategy at IBM, **addressed** growing security concerns across the North American business landscape. Lovejoy focused on global security threats facing organizations, unique challenges of managing security across IBM, and how security leaders can improve in 2011 and beyond.

"This is potentially the most dramatic trend," Lovejoy told **BankInfosecurity**. "There is a lot of complexity out there, and if you ask a customer what their biggest problem is, it isn't compliance, it's complexity."

Lovejoy goes on to say that while the global compliance landscape creates unique challenges for organizations across the industry, the greater issue is prioritizing the response to these mandates.

In other words, compliance!

Lovejoy, who is responsible for the overall security portfolio market direction and strategy at IBM, among other positions, says that with new regulations upping the ante on new compliance, the problem will be more complex -- customers may be asking what to do, when to do it, and how...

In the end, what are the benefits?

That's a good question, one that has been asked since June 30, 2007-- the deadline for companies to show that they were in compliance with the Payment Card Industry Data Security Standards, or PCI-DSS. According to Chris Farrow, Board Member at PCI Security Vendor Alliance, the Payment Card Industry required all organizations that store, process or transmit credit card payments to demonstrate compliance with PCI-DSS by that date.

In a 2008 bankinfosecurity.com article, Farrow states, “There has been much more positive awareness by banks and merchants. There's been much more media coverage on this issue, and all of it adds up to PCI-DSS being a higher priority focus for these institutions and merchants. That in turn is helping to improve the state of information security.”

Security through moving parts

Compliance doesn’t mean you’re secure; it’s a baseline to say that you’ve done an average job at securing the corporation, Certainly, tighter security requires several moving parts including patch management, end-point security, identity management and security information and event management (SIEM).

To keep up with fixing, automated patch management systems should be in place, sided with a similar lab environment so that patches can be tested properly and rolled out for production in a short period of time.

An appropriate lab is not always up and running. Hired by a software vendor, where I spent ten years, my clients averaged 50-600 servers with 200-25,000 users, at any time, of which two had a proper lab set up for testing.

Google™ Custom Search Search

SUBSCRIBE TO SECURITYWEEK

Enter Your Email Address Subscribe

Most Read Most Recent

- Survey Reveals How Stupid People are With Their Passwords
- New Tool Reveals Internet Passwords
- Hacker Uses XSS and Google Street View Data to Determine Physical Location
- Snoop Dogg Joins the War on Cybercrime
- Study Reveals 75 Percent of Individuals Use Same Password for Social Networking and Email
- The Rise of the Small Botnet
- An Inside Look at Hacker Business Models
- IT Salary Guide Shows Increase in Salaries for IT Security Professionals
- Nevercookie Eats Evercookie With New Firefox Plugin
- Defense Department’s Cyberwar Credibility Gap

Testing is not something to be overlooked. As we all know, a new patch would most likely break something else. The problem lies in the interim. For example, security groups expect a patch on the system to help mitigate a system compromise, but the IT staff may have to wait weeks to test it because they don’t have a proper lab set up.

This has the potential to create company in-fighting

Most corporations have IT staff who are overworked and underpaid. If something is left unchecked and running wild, they are handed the task of security. In most cases, these people lack the proper training.

Security on the “go”

Mobile is becoming critical. It isn’t easy to control how corporate smartphones are used. What applications are being installed and operated by end-users adds, or in these cases depletes, what security is available.

Those driving the enterprise IT strategy should have legitimate concerns about how to handle inventory, protect and comply with any corporate policies, and fulfil privacy and confidentiality requirements. Regardless of whether the employer or the employee owns the devices, their permanent position within the enterprise landscape means that they require comprehensive security protection, just like any other device in the network.

Heal thy self

Moving towards a self-healing infrastructure is key.

In a created scenario, a user logs in from any location, the system validates this user by a two or three-way factor authentication through SIEM-monitored identity management. Elsewhere in the system, the inventory and asset management processes are checking all servers, workstations and mobile devices for their patch and virus definition levels.

Once a discrepancy is found, the corporate patch management service automatically deploys the patch. Should the endpoint be infected or the user is disgruntled, then the Network access control; intrusion detection; SIEM with user activity monitoring configured; and other monitoring devices are policing the network for malicious signatures that would then shutdown access. Once this event occurs, the Log manager can then log a ticket and advise the IT staff in real time of what’s going on.

Indeed, Lovejoy’s future outlook is vital. While she recommends we look to 2011, companies need to see where they are now, where they need to be and from there, where they should be. In a fast changing world, where technology and new systems spin in and spin out, it seems, on a weekly basis, the look ahead may be 2012.

This will require being “on the job” 24 hours a day, seven days a week. In the end, it will take more than a checklist to lock down the environment.

Like Buzz Tweet 15 0 Digg Share 6 RSS

Terry Cutler is a co-founder of Digital Locksmiths, Inc., an IT security and data defense firm based in Montreal and serves as the company's Chief Security Evangelist and Certified Ethical Hacker. Prior to joining Digital Locksmiths, he was a Premium Support Engineer for Novell in Canada where he analyzed network vulnerabilities and transitioned security technologies into production. In addition to being a licensed private investigator in Canada, Terry is an internationally known author, trainer, speaker, and security consultant, Terry has appeared in numerous national television and radio programs and is very active on the conference circuit. Follow Terry on Twitter at @TerryPCutler

Previous Columns by Terry Cutler:

- A Compliance with a Complex Problem
- Beating Back the Botnets
- Enterprise Security Priorities for 2011
- Mobile Security: It's Time to Get Serious
- The Anatomy of an Advanced Persistent Threat

Software Trial

- Security Focus on Consumer Electronics w/ BONUS Free Software Trial
- Mobile & Smart Device Security Survey 2010 - Concern Grows as Vulnerable Devices Proliferate
- 2010 Device Integrity Report: U.S. Unprepared for Internet Device Flood

Tags: INDUSTRY INSIGHTS Compliance

Like 1 person liked this. DISQUS

Showing 0 comments

Sort by Best rating Subscribe by email Subscribe by RSS

Add New Comment

Type your comment here.

Post as ...

Trackback URL http://disqus.com/forums/securityweek/a_com

Popular Topics

- Information Security News
- IT Security News
- Risk Management
- Compliance
- Cloud Security
- Application Security

Security Community

- IT Security Newsletters
- Events
- Comments
- Most Read

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Stuxnet Group on LinkedIn
- RSS Feed
- Submit Tip

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us

Wired Business Media