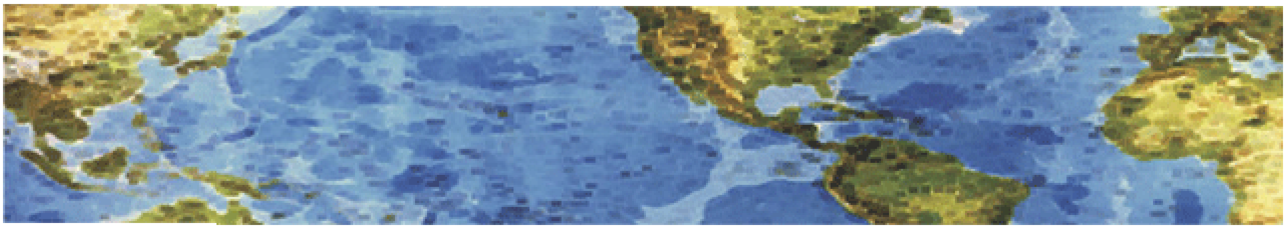
HALL ASSOCIATES



Risk-Based Decision Making Commentary
1 June 2014 Newsletter

Preparing for and Responding to the Next Heartbleed

Was your organization or website or network affected by the recent Heartbleed security bug? I hope that you at least asked your IT organization or company. Open source vulnerabilities on the scale of Heartbleed would seem a rare occurrence, yet over 5000 vulnerabilities are reported against open source components each year. While public resources exist to track these vulnerabilities, mapping them to the open source in use within your organization depends on you knowing what components you are using and where they are being used. Do you ever ask that question of your IT folks? **You** should be asking at least the following questions for due diligence:

1. Does your IT organization or company have a listing of what components/applications/programs you are using on ALL of your equipment? Note that this should include any privately owned equipment (phones, laptops, etc.) connected to your network.
2. Does your IT organization or company do periodic sweeps to ensure nothing has been put on ANY of your equipment without their knowing it?
3. Do you have policies in place and followed about attaching privately owned equipment (phones, home computers, etc.) to your network?
4. Does your IT organization or company periodically determine what vulnerabilities are known/developed and that ALL of your components/applications/programs (especially privately owned equipment) are successfully updated as required? In other words does **NOT** depend simply on developer updates but checks on their own.
5. Does your network or connected private equipment still use the Microsoft XP operating system in any equipment? Having a vulnerability in a home computer attached to your network is the same as having a vulnerability in your computers.

If you don’t get adequate answers to these questions I recommend an audit be conducted by an outside agent to protect your systems/equipment/data and allow you to understand what vulnerabilities you have.

Many organizations reacted very quickly to address the Heartbleed bug in their environments, says Satnam Narang, researcher at Symantec Security Response. "[Still], we have seen reports stating that out of 500,000 vulnerable sites, [only] 375,000 have been patched," he adds. The Heartbleed bug is still a significant issue, says David Rockvam of Entrust, a digital certificate provider. He cites a report from Internet research firm Netcraft that identified remaining gaps. "Although many secure websites reacted promptly to the Heartbleed bug by **patching OpenSSL, replacing their SSL certificates and revoking the old certificates,** some have made the critical mistake of reusing the potentially compromised private key in the new certificate," according to the Netcraft report.

"Since the Heartbleed bug was announced on April 7, more than 30,000 affected certificates have been revoked and reissued without changing the private key," Netcraft says. According to the research firm, **only 14 percent of affected websites completed all three necessary steps** after patching the Heartbleed bug: replacing the SSL certificates, revoking the old ones and making sure to use a different private key**. (Did your IT organization or company accomplish all three steps? Did you ask?)**

Another concern is that a new vulnerability like Heartbleed could emerge, says Christopher Paidhrin, security administration manager at PeaceHealth, a healthcare provider in the Pacific Northwest. "The pace of code development and feature enhancement is stressing the security testing and code validation processes," he says. "The complexity of core Web services is daunting. The frequency of announced exploits is a measure of how big a challenge we face." Organizations need to thoroughly test their critical infrastructure for bugs similar to Heartbleed. If they don't do that, it's just a matter of time before something else is found and exploited and they may suffer**. (With the automated search capability and extensive data mining being carried out by cybercriminals, no one is safe because they are "part of a big herd" and obscure. And small/very small businesses and individuals are increasingly targeted because they are easy to hack.)**

Meanwhile, Christopher Glyer, technical director at Mandiant, a cybersecurity firm, says the vast majority of his company's clients have patched most of their Internet-facing and internal systems. **"The larger risk going forward would be on devices that are more difficult to patch or require a consumer to take an action,"** he says. And the National Association of Federal Credit Unions, which educated its members about the vulnerability, has "heard very little impact from our members other than they were working with their IT divisions to work through the fixes," says Anthony Demangone, executive vice president and chief operating officer.

Mitigation Recommendations

A key step in mitigating any cyberrisk is to conduct a basic risk analysis of all your operating systems and applications/programs. Check to see if the Heartbleed vulnerability (or any other known vulnerability) is still found throughout your IT systems and your vendors/privately owned equipment connected to your network and then close the loop as quickly as possible. Basically that is classic risk management and should always be periodically accomplished. Prioritize patching devices that would allow remote access into the organization. Reach out to your vendors to determine if their software is vulnerable, and run vulnerability scanners on internal and Internet-facing systems to help identify what still needs to be fixed. **But the single most important mitigation step now for Heartbleed is revoke, reissue and re-install certificates.** Also upgrade systems to a software version that uses OpenSSL 1.0.1g or higher; renew SSL certificates with a new private key; ask users to change their passwords; and notify users if content may have been compromised. Bottom line for this vulnerability is that if you operate or use a website connected to your network then you need complete an exposure assessment and validate that remediations (if needed) were exhaustive.

http://www.govinfosecurity.com/heartbleed-bug-what-risks-remain-a-6872?rf=2014-05-28-eg&utm_source=SilverpopMailing&utm_medium=email&utm_campaign=enews-gis-20140528%20%281%29&utm_content=&spMailingID=6598461&spUserID=NTQ5MzMzMDA3ODES1&spJobID=442863040&spReportId=NDQyODYzMDQwS0