White House Cyber Czar Walks a Thin Line on Cybersecurity Info Sharing

Posted At : May 7, 2014 2:10 PM | Posted By : John Slye

Related Categories: Critical Infrastructure Protection, President, Open Government, Cybersecurity, Transparency, Policy & Legislation

If the federal government knew about the Heartbleed security bug before it became public, would they have said anything? The answer, according to Michael Daniel, the White House Cybersecurity Coordinator, is an unequivocal . . . "maybe."

In a recent **White House Blog post**, Daniel reiterated the NSA assertion that they had no prior knowledge of the existence of Heartbleed, the recently discovered vulnerability in OpenSSL that could expose online passwords and encrypted Internet traffic to hackers. Daniel used the occasion to wade into the murky waters of when the federal government would, and would not, withhold knowledge of a computer vulnerability from the public. He affirmed the administration's "commitment to an open and interoperable, secure and reliable Internet, and in the majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest."

But he also noted that a major reason they would delay disclosure is if the opportunity for critical intelligence gathering was deemed to outweigh the cost of the delay. At odds are the extremes of saying nothing and maintaining and exploiting a collection of undisclosed vulnerabilities while leaving users vulnerable . . . and saying everything and completely forgoing this knowledge as a way to conduct intelligence gathering.

In an effort to balance the trade-offs between transparency and secrecy with a strong leaning toward disclosure, Daniel outlined a list of question he wants agency officials to address whenever they are proposing to withhold their knowledge of vulnerability:

- How much is the vulnerable system used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
- Does the vulnerability, if left unpatched, impose significant risk?
- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- How likely is it that we would know if someone else was exploiting it?
- How badly do we need the intelligence we think we can get from exploiting the vulnerability?
- Are there other ways we can get it?
- Could we utilize the vulnerability for a short period of time before we disclose it?
- How likely is it that someone else will discover the vulnerability?
- Can the vulnerability be patched or otherwise mitigated?

The impact of the answers to these questions on the share/don't share decision is unclear, since by his own admission "there are no hard and fast rules."

In a previous blog post that ran about the same time that Heartbleed was coming to light, Daniel emphasized the **importance of information sharing** to improve the nation's overall cybersecurity posture. In that blog he said "reducing barriers to information sharing is a key element of this Administration's strategy to improve the nation's cybersecurity," and that they would "continue to work to address the concerns our private sector partners have raised that the government should share more of its own information, so that companies could better protect themselves." "Our goal is for the government to be a reliable information sharing partner, but only one of many."

In an era where government transparency and secrecy issues have become high-profile in the public mind, the above guidelines show the tightrope the White House is attempting to walk.

---

*Originally published in the **GovWin FIA** Analysts Perspectives Blog. Follow me on Twitter **@GovWinSlye**.*