Heartbleed: Understanding When We Disclose Cyber Vulnerabilities

APRIL 28, 2014 AT 3:00 PM ET BY MICHAEL DANIEL

Summary: For an agency whose acronym was once said to stand for "No Such Agency," speaking out about Heartbleed was unusual but consistent with NSA's efforts to appropriately inform the ongoing discussion related to how it conducts its missions.

When President Truman created the National Security Agency in 1952, its very existence was not publicly disclosed. Earlier this month, the NSA sent out a Tweet making clear that it did not know about the recently discovered vulnerability in OpenSSL known as Heartbleed. For an agency whose acronym was once said to stand for "No Such Agency," this step was unusual but consistent with NSA's efforts to appropriately inform the ongoing discussion related to how it conducts its missions.

While we had no prior knowledge of the existence of Heartbleed, this case has re-ignited debate about whether the federal government should ever withhold knowledge of a computer vulnerability from the public. As with so many national security issues, the answer may seem clear to some, but the reality is much more complicated. One thing is clear: This administration takes seriously its 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. This has been and continues to be the case.

This spring, we re-invigorated our efforts to implement existing policy with respect to disclosing vulnerabilities – so that everyone can have confidence in the integrity of the process we use to make these decisions. We rely on the Internet and connected systems for much of our daily lives. Our economy would not function without them. Our ability to project power abroad would be

crippled if we could not depend on them. For these reasons, disclosing vulnerabilities usually makes sense. We need these systems to be secure as much as, if not more so, than everyone else.

But there are legitimate pros and cons to the decision to disclose, and the trade-offs between prompt disclosure and withholding knowledge of some vulnerabilities for a limited time can have significant consequences. Disclosing a vulnerability can mean that we forego an opportunity to collect crucial intelligence that could thwart a terrorist attack stop the theft of our nation's intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks.

Building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest. But that is not the same as arguing that we should completely forgo this tool as a way to conduct intelligence collection, and better protect our country in the long-run. Weighing these tradeoffs is not easy, and so we have established principles to guide agency decision-making in this area.

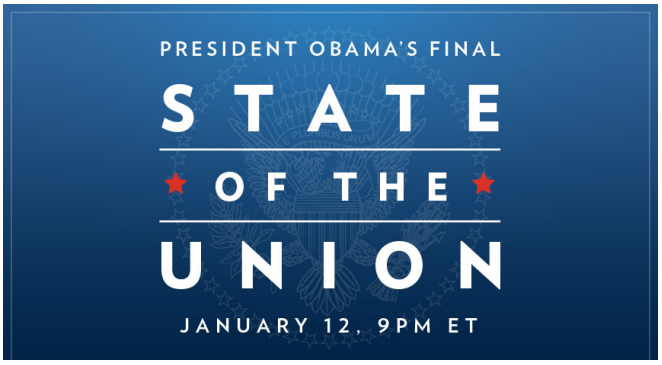
We have also established a disciplined, rigorous and high-level decision-making process for vulnerability disclosure. This interagency process helps ensure that all of the pros and cons are properly considered and weighed. While there are no hard and fast rules, here are a few things I want to know when an agency proposes temporarily withholding knowledge of a 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?

Enabling transparency about the intersection between cybersecurity and

intelligence and providing the public with enough information is complicated. Too little transparency and citizens can lose faith in their government and institutions, while exposing too much can make it impossible to collect the intelligence we need to protect the nation. We weigh these considerations through a deliberate process that is biased toward responsibly disclosing the vulnerability, and by sharing this list we want everyone to understand what is at stake. I hope this post will instill some confidence that your government is acting responsibly in the handling of this important issue.

Michael Daniel
Special Assistant to the President and Cybersecurity Coordinator



THE FINAL STATE OF THE UNION

Watch President Obama's final State of the Union address.

EXPLORE PAST ADDRESSES

Check out past State of the Union speeches now annotated on Genius.

CLEAN POWER PLAN

Learn more about the biggest step we've ever taken to combat climate change.