What's Up With Einstein?

by Greg Nojeim [1]
July 28, 2009

Last week, the Senate Intelligence Committee reported a bill that would require the government to disclose information about the intrusion detection system for government computers that has been dubbed, "Einstein." Section 340 of the Intelligence Committee's Intelligence Authorization Act for FY 2010 [2] (S. 1494) would require the government to report to Congress about privacy impact of Einstein, the legal authority supporting it, and about any audits that have been conducted on its operations. The bill, and recent press accounts, prompt CDT to ask the Administration to reveal more about Einstein.

There's no doubt that the government needs better cybersecurity immediately. Malicious code has been found in the computers that run the electric power grid, and terabytes of data about the Pentagon's $300 billion F-35 Joint Strike Fighter jet were recently stolen by computer spies.

Einstein is designed to partially meet this need for civilian government computer networks. It operates to detect malicious code in communications with the government. The latest iteration - Einstein 3 - reportedly can scan the content of such communications and, using technology based on a National Security Agency system called "Tutelage," can intercept the malicious computer code before it even reaches the government system.

But the Einstein intrusion detection system raises a whole host of questions: what is the scope of the NSA's role? What is done with the intrusion reports Einstein generates and shares with law enforcement and intelligence agencies? How are people notified that their communications with government officials, and their surfing of government websites, are being monitored for threatening code? CDT poses these and other questions about Einstein in a new report released today. [3]

The Department of Homeland Security did a Privacy Impact Assessment on the first two versions of the Einstein intrusion detection systems, and they reveal a lot of information. But, critical pieces to the puzzle are still missing, and a new version of the system that ups the privacy stakes is being developed.

Secrecy can undermine the effectiveness of a cybersecurity program, particularly one that relies, as Einstein 3 does, on the cooperation of private sector communications service providers. It's time for the Obama Administration to chart a new course by being more open about Einstein.

- surveillance
- tbp
-
- senate
- privacy
- cybersecurity
- einstein
- communications

Source URL: https://cdt.org/blogs/greg-nojeim/whats-einstein

Links:

[1] https://cdt.org/personnel/greg-nojeim
[2] https://cdt.org/intelligence.senate.gov/090722/s1494.pdf
[3] http://www.cdt.org/security/20090728_einstein_rpt.pdf