Will It Take a Real Zombie Attack to Improve Federal Cybersecurity?

Posted At : February 18, 2014 3:13 PM | Posted By : John Slye

Related Categories: Critical Infrastructure Protection, Department of Homeland Security, Homeland Security, Information Security, Congress, Department of Energy, Cybersecurity, Treasury, Policy & Legislation, Government Reform

It's been said that 80% of cyber-attacks could be prevented by implementing and maintaining the most basic cyber-measures like keeping software patched and using non-default passwords. Well, a recently released Senate study documents the dismal track record many federal agencies have at doing just that. The ramifications range from the now-infamous zombie attack warning that went out over a hacked emergency notification system to incidents of personally identifiable information (PII) theft.

As the White House releases updated critical infrastructure protection (CIP) guidance and Congress is **debating** its latest cybersecurity and CIP bill, the Republican Ranking Member of the Senate Homeland Security and Governmental Affairs Committee, Tom Coburn, **released** a report detailing how federal agencies are poorly prepared to defend against some of the even most routine attacks.

The Federal Government's Track Record on Cybersecurity and Critical Infrastructure was picked up by the **Washington Post**, which highlighted the February 2013 hack of the FCC's Emergency Broadcast System that led to several TV stations broadcasting the zombie attack warning. The report cites previous work by the GAO and by agency IGs to emphasize the breath and severity of the problem of not doing the basics when it comes to IT security.

Physician, Heal Thyself

The gist of the report is that while the White House has been very focused on improving the security of the computers and networks which run the nation's commercially-owned critical infrastructure, through efforts like last year's **executive order**, etc., for these efforts to be credible and taken seriously the federal government should address the dangerous insecurity of its own critical networks. This is especially true when the vulnerabilities are due to the failure to perform routine and basic measures.

The report cites the most recent FISMA report in noting that **civilian agencies fail to detect about 4 in 10 intrusions** and notes that many hacks often exploit mundane weaknesses that could be prevented with routine efforts, particularly out-of-date software patches. The report also cites a June 6, 2013 Congressional Research Service memo to the HSGAC Minority Staff on "FISMA Spending, Historical Trends," in which CRS estimates that the **federal government has spent at least $65 billion on IT security since 2006**. (Assuming that covers from FY 2006 to FY 2012, that would average more than $9 billion per year.)

Select examples mentioned in the report include:

- **Homeland Security** – In 2013 OMB found DHS rated below the government-wide average for using anti-virus software or other automated detection programs encrypting email, and security awareness training for network users. DHS also came in at 72% of their internet traffic going through Trusted Internet Connections (TIC), missing its OMB-set goal of 95% and even the general government agency goal of 88%. Other widespread issues deal with unpatched software and poor password practices (using weak/default passwords, written/posted passwords, etc.)
- **Internal Revenue Service** – Every year since 2008, GAO has identified about 100 cybersecurity weaknesses which compromise computers and data, often repeating weaknesses GAO cited the previous year. Issues include routine lack of encryption to protect sensitive data, lax password standards/administration, failure to fix known vulnerabilities that have been identified by their security monitoring, and lagging software patch installation.
- **Energy** – In January 2013 hackers compromised 14 servers and 20 workstations, stealing personal information on hundreds of government and contract employees, and possibly other information. In another incident six months later, hackers took personal information for 104K past and present employees. Vulnerabilities include from unprotected servers, unapplied software patches, weak access controls and passwords, and poorly-secured web applications.

Implications

Shining the spotlight on the ongoing deficiencies of federal agencies to effectively deploy rudimentary security measures may add fuel to the fire in the debate over the fed's role in private CIP and cybersecurity. The lines have been drawn largely between those who favor a regulatory approach with rules and requirements versus those who advocate an incentives-based approach with liability protections. Whatever the merits of either side, the fact still remains that more must be done to secure federal networks, systems and devices.

The Post article notes that Coburn and others see as the underlying problem the fed's failure to hire and maintain highly-skilled IT workers that have the proper authorities to enforce simple security protocols, combined with a lack of accountability at the agency senior level for security failures. The examples emphasize that the problem in this area is not technical, really. It's more about policy, governance and administration. That comes back to strategy, training, and execution, to which agencies should turn to their cyber- industry partners for support and expertise.

Maybe a report like this will give federal IT managers and cybersecurity staff a little more clout to shake the current system out of "zombie mode" and into effective action. We'll see what the next FISMA report reveals.

Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about ***GovWin FIA****. Follow me on Twitter* ***@GovWinSlye****.*