theguardian

US government responds to latest hack: give us more power over data collection

‘Zero day’ attack on high-level security clearance agency reignites push by Congressional leaders to hand federal government greater cybersecurity powers

Spencer Ackerman

June 5, 2015

Congressional leaders are warning the latest major government data hack proves the Senate should hand the US government greater cybersecurity powers – even as the stalled legislation to do so would place even more consumer data into the hands of the same government that could not secure its existing information.

An estimated 4 million federal employees had their personal data compromised after what was reported by authorities on Thursday to be a previously unknown software intrusion, known as a “zero day” attack, accessed networks operated by the Office of Personnel Management, the federal human resources department that houses high-level security clearances and government employee records.

The latest data breach prompted calls from bipartisan leaders of the House intelligence committee for the Senate to pass the Cybersecurity Information Sharing Act (Cisa), the Senate counterpart of a House bill, the Protecting Cyber Networks Act, that the House approved in April, 307-116.

But cybersecurity experts and technologists questioned the wisdom of turning over vast new amounts of private data to the government after another massive exposure of federal government data insecurity. The additional powers sought by the government are a major legislative priority for the National Security Agency, which would gain access to new private data, particularly from financial firms, via the Department of Homeland Security.

“The government must take fast, decisive measures to counter these intrusions, which emanate from hostile nation-states as well as non-state actors,” the chairman of the committee, California Republican Devin Nunes, said on Friday. “The House of Representatives has sought to strengthen our cyber defenses by approving the Protecting Cyber Networks Act, and the Senate urgently needs to pass the bill.”

Lynn Westmoreland, the Georgia Republican who chairs the cybersecurity subcommittee, added: “Business and industry leaders warned us of the growing threats during various hearings, and this attack shows why the Senate needs to move quickly on a cyber bill.”

On Thursday, the subcommittee’s co-chair, Democrat Adam Schiff of California, sounded a similar alarm: “The cyber threat from hackers, criminals, terrorists and state actors is one of the greatest challenges we face on a daily bases, and it’s clear that a substantial improvement in our cyber databases and defenses is perilously overdue. That’s why the House moved forward on cybersecurity legislation earlier this year, and it’s my hope that this latest incident will spur the Senate to action.”

The new breach, however, “undercuts the arguments for Cisa”, said Eli Dourado of the Mercatus Center at George Mason University.

“We’ve been saying for months now that the federal government just sucks at cybersecurity.”

The “information-sharing” bills, which have stalled in the Senate, would expand legal protections for private businesses to share threat patterns of malicious intrusions with the federal government. Privacy advocates have warned since the legislation’s introduction that the nature of cyber threats will require a substantial amount of customer and private data also being provided to the government without adequate privacy protections.

Senator Ron Wyden, an Oregon Democrat on the intelligence committee who voted against Cisa, said on Friday that the bill threatened American privacy.

“It is unlikely that information sharing by private companies would have made any significant difference in protecting federal employee data,” Wyden said in a statement. “That’s why cybersecurity experts say that passing a bill like this will do little to reduce security breaches.

“This is a bad excuse to try and pass a bad bill.”

A coalition of dozens of civil-society groups and cybersecurity experts noted in an April letter that US agencies will “automatically disseminate to the NSA all cyber threat indicators they receive, including personal information about individuals” under the bill.

In April, the Mercatus Center at George Mason University noted in a report that the past year has been “the worst year for federal information security failures on record”. An estimated 67,196 actual or detected security breaches occurred in fiscal 2014, the report found.

“Importantly,” the Mercatus Center found, “the agencies that would be entrusted with significant new data extraction and management responsibilities under Cisa reported alarming security breaches last year.”

In the past year, the homeland security department, which leads the government’s efforts to secure its own networks, reported 1,816 “pieces of computer equipment lost or stolen”, the report found.

Justice Department employees were fooled into downloading malicious software 182 times, a total dwarfed by malware downloads that occurred 370 times at the significantly larger Department of Defense, another wing of government with significant cybersecurity equities and responsibilities. Additionally, a September 2014 report from the cybersecurity firm McAfee Labs noted that such so-called "phishing" attacks are increasing in sophistication.

The prospect of unreported or undetected network breaches means the actual picture of federal cyber vulnerability is likely even more dire than the reported statistics.

"Information-sharing agencies already exist. We've identified 20. Nobody knows how cybersecurity works but they've all decided that information-sharing is the answer. You've got to wonder if that's really more about surveillance than about actual cybersecurity, since it doesn't appear to be working," Dourado said.

Patrick Eddington of the libertarian Cato Institute added: "The notion that the federal government should get still more personal information from Americans as part of a misguided, centralized legislative response to cyber incidents is insane. That approach puts Americans at more, not less, risk of having their personal information compromised."

James Lewis, a cybersecurity expert at the Center for Strategic and International Studies, noted that private banks spend lavishly on security and still get hacked.

"The 'government' doesn't do any worse than companies, and in some ways they do better. US law splits the responsibility – civilian agencies are protected by DHS, national security agencies are protected by NSA. The Chinese succeeded against DHS, but not NSA," Lewis said. Authorities suspect but have not demonstrated Chinese culpability for the newest attack.

"We need to rethink this split responsibility when it comes to information sharing. It's OK to say NSA shouldn't play a bigger role as long as you're willing to accept things like the OPM hack happening over and over again."

The Department of Homeland Security said in a Thursday statement that its automated system for cyber intrusions, Einstein, identified the intrusion, evidently after the data had been exfiltrated. By its nature, Einstein does not identify previously unknown "zero day" threat patterns, which is key to the contention – by the architects of the legislation themselves – that the government needs additional threat data from private firms that detect new threats.

A homeland security spokesman, SY Lee, declined to elaborate on an ongoing investigation of the hack.