NCSL Cybersecurity Task Force
April 21, 2017

Unsuccessful Cyber Attack on Georgia Secretary of State Server

Presented by State representative Don Parsons, HD-44, GA

The Georgia Secretary of State, Brian Kemp ordered his department to conduct an overhaul of its Information Technology (IT) operations in 2013-2014. As part of that overhaul, it was decided to move its cyber protection capabilities from The Georgia Technology Authority (GTA) to a third party private entity. The Secretary of State chooses to not identify the third-party entity it now uses for cyber security, but says it is one of the top firewall monitoring companies, and one that is recognized for its capabilities internationally.

In the months leading up to the 2016 General Election, The U.S. Department of Homeland Security (DHS) offered every state the opportunity to have a "Penetration test" conducted on their respective elections servers. The Georgia Secretary of State was then, and remains confident that its web services and servers are securely protected from cyber-attacks and/or any other attacks due to steps it has taken, including protection provided by the third-party cybersecurity entity with which it contracts. The Georgia Secretary of State declined the offer by DHS. It is my understanding that Georgia was one of just a few states that declined the offer by DHS.

On November 15, 2016, just days after the 2016 General Election, The Georgia Secretary of State was notified by its cyber security entity that there had been an unsuccessful, medium grade attack (defined by Secretary of State office to me as a serious attack against multiple ports of the firewall), and that the attack had been attributed to an IP address assigned to DHS. There had been activity from that IP address before, but they were low grade probes.

Georgia Secretary of State Kemp immediately demanded information from then Secretary of DHS, Johnson. Secretary Johnson's office responded at first that the department knew nothing of the attack. It then identified the attack as coming from Texas. Finally, the Department agreed that it did, in fact, originate from one of its IP addresses, one assigned to the Federal Law Enforcement Training Center (FLETC) in Brunswick, GA.

When the Secretary of State Kemp continued to demand more information, DHS responded that the attack was initiated accidentally because of a system, or program of some kind – possibly an old version of MS WORD that was being used at FLETC, and that it could prove it by recreating the event. Thus far, DHS has never demonstrated that it could recreate it. I asked the Secretary of State if it is possible that the attack was created from another IP address other than DHS, and made to appear as a DHS IP address. The answer, in this case is no. First of all, DHS has acknowledged that the attack is attributable to it. Second, DHS claims that it is

“unspoofable”, that its IP addresses cannot be accessed to appear as the point of attack by another party.

Secretary of State Kemp has asked the Georgia congressional delegation to investigate the attack. He has asked the current Secretary of DHS to look into the issue further. I learned from the Secretary of State that all federal agencies have an Inspector General assigned to the agency, and appointed for a ten (10) year term by a bi-partisan congressional body. Secretary Kemp has requested that the Inspector General for DHS, John Roth, conduct an investigation.

Since the cyber-attack on The Georgia Secretary of State’s website and servers, a number of other states have announced that their servers were also attacked by a DHS IP address. Those states include Kentucky and West Virginia. Indiana, Nevada and Maine might also have been targets.

END