New American

Written by C. Mitchell Shaw on December 9, 2016

Georgia Secretary of State: DHS Attacked Our Firewall

On Thursday, Georgia Secretary of State Brian Kemp sent a letter to the Department of Homeland Security (DHS) to ask "why [it] was attempting to breach" the firewall protecting his computer infrastructure. The letter also drew attention to the fact that "under 18 U.S.C. 1030, attempting to gain access or exceeding authorized access to protected computer systems is illegal."

In the weeks and months leading up to the elections, DHS and other federal agencies expressed growing concerns over the threat of Russian hackers penetrating government computers. Many of those concerns were based in the oft-repeated claim that the hacking of the databases and e-mail servers of the Democratic National Committee (DNC) was the work of Russian hackers. That claim has never been proved, and many experts have said it is not the case. In fact, Julian Assange — the founder and public face of WikiLeaks, which published the DNC documents — flatly denied that the source was Russian.

Based on the accepted "wisdom" that the hacks came from Russia — whether from individual hackers or directed by Moscow — DHS issued a series of recommendations to the states for protecting their voter registration and election systems against attacks aimed at hacking the election. DHS also offered its assistance in providing "cyber hygiene scans or penetration testing" before the elections. As Kemp reminded DHS in his letter:

> Georgia was one of the only few states that did not seek DHS assistance with cyber hygiene scans or penetration testing before this year's election. We declined this assistance due to having already implemented the security measures suggested by DHS.

It appears that — in keeping with its heavy-handed approach in general — DHS was unwilling to take no for an answer. On November 15 — days *after* the election — "an IP address associated with the Department of Homeland Security made an unsuccessful attempt to penetrate the Georgia Secretary of State's firewall," according to Kemp's letter. Kemp also reminded DHS of the fact that its attempted penetration of the firewall was both unwanted and unsuccessful:

> At no time has my office agreed to or permitted DHS to conduct penetration testing or security scans of our network. Moreover, your Department has not contacted my office since this unsuccessful incident to alert us of any security event that would require testing or scanning of our network. This is especially odd and concerning since I serve on the Election Cyber Security

> Working Group that your office created.

Kemp's letter also makes the point that one of his responsibilities as secretary of state is to "protect Georgians' data against the type of event that occurred on November 15" and that since he takes that responsibility seriously, he has "contracted with a global leader in monitored security services to provide immediate responses to these types of threats." He wrote:

> As you may know, the Georgia Secretary of State's office maintains the statewide voter registration data base containing the personal information of over 6.5 million Georgians. In addition, we hold the information for over 800,000 corporate entities and over 500,000 licensed or registered professionals.
>
> As Georgia's Secretary of State, I take cyber security very seriously. That is why I have contracted with a global leader in monitored security services to provide immediate responses to these types of threats. This firm analyzes more than 180 billion events a day globally across a 5,000+ customer base which includes many Fortune 500 companies. Clearly, this type of resource and service is necessary to protect Georgians' data against the type of event that occurred on November 15.

It is noteworthy that Kemp sees this attempted intrusion by DHS as a threat. If DHS were correct and Georgia were in need of DHS "assistance," it would seem that DHS would have *succeeded* in penetrating the firewall protecting the Georgia secretary of state's computer infrastructure. Since DHS *failed* to hack into those systems, it is fair to assume that Russian hackers do not pose a credible threat to those systems, either.

Perhaps the only thing more embarrassing to an overreaching federal agency than telling it you don't need its help is proving it by preventing them from forcing it on you.

This case illustrates the value of a free-market approach. By contracting with "a global leader in monitored security services" (a private firm), Kemp was able to "protect Georgians' data against" *even an attack launched by DHS*. By demonstrating the value of a free-market approach and the fact that states can handle these matters themselves without "assistance" from the federal government, Kemp also demonstrated the lack of value of DHS and its heavy-handed approach.

That is just peachy.