Third Government Hack in the Last Month â€“ This Time itâ€™s the Army

June 11, 2015 â€“ If you ever needed proof that the NSA is watching the wrong people, all you have to do is look at the recent history of hacks against government computer systems. There have been three in the past month, and five big ones announced in the past three months. They include the State Department, the White House, the IRS, the Office of Personnel Management and most recently, the Army. If federal systems are this vulnerable, just imagine the damage that would be done if anyone really wanted to hurt us!

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

You probably couldnâ€™t write a book about this and make it believable. The most powerful government in the world has had five systems hacked in the past few months, all from overseas hackers. Even with the vast electronic intelligence gathering apparatus at its disposal, that government hasnâ€™t been able to keep the hackers out. Perhaps thatâ€™s because it has been using that vast intelligence apparatus to gather data on every phone call made by Americans living in the United Statesâ€¦ but weâ€™ll just leave that alone for the moment.

In March, the State Department revealed that its email system had been hackedâ€¦ thank goodness that Hillary was using her own server. Federal law enforcement authorities called it the â€œworst everâ€• hacking intrusion against a federal agency. But that was then.

Now the worst ever hacking intrusion appears to be the one against the Office of Personnel Management. That one revealed the personally identifiable information of 4 million federal employees and included data on employees with security clearances.

In between these two massive attacks, there were a couple of smaller ones. The attack against White House computers was made possible by the attack on State Department Computers. The hackers used their access to the State Department to gain access to the White House. But thatâ€™s not the funny part. No, the funny part is that the State Department knew about the attack on its systems for about a year. Oh, but wait, thatâ€™s not the funny part either. The funny part is that the State Department revealed the hack because they were trying to help Hillary justify the use of a personal email server for government business. They made the claim that the State Departmentâ€™s email system had so many security flaws that it was safer for the Secretary of State to keep a private email server in a closet in her house. Whatâ€™s wrong with this picture?

And then of course there is the IRS hack. That one gained access to the tax returns of 100,000 people and targeted more than 200,000 people.

Now comes word that the Armyâ€™s public computer system has been hacked. In this most recent case, the hackers managed to take down the Armyâ€™s website and replace it with their own message.

All of these hacks have one thing in common. As previously mentioned, none of them originated in the US. The State Department, White House and IRS hacks all originated in Russia. The Office of Personnel Management hack originated in China. And the group claiming responsibility for the Army hack is supposedly from Syria.

The White House is blaming congress for these problems. They are saying that its congressâ€™s fault that the government is using antiquated technology. But that doesnâ€™t hold up under a little scrutiny.

For instance, in the case of the IRS hack, the agency admitted that it was running systems that hadnâ€™t been updated with the latest security patches even though these patches were availableâ€¦ free of chargeâ€¦ from the software manufacturers. Thatâ€™s a matter of incompetence and Congress has nothing to do with it.

Furthermore, if agencies within the federal government know that their systems are vulnerable â€“ regardless of reason â€“ there is absolutely no reason to load those systems with classified or sensitive information that can then be accessed via the internet. There is actually an argument to be made here that anyone who does expose classified information this way is guilty of a crime and should be prosecuted. Thatâ€™s certainly the case for anyone who knowingly uploads data to a system which they know has inferior security.

It is absolutely no secret that the federal governmentâ€™s data security record is abysmal. It is time for someone â€“ at the White House or in congress â€“ to step up to the plate, display a small modicum of leadership skill and secure all federal IT systems. The utter incompetence displayed in just these five hacks in inexcusable and it hurts every single one of us.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS