The frightening potential of hackers disrupting the ballot

Business, Accounting

The foundation of our Republic is confidence that our elected officials are chosen in a fair and democratic system. If that system is called into question, the distrust could create chaos. What would a breach in the election system mean for the electoral process? The mere suggestion of any type of tampering has already lead to some mistrust amongst both candidates and voters -- so evidence of an actual breach could throw the entire system into question.

In 2016, the bulk of our entire election process is operated digitally, leaving each step in the process vulnerable to criminal intervention. From sensitive information held in the inboxes of political party leaders, to digital polling, to vulnerabilities in the voting machines themselves, to reporting of the results by the media, there are many avenues that a criminal could take to make an impact on the United States’ democratic process. And it's already happening, as evidenced by recent reports that the DNC was hacked by the Russians, as well as alleged breaches of the state election systems in Arizona and Illinois. Other states have also noticed suspicious activity probing their systems.

Related:

How would it be done?

There are three main aspects of the election that could be tampered -- namely electronic voting machines, election management and tabulation systems (many run Windows), and voter registrations.

Tampering with any one of these particular features is surprisingly easy. We can look to ATM hacks as a model for voting machine hacks. For instance, we have seen specially programmed smart cards modify ATM software. ATMs have also been hacked by physically modifying their software. Similar attacks could be used on voting machines in several states, such as Pennsylvania, which have no paper record.

Another method a cyber criminal could use would be a denial of service (DoS) attack. These attacks can be launched to disable a system or slow its functionality to the point of uselessness. Distributed denial of service attacks, in particular, have gained popularity due to the power . However, it would not be easy for an adversary armed with this weapon to disrupt the elections. While vote submissions and tallying would be slowed down, the actual results would not be changed. Additionally, these attacks are not simple to create.

There is also the hijacking and defacement of these systems -- even when not connected to the web. Getting malware onto the Election Headquarters system could be done with typical USB flash drives and can even be done remotely if an election worker’s computer is compromised so that software updates or data is moved from an internet connected machine to the Election Headquarters’ machines.

Related:

It’s not hard to imagine blocked voting machines with a display that reads, “ Your vote was hacked by Guccifer 2. 0!” is it?

Implications and contingency plan.

Any of these methods could potentially change the election’s direction and call the legitimacy of an election into question. Unfortunately, we don’t know what capabilities the Department of Homeland Security has in place. Is there a cyber-SWAT team on call to figure out what happened and respond? And how would we deal with the general voter fallout?

Consider that in 2004 due to a bug in their Unilect voting machines. If fewer than 5, 000 votes seems trivial in the context of a presidential election, remember that the 2000 presidential election was won by George W. Bush with less than 1, 000 votes. An election that was then hotly contested over the next month. In this light, the tampering could directly affect election results as voter sentiment is already being influenced. Bloomberg is reporting that even state election officials have warned against online voting at a recent gathering of governors. Per the article, "... the officials said that the climate for adopting long distance means of casting ballots -- including voting online -- has cooled in reaction to hacking incidents."

Related:

The possibility of a contested result could also fuel further uncertainty, government contention and generate a negative vision of the U. S. electoral process. We must be extremely wary of the negative possibilities and do something to address the problem now. Whatever it takes, from going back to chads and paper ballots to doing a careful and thorough vetting process of the security controls currently in place, we need to make sure we maintain the integrity of our democratic election process.