**US Cyber Pros: Hackers Could Hit Electronic Voting Machines Next**

Michael Lipin

August 03, 2016 4:45 PM

WASHINGTON—U.S. cyber security professionals say suspected foreign hackers who recently attacked computer systems of the Democratic Party could do something even more sinister in the future.

The cyber pros, who appeared on this week's Hashtag VOA program, said U.S. electronic voting systems are likely to be among the next targets.

When the whistle-blowing website WikiLeaks published leaked emails of the U.S. Democratic National Committee last month, it caused major embarrassment to the party, and forced U.S. Congresswoman Debbie Wasserman Schultz to quit her position as the DNC chairperson.

Cybersecurity analyst Richard Forno said that outcome shows foreign hackers can achieve political goals and incentivizes them to escalate their attacks.

"Interfering with the electoral and political process of countries is a classic tool of intelligence and foreign policy,” said Forno, who directs the University of Maryland’s Center for Cybersecurity. “Even though we are moving toward an era of electronic and technology-enabled voting in more places, this [DNC cyberattack] reinforces the fact that the traditional threats are still with us, and are now moving further into cyberspace."

Electronic voting machines are part of that cyberspace. The vast majority of U.S. states will use them for this November's national elections.

But a 2015 study by New York University found that 43 of those states had machines that were at least a decade old.

Could they be hacked as well? Cyber security pros attending an annual Las Vegas conference known as Black Hat think so.

Attack in Ukraine

One of them is Toni Gidwani, research director at ThreatConnect, a cyberdefense platform used by 1,200 companies and organizations worldwide. She said there is a precedent for attacks on voting systems.

"We saw that in Ukraine in 2014, where three days before the election, the Ukrainian central election committee suffered a massive hack that threatened their ability to hold voting on schedule,” she said. “And then malware was discovered right before results were announced – malware that would have projected a totally different outcome in which an ultranationalist candidate, who in reality received less than 1 percent of the vote, would have won. So this is not science fiction - we have already seen this happen."

Some U.S. voting machines produce paper records that can be used in case of problems with a vote count. But keeping a paper trail might not be enough.

Yong-Gon Chon, another Black Hat attendee, said any organization seeking to protect itself from hackers needs all of its personnel to play their part.

"It is no longer just the responsibility of a chief security officer or CIO to protect an organization's infrastructure - everyone has a role to play,” said Chon, who serves as CEO of Cyber Risk Management and has led global security teams for more than 20 years. “There is a shared level of responsibility, whether you are using cloud systems or your own systems within your organizations. And ultimately it is about being able to practice safe and healthy (cyber) activities on a day to day basis."

One healthy habit recommended by Chon is being skeptical when you receive an email containing a hyperlink that could expose you to a hacker.

“You should determine whether or not that is something that you should trust and is acceptable for your business,” he said.