Hacking of DNC raises fears of cyber attack on US election

04/11/2016

The recent breach of Democratic National Committee data, along with other electronic intrusions, has raised concerns about cyber incidents that could affect the outcome of the US presidential race, or other contests.

The campaign of Democratic presidential nominee Hillary Clinton said the hack that targeted the DNC had accessed an analytics data program that it used as well.

Cybersecurity experts see a potential for more hacks and incidents in the coming months which could hurt the integrity of the election campaign.

Bob Hansmann of the security firm Forcepoint, which last year predicted a rise in political cyber intrusions, said a variety of groups might target US political campaigns.

"There are a lot of motivations out there," Hansmann told AFP. "It could be to disrupt, discredit or embarrass a candidate. Or it could be to disrupt the entire political system."

Campaign organizations can be soft targets, Hansmann said, because they have large numbers of employees and volunteers who are on the move, often with their own computers and smartphones with varying degrees of security.

Almost anyone can employ hackers-for-hire to break into networks, steal data or "spoof" a campaign organization to deliver faked emails or social media messages, he said.

Steve Grobman, chief technical officer at Intel Security, said the hack at the DNC "is the latest high-profile reminder that information of tremendous value internally can be used as a devastating weapon if disclosed externally."

Grobman said the DNC breach is "a classic example of a 'hacktivist' event, where the objective of a cyber attack is to steal an organization's sensitive information and disclose it in such a way that the reputational, operational or

organizational damage to that organization is maximized."

Russian connection?

The possibility that Russian hackers have been behind the cyber intrusions—as widely suspected by some officials and experts—raises the stakes. Foreign intervention in the election process would be a grave matter.

US officials say the FBI is investigating but has drawn no conclusions. Russia has denied any involvement.

President Barack Obama said Tuesday that "we have provisions in place where, if we see evidence of a malicious attack by a state actor, we can impose, potentially, certain proportional penalties."

But he added that taking such action "requires us to really be able to pin down and know what we're talking about. And so I don't want to get out ahead of the legal evidence and facts that we may have in order to make those kinds of decisions."

Recent breach of Democratic National Committee data, along with other electronic intrusions, has raised concerns

about cyber incidents that could affect the outcome of the US presidential race
Security analysts said the US should take action once the source of the threat is known.

This kind of attack "meets the definition of an act of cyber-war, and the US government should respond as such," said Dave Aitel, chief executive of the security firm Immunity Inc. in a blog post on the website Ars Technica.

Bruce Schneier, chief technology officer of the IBM security firm Resilient and a fellow at Harvard's Berkman Center, also warned of the gravity of such attacks.

"This kind of cyber attack targets the very core of our democratic process," Schneier said in a blog post.

"And it points to the possibility of an even worse problem in November—that our election systems and our voting machines could be vulnerable to a similar attack."

As the close and fiercely disputed 2000 presidential election showed, the results of a single state—like Florida—can determine the national outcome, potentially simplifying hackers' work.

Schneier said interference from abroad cannot go without a response, saying that "if foreign governments learn that they can influence our elections with impunity, this opens the door for future manipulations, both document thefts and dumps like this one that we see and more subtle manipulations that we don't see."

Information as weapon

If the DNC intrusion was indeed a Russian-sponsored hack, "it would be a bold move," said James Lewis, who heads strategic technologies at the Washington-based Center for Strategic and International Studies.

Lewis said the DNC attack bears the hallmarks of a Russian hack, "but they are usually more skillful at hiding their tracks."

It is not surprising to see Russia involved in this type of attack, said Lewis.

The Russians "see themselves in a new conflict where control of information is a tool or even a weapon," he said.

"They feel that Western institutions dominate global perceptions, and they feel there's a need to push back."

The evidence against Russia "is about as close to a smoking gun as can be expected where a sophisticated nation-state is involved," said Susan Hennessey, a national security fellow at the Brookings Institution, on the Lawfare Blog.

"This means, put simply, that actors outside the US are using criminal means to influence the outcome of a US election. That's a problem. The question before us now is how to construct a response to mitigate damage to our democratic institutions."