US studying Australian Internet security program

October 16 2010, By LOLITA C. BALDOR , Associated Press Writer

(AP) -- The government is reviewing an Australian program that will allow Internet service providers to alert customers if their computers are taken over by hackers and could limit online access if people don't fix the problem.

Obama administration officials have met with industry leaders and experts to find ways to increase online safety while trying to balance securing the Internet and guarding people's privacy and civil liberties.

Experts and U.S. officials are interested in portions of the plan, set to go into effect in Australia in December. But any move toward Internet regulation or monitoring by the U.S. government or industry could trigger fierce opposition from the public.

The discussions come as private, corporate and government computers across the U.S. are increasingly being taken over and exploited by hackers and other computer criminals.

White House cybercoordinator Howard Schmidt told The Associated Press that the U.S. is looking at a number of voluntary ways to help the public and small businesses better protect themselves online.

Possibilities include provisions in the Australia plan that enable customers to get warnings from their Internet providers if their computer gets taken over by hackers through a botnet.

A botnet is a network of infected computers that can number in the thousands and that network is usually controlled by hackers through a small number of scattered PCs. Computer owners are often unaware that their machine is linked to a botnet and is being used to shut down targeted websites, distribute malicious code or spread spam.

If a company is willing to give its customers better online security, the American public will go along with that, Schmidt said.

"Without security you have no privacy. And many of us that care deeply about our privacy look to make sure our systems are secure," Schmidt said in an interview. Internet service providers, he added, can help "make sure our systems are cleaned up if they're infected and keep them clean."

But officials are stopping short of advocating an option in the Australian plan that allows Internet providers to wall off or limit online usage by customers who fail to clean their infected computers, saying this would be technically difficult and likely run into opposition.

"In my view, the United States is probably going to be well behind other nations in stepping into a lot of these new areas," said Prescott Winter, former chief technology officer for the National Security Agency, who is now at the California-based cybersecurity firm, ArcSight.

In the U.S., he said, the Internet is viewed as a technological wild west that should remain unfenced and unfettered. But he said this open range isn't secure, so "we need to take steps to make it safe, reliable and resilient."

"I think that, quite frankly, there will be other governments who will finally say, at least for their parts of the Internet, as the Australians have apparently done, we think we can do better."

Cybersecurity expert James Lewis, a senior fellow at the Center for Strategic and International Studies, said that Internet providers are nervous about any increase in regulations, and they worry about consumer reaction to monitoring or other security controls.

Online customers, he said, may not want their service provider to cut off their Internet access if their computer is infected. And they may balk at being forced to keep their computers free of botnets or infections.

But they may be amenable to having their Internet provider warn them of cyberattacks and help them clear the malicious software off their computers by providing instructions, patches or anti-virus programs.

They may even be willing to pay a small price each month for the service - much like telephone customers used to pay a minimal monthly charge to cover repairs.

Lewis, who has been studying the issue for CSIS, said it is inevitable that one day carriers will play a role in defending online customers from computer attack.

Comcast Corp. is expanding a Denver pilot program that alerts customers whose computers are controlled through a botnet. The carrier provides free antivirus software and other assistance to clean the malware off the machine, said Cathy Avgirls, senior vice president at Comcast.

The program does not require customers to fix their computers or limit the online usage of people who refuse to do the repairs.

Avgrils said that the program will roll out across the country over the next three months. "We don't want to panic customers. We want to make sure they are comfortable. Beyond that, I hope that we pave the way for

others to take these steps."

Voluntary programs will not be enough, said Dale Meyerrose, vice president and general manager of Cyber Integrated Solutions at Harris Corporation.

"There are people starting to make the point that we've gone about as far as we can with voluntary kinds of things, we need to have things that have more teeth in them, like standards," said Meyerrose.

For example, he said, coffee shops or airports might limit their wireless services to laptops equipped with certain protective technology. Internet providers might qualify for specific tax benefits if they put programs in place, he said.

Unfortunately, he said, it may take a serious attack before the government or industry impose such standards and programs.

In Australia, Internet providers will be able to take a range of actions to limit the damage from infected computers, from issuing warnings to restricting outbound e-mail. They could also temporarily quarantine compromised machines while providing customers with links to help fix the problem.

More information: Homeland Security Department/Cybersecurity: http://tinyurl.com/24xpfg3
White House Cybersecurity: http://tinyurl.com/2wnv3sz

2024 from https://phys.org/news/2010-10-australian-internet.html