Clinton email server setup risked intrusions

13 October 2015, byJack Gillum And Stephen Braun

In this Oct. 18, 2011, file photo, then-Secretary of State Hillary Rodham Clinton checks her Blackberry from a desk inside a C-17 military plane upon her departure from Malta, in the Mediterranean Sea, bound for Tripoli, Libya. The private email server running in Clinton's home basement when she was secretary of state was connected to the Internet in ways that made it more vulnerable to hackers, according to data and documents reviewed by The Associated Press. (Kevin Lamarque/Pool Photo via AP, File)

The private email server running in Hillary Rodham Clinton's home basement when she was secretary of state was connected to the Internet in ways that made it more vulnerable to hackers while using software that could have been exploited, according to data and documents reviewed by The Associated Press.

Clinton's server, which handled her personal and State Department correspondence, appeared to allow users to connect openly over the Internet to control it remotely, according to detailed records compiled in 2012. Experts said the Microsoft remote desktop service wasn't intended for such use without additional protective measures, and was the subject of U.S. government and industry warnings at the time over attacks from even low-skilled intruders.

Records show that Clinton additionally operated two more devices on her home network in Chappaqua, New York, that also were directly accessible from the Internet. One contained similar remote-control software that also has suffered from security vulnerabilities, known as Virtual Network Computing, and the other appeared to be configured to run websites.

The new details provide the first clues about how Clinton's computer, running Microsoft's server software, was set up and protected when she used it exclusively over four years as secretary of state for all work messages. Clinton's privately paid technology adviser, Bryan Pagliano, has declined to answer questions about his work from congressional investigators, citing the U.S. Constitution's Fifth Amendment protection against self-incrimination.

Some emails on Clinton's server were later deemed top secret, and scores of others included confidential or sensitive information. Clinton has said that her server featured "numerous safeguards," but she has yet to explain how well her system was secured and whether, or how frequently, security updates were applied.

Clinton has apologized for running her homebrew server, and President Barack Obama said during a "60 Minutes" interview aired Sunday that it was "a mistake." Obama said national security wasn't endangered, although the FBI still has yet to complete its review of Clinton's server for evidence of hacking.

On Tuesday, however, the White House left room for results of the Justice Department's investigation into her server. "The president certainly respects the independence and integrity of an independent investigation, including those that are conducted by the FBI," press secretary Josh Earnest said.

Clinton spokesman Brian Fallon said late Monday that "this report, like others before it, lacks any evidence of an actual breach, let alone one specifically targeting Hillary Clinton. The Justice Department is conducting a review of the security of the server, and we are cooperating in full."

The AP exclusively reviewed numerous records from an Internet "census" by an anonymous hacker-researcher, who three years ago used unsecured devices to scan hundreds of millions of Internet Protocol addresses for accessible doors, called "ports." Using a computer in Serbia, the hacker scanned Clinton's basement server in Chappaqua at least twice, in August and December 2012. It was unclear whether the hacker was aware the server belonged to Clinton, although it identified itself as providing email services for clintonemail.com. The results are widely available online.

Remote-access software allows users to control another computer from afar. The programs are usually operated through an encrypted connection—called a virtual private network, or VPN. But Clinton's system appeared to accept commands directly from the Internet without such protections.

"That's total amateur hour," said Marc Maiffret, who has founded two cybersecurity companies. He said permitting remote-access connections directly over the Internet would be the result of someone choosing convenience over security or failing to understand the risks. "Real enterprise-class security, with teams dedicated to these things, would not do this," he said.

The government and security firms have published warnings about allowing this kind of remote access to Clinton's server. The same software was targeted by an infectious Internet worm, known as Morta, which exploited weak passwords to break into servers. The software also was known to be vulnerable to brute-force attacks that tried password combinations until hackers broke in, and in some cases it could be tricked into revealing sensitive details about a server to help hackers formulate attacks.

"An attacker with a low skill-level would be able to exploit this vulnerability," said the Homeland Security Department's U.S. Computer Emergency Readiness Team in 2012, the same year Clinton's server was scanned.

Also in 2012, the State Department had outlawed use of remote-access software for its technology officials to maintain unclassified servers without a waiver. It had banned all instances of remotely connecting to classified servers or servers located overseas.

The findings suggest Clinton's server "violates the most basic network-perimeter security tenets: Don't expose insecure services to the Internet," said Justin Harvey, the chief security officer for Fidelis Cybersecurity.

Clinton's email server at one point also was operating software necessary to publish websites, although it was not believed to have been used for this purpose. Traditional security practices dictate shutting off all of a server's unnecessary functions to prevent hackers from exploiting design flaws.

In Clinton's case, Internet addresses the AP traced to her home in Chappaqua revealed open ports on three devices, including her email system. Each numbered port is commonly, but not always uniquely, associated with specific features or functions. The AP in March was first to discover Clinton's use of a private email server and trace it to her home.

Mikko Hypponen, the chief research officer at F-Secure, a top global computer security firm, said it was unclear how Clinton's server was configured, but an out-of-the-box installation of remote desktop would have been vulnerable. Those risks—such as giving hackers a chance to run malicious software on her machine—were "clearly serious" and could have allowed snoops to deploy so-called back doors.

The U.S. National Institute of Standards and Technology, the federal government's guiding agency on computer technology, warned in 2008 that exposed server ports were security risks. It said remote-control programs should only be used in conjunction with encryption tunnels, such as secure VPN connections.

APA citation: Clinton email server setup risked intrusions (2015, October 13) retrieved 19 September 2019 from https://phys.org/news/2015-10-clinton-server-ran-software-hacking.html