US works to secure networks as hackers advance

December 5 2010, By LOLITA C. BALDOR , Associated Press

In this Sept. 24, 2010, file photo the National Cybersecurity & Communications Integration Center (NCCIC) prepares for the Cyber Storm III exercise at its operations center in Arlington, Va. It will take several more years for the government to install high-tech systems capable of detecting and blocking computer intrusions, giving hackers more time to figure out how to breach networks and steal sensitive data. The government's computer security weaknesses were laid bare with the WikiLeaks release. (AP Photo/J. Scott Applewhite, File)

(AP) -- It will take several more years for the government to fully install high-tech systems to block computer intrusions, a drawn-out timeline that enables criminals to become more adept at stealing sensitive data, experts say.

As the Department of Homeland Security moves methodically to pare down and secure the approximately 2,400 network connections used every day by millions of federal workers around the world, experts

suggest that technology already may be passing them by.

The department that's responsible for securing government systems other than military sites is slowly moving all the government's Internet and e-mail traffic into secure networks that eventually will be guarded by intrusion detection and prevention programs. The networks are known as Einstein 2 and Einstein 3.

Progress has been slow, however. Officials are trying to complete complex contracts with network vendors, work out technology issues and address privacy concerns involving how the monitoring will affect employees and public citizens.

The WikiLeaks release of more than a quarter-million sensitive diplomatic documents underscores the massive challenge ahead, as Homeland Security labors to build protections for all of the other, potentially more vulnerable U.S. agencies.

"This is a continuing arms race and we're still way behind," said Stewart Baker, former Homeland Security undersecretary for policy.

The WikiLeaks breach affected the government's classified military network and was as much a personnel gap as a technological failure. Officials believe the sensitive documents were stolen from secure Pentagon computer networks by an Army intelligence analyst who downloaded them onto a CD.

The changes sought by Homeland Security on the government's nonmilitary computers would be wider and more systemic than the immediate improvements ordered recently by the Departments of Defense and State as a result of the WikiLeaks releases. Those changes included improving the monitoring of computer usage and making it harder to move material onto a portable computer flash drive or CD.

"There are very few private sector actors who depend on information security who think that installing intrusion prevention systems is sufficient protection against the kinds of attacks that we're seeing," Baker said.

Navy Rear Adm. Michael Brown, Homeland Security's director for cybersecurity coordination, said that slightly more than half of the government's 2,400 network connections are already protected by Einstein 2 - the automated system that monitors federal Internet and e-mail traffic for malicious activity.

Those, however, cover fewer than 20 of the 110 federal agencies.

Einstein 2 is installed and working at 13 of the 19 agencies that plan to police their own networks, with two others close to completion. The remaining 91 departments will go through one of four major communications companies for the monitoring. So far just four to six agencies have put the program in place, he said.

In the end, all network traffic with flow through 72 sites called Trusted Internet Connections, including eight operated by the four communications companies and 64 operated by individual agencies.

A more sophisticated system known as Einstein 3, which will detect and automatically block intrusions, has just completed testing and will take several years to fully implement, Brown said.

Brown insisted that the government is not lagging behind private industry in its efforts to secure computer networks. He said each agency is responsible for setting up safe cybersecurity practices. Criminals these days "are more targeted, are more professional, and have greater sophistication and capabilities," he said.

Einstein will add a valuable safeguard to government agencies but "there still is not a magic bullet" to defeat the increasingly sophisticated threats, said Jerry Dixon, former director at Homeland Security's Computer Emergency Readiness Team.

"We're always playing catch-up or reacting to the last major cyberincident or event but not doing a lot to think about what the future might hold," said Dixon, who is now director of analysis at the Internet security firm Team Cymru.

Complicating the Einstein installation process is that federal agencies have offices and personnel strewn around the globe, from post offices to nuclear labs and national parks. They can be small outposts with a handful of workers or huge complexes employing thousands, and they are operating under many contracts with different Internet vendors.

Baker said legal questions bog down the process. There are concerns that the monitoring programs could violate privacy safeguards for federal workers, members of the public who communicate with them, or other individuals whose e-mail might accidentally get caught in the system.

"The search for legal certainty and legal guarantees may be part of the problem," he said.

U.S. officials and security experts have warned that government networks are persistently scanned and attacked millions of times a day. The recent discovery of the Stuxnet worm, which experts say appeared to target Iranian nuclear plants, stunned and worried U.S. officials, who said it could be modified to wreak havoc on industrial control systems around the world.

Those systems control vital facilities like the electric grid, water plants, traffic systems and industries that produce everything from deadly

chemicals to baby formula.

More information: Homeland Security: http://www.dhs.gov/files/cybersecurity.shtm