Pentagon Faces Computer Security Problems

by Vicky O'Hara

December 12, 2005

Listen

Morning Edition

- Add to Playlist
- Download

text size A A A

December 12, 2005

The Pentagon's 5 million computers make a tempting target for computer hackers. Officials reported 80,000 attempts to disrupt the system last year. What is being done to improve security?

STEVE INSKEEP, host:

As computers spread around the globe, so do computer hackers. The potential cost of cybercrime to US commerce and industry increase exponentially every year, and then there's the threat that hackers pose to national security. NPR's Vicky O'Hara reports.

VICKY O'HARA reporting:

Neither the Pentagon nor military contractor want to discuss specific cases of cyberintrusion that have undermined national security. But one case has been well documented in the public realm. The operation is known as Tighten Reign. It was discovered by cyberinvestigators at Sandia National Laboratories in New Mexico two and a half years ago. Tighten Reign involved a group of highly organized, sophisticated and prolific hackers operating out of China's southern Guangdong province. The Tighten Reign perpetrators targeted a variety of US agencies, but they concentrated their attacks on the Defense Department and defense contractors. Allen Paller is director of research at the SANS Institute in Maryland, which teaches cybersecurity.

Mr. ALLEN PALLER (SANS Institute): In one evening, at about 10:23 at night Pacific time, they found vulnerabilities in the US Army Information Systems Engineering Command at Ft. Huachuca, Arizona. Three hours later, they found the same hole in computers at the Defense Information Systems Agency in

Arlington. A little more than two hours later, they hit the Naval Ocean Systems Center(ph), a Defense Department installation in San Diego. And an hour and a half later, they hit the United States Army Space & Strategic Defense installation in Huntsville.

O'HARA: Cyberanalysts who followed the investigation of Tighten Reign say that among the massive amounts of data that the hackers penetrated were detailed specifications on the Mars lander as well as information about satellite and missile technology and about US troop deployments. One of the original investigators of Tighten Reign, who asked not to be identified to preserve his job, confirms that account. Allen Paller of the SANS Institute says the damage was serious.

Mr. PALLER: We don't have data that any classified information was taken, but it was important information that is very sensitive militarily.

O'HARA: Cybersecurity analysts warn that hackers don't have to have the expertise of Tighten Reign to penetrate DOD systems. And Colonel Carl Hunt, director of technology for the Pentagon's Joint Task Force for Global Network Operations, says the number of cyberattacks against Defense Department systems is increasing.

Colonel CARL HUNT (Joint Task Force for Global Network Operations): In 2004 we experienced approximately 80,000 intrusion attempts.

O'HARA: According to Colonel Hunt, that compares to about 55,000 in 2003. Hunt defines intrusion attempts as anything that went beyond probing and was an actual documented attempt to break into Defense Department systems. He said that of the intrusions last year, only about 600 were what he defines as successful, meaning something as mundane as compromising a password or as serious as a hacker downloading code into a Pentagon computer to affect its operations. Colonel Hunt says that as far as the Pentagon can detect, none of those 600 intrusions was directed against classified systems.

Col. HUNT: However, any information that is stolen from a DOD computer in an unclassified setting is still considered to be a serious incident in our view.

O'HARA: Colonel Hunt points out that the explosion in cyberattacks is not unique to the Defense Department. Western financial institutions, academia and corporations also are under attack. What makes the Pentagon different is its sheer size. Colonel Hunt says the Defense Department has five million computers and as that number increases, so does the Pentagon's vulnerability to attack.

Cybersecurity analysts say that each person using those Pentagon computers could unwittingly invite an attack. Steven Spoonamore is CEO of Cybrinth Corporation, which advises government agencies and the defense industry.

Mr. STEVEN SPOONAMORE (CEO, Cybrinth Corporation): Most people today do not understand that when they lock their door at night but leave their fiber-optic cable or their CAT5 on, that they might as well not have locked the door.

O'HARA: Colonel Hunt says the Pentagon does train its personnel in cybersecurity, but he acknowledges that more needs to be done.

Col. HUNT: I think many of our people don't understand the consequences of having this type of connectivity.

O'HARA: Professor Gene Spafford of Purdue University has acted as a White House consultant on cybercrime. He says the Pentagon's problem is not just training of personnel but its choice of technology. Some Pentagon systems, he says, are highly protected, but in general, according to Spafford, the Defense Department relies heavily on commercially available technology.

Professor GENE SPAFFORD (Purdue University): So the very same thing that you might use at home for cruising the Net and paying video games is being purchased and deployed with some configuration to do command and control and weapons control. We need to get into a mode where we evaluate the risk and try to pick the best possible tool rather than the cheapest and most convenient.

O'HARA: Under the current setup, Spafford says, all a hacker needs to do is to find a few poorly protected systems somewhere in the vast Defense Department network and then use that as a steppingstone to get in to more protected systems. Colonel Hunt concedes that using commercially available technology is a security weakness, but he says it's hardly feasible at this point for the Defense Department to develop completely separate systems. According to cyberspecialists, it's almost impossible to achieve total cybersecurity because today's hackers are so good. Tom Kellermann is chief knowledge officer with Cybrinth Corporation.

Mr. TOM KELLERMANN (Cybrinth Corporation): Even if you don't understand how to hack, per se, all you need to do is go to an Internet relay chat room and essentially hire a number of mercenaries that are at your disposal that will create you weapons to penetrate a number of various network configurations.

O'HARA: Tom Kellermann notes that technology has leveled the playing field in cyberspace.

Mr. KELLERMANN: This is a symmetrical warfare.

O'HARA: And rogue states, Kellermann says, are seizing the opportunity.

Mr. KELLERMANN: It's been well documented that the North Koreans, for example, created a hacking academy, per se, so that they could essentially either read the minds of the Americans or South Koreans and/or steal intellectual property that would benefit their economy.

O'HARA: Part of what makes cyberintrusion so dangerous is the difficulty in identifying the source. Again, Colonel Hunt.

Col. HUNT: You don't just get an attack one day and call the State Department and tell them to go off and see the ambassador to so-and-so and tell them to stop this attack. It takes time for us to understand all the implications and sources of that attack.

O'HARA: What's worse, many attacks go undetected for a long time. Colonel Hunt says the Pentagon puts scanners on everything these days in an effort to identify intrusions, but cybersecurity experts say that scanners typically pick up less than half of all cyberattacks.

Vicky O'Hara, NPR News, Washington.

INSKEEP: Our series continues tomorrow when we'll learn more about the implications of cyberattacks against defense contractors.

This is NPR News.