PHYS ORG

24,000 files stolen from defense contractor: Pentagon

July 15 2011, by Chris Lefkow

A foreign intelligence service swiped 24,000 computer files from a US defense contractor in March in one of the largest ever cyberattacks on a Pentagon supplier, a top Defense Department official revealed on Thursday.

"It is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies," Deputy Defense Secretary William Lynn said.

"In a single intrusion this March, 24,000 files were taken," Lynn said in a speech at National Defense University here outlining the Pentagon's strategy in cyberspace.

Speaking to reporters after his speech, Lynn described the theft of data from the unidentified defense contractor as "significant" and one of the largest ever.

"It was large -- 24,000 files," he said. "It was data-related to systems that are being developed for the Department of Defense.

"It was done, we think, by a foreign intelligence service," he said. "In other words a nation state was behind it."

China has been blamed for a number of probes of US corporate and military computer systems over the past few years but Lynn declined to point the finger at any specific suspects in the March intrusion.

"We don't get into our understanding of exactly who it was," he said.

Lynn said the data theft had "compromised information relative to the design of military equipment" but had not "set us back in terms of the development of the system."

In his speech, Lynn said some of the data stolen by intruders is "mundane, like the specifications for small parts of tanks, airplanes, and submarines.

"But a great deal of it concerns our most sensitive systems, including aircraft avionics, surveillance technologies, satellite communications systems, and network security protocols," he said.

"The cyber exploitation being perpetrated against the defense industry cuts across a wide swath of crucial military hardware, extending from missile tracking systems and satellite navigation devices to UAVs (unmanned aerial vehicles, or drones) and the Joint Strike Fighter," he said.

Lynn also said he did not believe the March intrusion involved the use of SecurID tokens that were stolen from US computer security titan RSA Security in a sophisticated hacking attack in March.

RSA's parent company, EMC Corp. has acknowledged that intruders breached its security systems at defense contractor Lockheed Martin in May using data swiped from RSA.

Outlining the Defense Department's strategy in cyberspace, Lynn said the Pentagon considers cyberspace an operational domain, like land, air, sea and space.

"Treating cyberspace as a domain means that the military needs to operate and defend its networks, and to organize, train and equip its forces to perform cyber missions," he said.

"In the 21st Century, bits and bytes can be as threatening as bullets and bombs," he said. "Keystrokes originating in one country can impact the other side of the globe in the blink of an eye."

Lynn said information technology has become so important to US military operations that it "virtually guarantees that future adversaries will target our dependence on it.

"Our assessment is that cyber attacks will be a significant component of any future conflict, whether it involves major nations, rogue states, or terrorist groups," he said.

Lynn said US military power served as a deterrent against cyberattack from a nation state but "if a terrorist group gains disruptive or destructive cyber tools, we have to assume they will strike with little hesitation."

The thrust of the Defense Department's cyber strategy is defensive, he said, and "it should come as no surprise that the United States is prepared to defend itself.

"Just as our military organizes to defend against hostile acts from land, air and sea, we must also be prepared to respond to hostile acts in cyberspace," he said.

"Accordingly, the United States reserves the right, under the laws of armed conflict, to respond to serious cyber attacks with a proportional and justified military response at the time and place of our choosing," he said.

Lynn, who was accompanied by Marine General James Cartwright, vice chairman of the Joint Chiefs of Staff, declined to elaborate on US offensive cyber capabilities or what would constitute an act of war in cyberspace.

"It's a judgment," Cartwright said of an act of war. "It's subjective. It's in the eye of the beholder."

Citation: 24,000 files stolen from defense contractor: Pentagon (2011, July 15) retrieved 24 April 2024 from https://phys.org/news/2011-07-stolen-defense-contractor-pentagon.html