

Cyberattacks target U.K. national infrastructure

Published 4 November 2008

The computer systems of critical businesses in the United Kingdom, such as power companies and large financial institutions, are being repeatedly probed to steal information or uncover weaknesses that could take them down

Sustained cyber-espionage attacks are being waged on companies that play a key role in the Britain's national infrastructure, a U.K. cyber-defense chief has warned. *ZDNet* reports that the computer systems of critical businesses in the United Kingdom, such as power companies and large financial institutions, are being repeatedly probed to steal information or uncover weaknesses that could take them down. This was the warning from Mark Oram, head of the threat and information-security knowledge department at the Center for the Protection of National Infrastructure (CPNI), the security service tasked with protecting key government and private organizations in the United Kingdom.

Speaking at the RSA Conference Europe 2008 in London, Oram said: "We see frequent attacks on organizations for the purpose of theft of property. There are known threat sponsors with known requirements looking to gather information from industry. The use of cyber-techniques is relatively easy, cheap and low risk in terms of being caught. Most of the time, we know the likely culprit but proving it is very difficult."

He added, however, that the U.K. government feels the risk of a cyber-terrorist attack is low due to a "lack of capability and difficulties with understanding the vulnerabilities in the infrastructure." Oram said the CPNI would continue to work closely with key industries to help them understand the vulnerabilities and threats they face.

Internet-warfare expert Ira Winkler, president of the Internet Security Advisors Group, said Chinese hackers are "vacuuming up the Internet for security and economic secrets". Winkler cited examples such as the Titan Rain hacking attacks.

The announcement came as the EU presented a blueprint for how European countries can strengthen national communications networks. The report from the European Network and Information Security Agency recommends prompt reaction to reported incidents, collaboration between public and private stakeholders, and development of a national strategy for information-sharing and responsibilities for different parts of the network.

In the United States, DHS's National Cybersecurity Division has tripled its budget to \$350 million over the past two years, to upgrade security systems protecting critical civilian networks and build up its US-CERT emergency-response team.