Infrastructure cyberattack fears on the rise: study

April 19 2011, by Chris Lefkow

The logo of the security software maker McAfee is displayed outside of the company's headquarters in 2010 in Santa Clara, California. Cyber threats such as Stuxnet pose an increasing risk to critical infrastructure but many facilities around the world are unprepared to face the danger, according to a report released on Tuesday that was conducted with McAfee.

Cyber threats such as Stuxnet pose an increasing risk to critical infrastructure worldwide but many facilities are unprepared to face the danger, according to a report released on Tuesday.

"We found that the adoption of security measures in important civilian industries badly trailed the increase in threats over the last year," said Stewart Baker of the Center for Strategic and International Studies (CSIS), releasing a report conducted with computer security firm McAfee.

For the report, "In the Dark: Crucial Industries Confront Cyberattacks," McAfee surveyed 200 information technology executives charged with security at power, oil, gas and water facilities in 14 countries.

"What we found is that they are not ready," the McAfee-CSIS report said. "The professionals charged with protecting these systems report that the threat has accelerated -- but the response has not."

"The fact is that most critical infrastructure systems are not designed with cybersecurity in mind, and organizations need to implement stronger network controls, to avoid being vulnerable to cyberattacks," McAfee vice president Phyllis Schneck said.

Forty percent of the critical infrastructure executives surveyed said they believed that their industry's vulnerability had increased and 30 percent said their company was not prepared for a cyberattack.

Forty percent said they expect a major cyberattack within the next year -- defined as one that causes severe loss of services for at least 24 hours, a loss of life or personal injury, or the failure of a company.

Nearly 70 percent said they frequently found malware designed to sabotage their systems and nearly half of the respondents in the electricity industry sector said they had found Stuxnet on their systems.

A top Iranian military officer last week accused the United States and Israel of being behind the computer worm designed to sabotage Iran's nuclear program.

Stuxnet targets computer control systems made by German industrial giant Siemens and commonly used to manage water supplies, oil rigs, power plants and other critical infrastructure.

Stuxnet reportedly targeted Iran's Bushehr nuclear power plant, where technical problems have been blamed for delays in getting the facility fully operational, but it also hit systems in other countries.

Eighty percent of the respondents said they have faced a large-scale denial of service attack (DDoS), in which a large number of computers are commanded to simultaneously visit a website, overwhelming its servers.

About one in four of the IT executives surveyed reported daily or weekly DDoS attacks and the same number said they have been victims of extortion through cyberattacks or threatened cyberattacks.

The 14 countries surveyed were Australia, Brazil, Britain, China, France, Germany, India, Italy, Japan, Mexico, Russia, Spain, the United Arab Emirates and the United States.

India and Mexico have the highest rate of extortion attempts with 60 percent to 80 percent of executives in those countries reporting extortion bids.

The report said Brazil, France and Mexico are lagging in their security measures, adopting only half as many as leaders China, Italy and Japan.

China was the country most recently cited as the major source of concern for government-sponsored cyber sabotage or espionage, followed by Russia, the United States, North Korea and India.

Over half of the executives surveyed said they believe that foreign governments have been involved in network probes against their domestic critical infrastructure.

To counter the growing cyber threat, the report recommended increased use of tokens and biometric identifiers instead of passwords, better encryption and network monitoring and greater oversight of connections to the Internet and mobile devices.

Citation: Infrastructure cyberattack fears on the rise: study (2011, April 19) retrieved 24 April 2024 from https://phys.org/news/2011-04-infrastructure-cyberattack.html