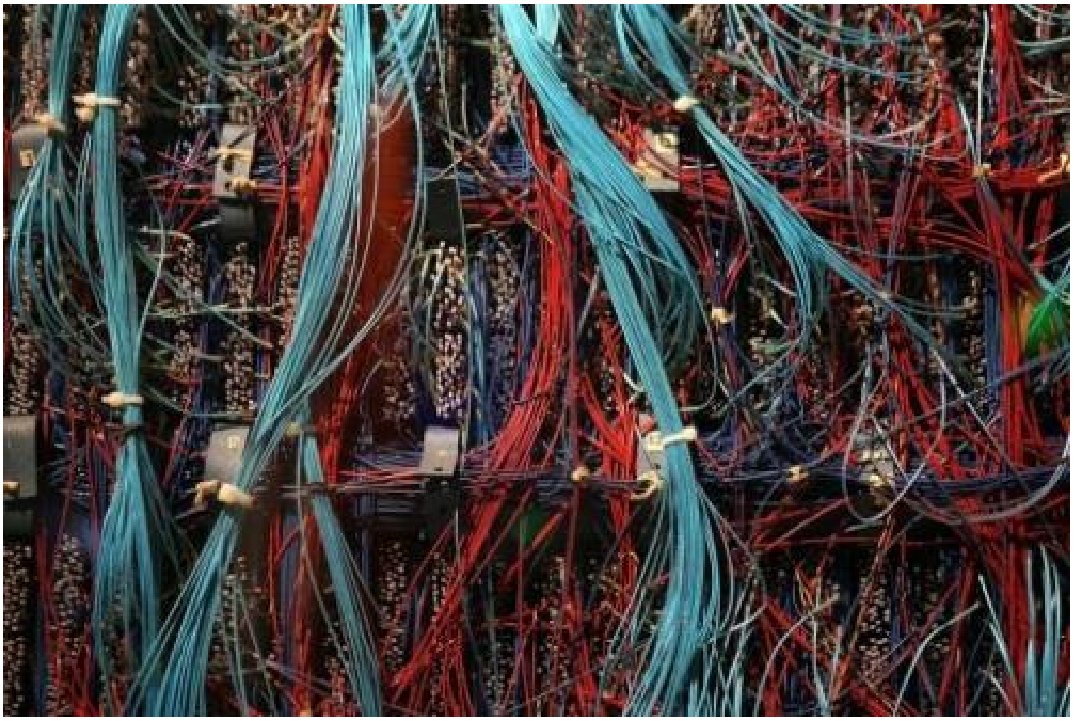
Industrial control a weak link in cybersecurity, study says

July 10 2014, by Rob Lever



Wires and switches of a supercomputer are displayed on January 19, 2011 in Mountain View, California. US military officers have endorsed the principle of pre-emptive cyber-strikes if the United States ever faces an imminent and large-scale digital attack, officials said Monday.

Cybersecurity threats are rising for industrial control systems around the world, a growing target for attackers seeking to wreak havoc, a study showed Thursday.

The study by Ponemon Institute and Unisys Corp of 599 technology executives in 13 countries found that even as threats are rising, organizations are not as prepared as they should be to deal with cyber attacks.

The study said the risk to industrial control systems "is believed to have substantially increased," with 57 percent of the respondents citing greater threats.

"Security compromises are occurring in most companies," the report said.

"It is difficult to understand why security is not a top a priority because 67 percent of respondents say their companies have had at least one security compromise that led to the loss of confidential information or disruption to operations over the last 12 months."

About one-fourth of these breaches were due to an insider attack or inadequate internal controls, the report added.

One-third of those surveyed said their companies do not get real-time alerts, or intelligence that can be used to stop or minimize the impact of a cyber attack.

And among those who they do receive such intelligence, 22 percent of respondents say this is ineffective.

The report is the latest to suggest slow progress in improving cybersecurity for so-called critical infrastructure—which includes electric power grids, utilities, oil and gas production operations and some manufacturing.

Last month, the US security firm Symantec said it identified malware targeting industrial control systems which could sabotage electric grids, power generators and pipelines.

It said the cyberattackers, probably state-sponsored, have been targeting energy operations in the United States and Europe since 2011 and were capable of causing significant damage.

According to the Ponemon-Unisys study, the majority of companies say important security countermeasures are implemented only partially or not at all.

Some said security checks fail to verify contractors, vendors and other third parties.

"People across the board recognize the problem, but as a corporate priority it is not in the top five," said Larry Ponemon, one of the authors of the study.

Unisys chief information security officer Dave Frymier said that for top executives to take notice there needs to be a "precipitating" event.

"Unfortunately it has to be something bad," such as a catastrophic attack, Frymier told a group of journalists.

Frymier said it is likely "that the bad guys are in all these networks" but have yet to take any action because they have not determined how to cash in or utilize their access.

The report is based on a survey of IT security professionals in the United States, Britain, Germany, Canada, Brazil, Australia, France, Mexico, Malaysia, the Netherlands, Spain, New Zealand and Colombia.

A high percentage of the security incidents—47 percent—came from a breach from actions of a "negligent employee," the study found.

While computer networks appeared to be the biggest target for attacks, 26 percent said attackers gained access through mobile devices.

"Hackers already have well-developed toolsets for intercepting and capturing data from mobile communications. These interception tools are growing in sophistication," the report said.

Citation: Industrial control a weak link in cybersecurity, study says (2014, July 10) retrieved 7 August 2024 from https://phys.org/news/2014-07-industrial-weak-link-cybersecurity.html