PHYS.ORG

What do you do when hackers threaten to shut down an oil platform?

August 25 2016, by Claude Olsen

No computer system is safe. How can we defend ourselves? Credit: Thinkstock

Espionage, sabotage and blackmailing threaten commercial enterprises as well as governmental agencies when all computer systems are interconnected. Countering this is complex and challenging, but possible.

The Stuxnet computer worm discovered in 2012 set alarm bells ringing in industry and public sector offices all over the world. This very advanced software worm had the ability to infect and disable industrial process control systems. The scary thing was that the worm had crept its way into many of the most common industrial control systems.

If a state or a hacker is able to spread malignant software so widely, what can we expect next?

The Internet of Things, virtually connecting everything to everyone, is rapidly proliferating to businesses, public sector offices and our homes. How can we defend ourselves against a threat when we don't know what it looks like, or where it will strike next?

Finding a defence against the unknown

Researchers at SINTEF are working to find a way of counteracting such threats. They are developing methods that will enable companies and public sector agencies to manage threats and attacks, including those that no-one has thought of.

"Society is under pressure from new threat and vulnerability patterns", says Tor Olav Grøtan, a Senior Research Scientist at SINTEF. "Standard approaches involving defence systems based on clear control procedures and responsibility are inadequate when the risk is moving around between a diversity of areas and sectors. There is an urgent need for innovative thought and new approaches", he says.

Grøtan is heading the project "New Strains of Society", which is aiming to develop new scientific theories in the field of hidden, dynamic and, what researchers call, "emergent" vulnerabilities. SINTEF's research partners are the Norwegian University of Science and Technology (NTNU), the Norwegian Defence Research Establishment (FFI), and the

University of Tulsa in the USA.

Professor Sujeet Shenoi at the University of Tulsa is closely involved. He lectures his students on "ethical hacking", with the aim of raising expertise in the US public sector to the same levels as those possessed by malicious experts and hackers.

No system is safe

For the last twenty years, Professor Shenoi has been instructing almost 400 Master's and Doctoral (PhD) students in how to hack into public and private sector networks. The students need security clearance and must undertake to work in the American public sector after they have qualified.

With the consent of the owners, the students have penetrated deep into computer systems controlling payment terminals, smart electricity meters, gas pipelines, coal mines and wind farms. They have succeeded every time.

"Someone or other, not necessarily us, has the ability to break into any computer system", says Shenoi. "We have to live with this and manage it, and that is why the concept of resilience (the dynamic ability to resist and adapt) is so important", he says.

Using Norway as a computer lab

Professor Shenoi sees Norway as an ideal location for the development of such resilience.

"Norway is one of the most digital countries in the world", he says. "With a relatively small population of 5.2 million, it can become a wholeworld laboratory. This is not easy to achieve in the USA, which is too big and too diverse", he says.

SINTEF and its partners are looking into three so-called 'threat landscapes': oil industry activity in the high north, a global pandemic, and ICT systems embedded in critical infrastructure in the oil and electrical power sectors.

A workshop was held recently with the aim of addressing vulnerabilities in the energy sector. It was attended by representatives from the Norwegian Ministry of Justice and Public Security, the Norwegian National Security Authority (NSM), the Norwegian Communications Authority (NKOM), the US National Security Agency (NSA), the Norwegian Water Resources and Energy Directorate (NVE), the Norwegian Petroleum Safety Authority, research scientists, consultants and businesses.

"We were there to test a new method of exposing unknown threats and vulnerabilities, and to prepare a stress test", says Grøtan. "People from the oil and electrical power sectors, who aren't normally thinking on the same wavelength, had the chance to work and reflect on issues together. We will apply this experience as the project progresses as part of our work to develop a stress test method designed to investigate how well an organisation is equipped to handle an unexpected situation", he says.

And the need is urgent. In 2014 Statnett and hundreds of other Norwegian energy sector companies were subject to a large-scale hacker attack. They are not alone. All sectors of society are under attack and the number of attacks increases every year. For example, Statoil intercepts 10 million spam e-mails every month. Opening an e-mail attachment is a very common way of allowing malignant software to enter a company's computer systems. Another is when careless employees give system access to subcontractors and other external parties.

Provided by SINTEF

Citation: What do you do when hackers threaten to shut down an oil platform? (2016, August 25) retrieved 26 April 2024 from https://phys.org/news/2016-08-hackers-threaten-oil-platform.html