Hackers pose a real threat against Norwegian energy providers

December 16 2015

Skotnes was surprised to discover that the network companies themselves perceived the risk as relatively low.

Consider the following:

Someone hacks into the network companies that provide electric power, shutting down their systems. This will knock out the electricity in the entire region supplied by the network company, such as Lyse Elnett in Rogaland, Agder Energi Nett in the Agder counties, or Hafslund Nett, which supplies electricity to 1.5 million people in the Oslo area.

A simultaneous attack on several network companies could affect large parts of the country. Trains would stop, planes would not be able to land, there would be no electricity, the water supply would stop and the sewerage system would break down. Hospitals have emergency generators and would manage for a while, but over a longer period of time, this would be critical for life and health.

Add a cold winter, and it would not take much imagination to visualise the effects of such an attack.

A disaster movie

"This is the worst that could happen—a worst case scenario. The consequences for society would be huge", says Ruth Østgaard Skotnes.

She is a researcher at the International Research Institute of Stavanger (IRIS) and Centre for Risk Management and Societal Safety (SEROS) at the University of Stavanger. She has recently completed a PhD in safety and security management of electric power supply networks.

You may think that this sounds like a scene from an unrealistic disaster movie. "That's not the case", says Skotnes.

"We must prepare ourselves for the improbable, and the threat to Norwegian energy providers is very much a reality."

This is according to reports from, among others, the Norwegian National

Security Authority (NSM), the Norwegian Police Security Service (PST), and the Norwegian Government's Cyber Security Strategy for Norway from 2012.

"Everything indicates that we now must expect sophisticated attacks aimed at critical societal information, including information and communication technology (ICT) systems that operate industrial processes and critical infrastructure", says Skotnes.

Vulnerable to attack

Over the past decades, modern ICT has been introduced for operation of the various parts of the electric power supply. Previously operated manually, electric power plants now control and monitor production and distribution systems from a few control centers.

Process control systems were traditionally closed systems, however increased connectivity via standard ICT technologies has made these formerly isolated ICT systems vulnerable to a set of threats and risks they have not been exposed to before.

Skotnes was therefore surprised to discover that the network companies themselves perceived this risk as relatively low, despite the fact that many of the companies had experienced attempts to hack into their process control systems. Some even reported about daily attacks from the outside.

"Many network companies put too much trust in their own systems, and take it for granted that attacks will not be successful. This contrasts strongly with what research and reports from the authorities tell us", says Skotnes.

Computer worm against a nuclear programme

Another reason may be that the network companies find it difficult to prepare for something that might happen, but hasn't happened yet. Up until now, Norway has been spared harmful cyber attacks on critical infrastructures. However, worldwide there have been several incidents of cyber attacks during the last few years.

The best known of these, Stuxnet, was discovered in 2010. This was the first known computer worm that could spy on and reprogramme industrial control systems. Among other things, Stuxnet was supposed to have been used against and damaged the Iranian nuclear programme.

The attacks on the twin towers in New York, the bombing of the Government Quarter in Oslo and the subsequent attack in Utøya on 22 July 2011 have taught us that the unthinkable can happen.

"We need to be better prepared for attacks against critical infrastructure than we currently are in Norway", says Skotnes.

Management commitment

So, how can the network companies protect themselves against cyber attacks? System updates and antivirus software are important measures, but vigilant employees and management commitment are just as important, according to Skotnes.

Last year, around 50 companies in the oil and energy sector were exposed to the biggest cyber attack in Norway's history. In Statnett, the transmission system operator in Norway, the attempt was discovered by a vigilant employee, which meant that the company was able to prevent malicious software from being installed or run on computers within the company.

"My study showed a strong relationship between management commitment to ICT safety and security, and the implementation of awareness creation and training measures for ICT safety and security in the network companies. I was told that it was difficult to implement measures if the management was not committed to the issue", says Skotnes.

Involving the employees in the development of ICT safety and security measures can be a useful way to raise awareness in the network companies. This can make it easier for the employees to realize the benefits of these safety and security measures, and not consider practicality and efficiency as far more important for their work.

Subculture

Her thesis shows that there exists at least two different subcultures in today's network companies, depending on whether the people operating the process control systems have an education in ICT or a background from the electricity industry. The latter group generally focus on keeping the systems running without interruption. Downtime is not acceptable, and the most important thing for this group is constant supply of electricity.

"Supply reliability is important, but this way of thinking has to change so that everyone understands how crucial ICT safety and security is", says Skotnes.

A critical point

Power production in Norway is more difficult to affect. Ruth Østgaard

Skotnes chose to concentrate on power distribution because this is considered to be most critical for societal safety.

She collected data for her thesis through a survey questionnaire that she sent to all the 137 network companies operating in Norway in 2012. Skotnes also interviewed representatives from the contingency planning department in the Norwegian Water Resources and Energy Directorate (NVE) who are responsible for safety, security, contingency planning and supervision in the Norwegian electric power supply sector.

By 2019, smart meters (Advanced Metering Infrastructure) will be installed in all Norwegian households. Smart meters will provide increased capacity, reliability and efficiency of electric power supply, but will also increase the vulnerability to cyber attacks.

"Society's vulnerability will increase because the number of possible entry points and paths for attacks are continually increasing. This is why we as a society need to take such threats seriously", says Skotnes.

More information: Ruth Østgaard Skotnes: Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector. Doctoral thesis, the Faculty of Social Science at the University of Stavanger, 2015

Provided by University of Stavanger

Citation: Hackers pose a real threat against Norwegian energy providers (2015, December 16) retrieved 26 April 2024 from https://phys.org/news/2015-12-hackers-pose-real-threat-norwegian.html