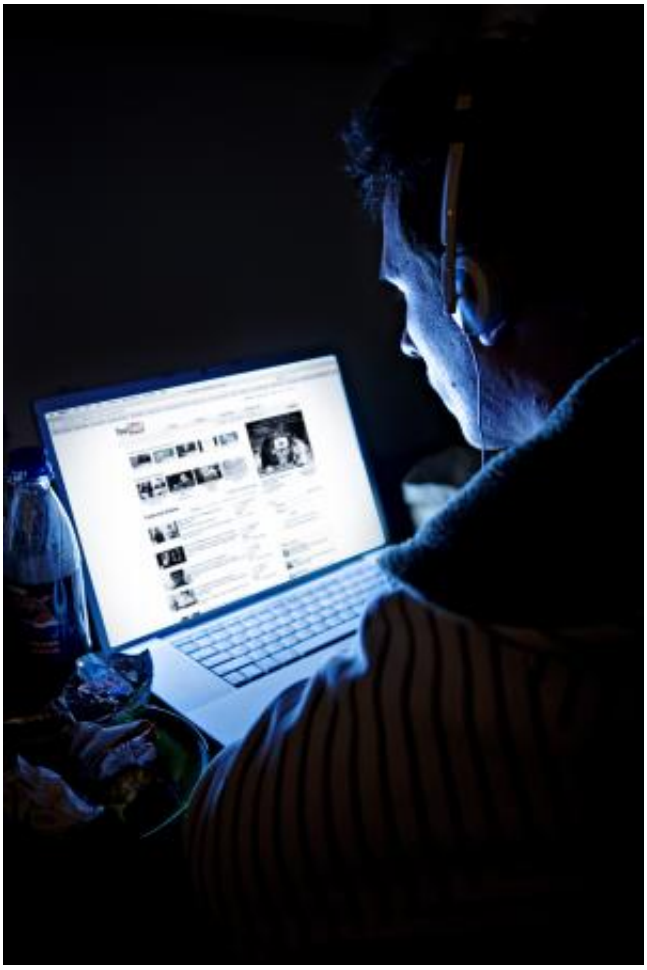
Power companies unprepared for hacking attacks

March 19 2015



In spite of impending threats of malicious hackers putting the lights out all over Norway, Norwegian power companies seem to be taking a very laid back approach. Credit: SINTEF

Researchers are recommending that Norwegian power distribution companies should carry out more regular contingency exercises to prepare themselves for hacking attacks. If they don't, they won't be equipped to identify and deal with crisis situations.

A number of attacks have already been made on energy and distribution companies worldwide. Last summer the Norwegian power industry was victim to its first attack – which certainly made the distribution companies sit up and think.

However, in spite of impending threats of malicious hackers putting the lights out all over Norway, Norwegian power companies seem to be taking a very laid back approach.

Three exercises

"The introduction of SmartGrid comes with great visions of grandeur, but the major investments and technological changes involved also entail enhanced vulnerability", says Maria Line at SINTEF/NTNU. "The companies will soon have to wake up to what's happening", she says.

Together with SINTEF researcher Nils Brede Moe, she has recently acted as an observer of IT contingency exercises at three different power distribution companies, all of which were carrying out an exercise for the very first time. The impressions obtained by the researchers have resulted in a set of recommendations.

Everyone takes part

One of the main recommendations is that all those who will have a role during a real incident, including managers and IT system suppliers, should take part in the exercises.

"Getting top management to participate in exercises has always been a problem. These are busy people with little time to spare", says Moe. "At the same time their continued absence is far from ideal because they will undoubtedly be involved if a real situation arises", he says.

"One of the companies we talked to had an agreement simply to call and rely on its supplier if a crisis occurred", says Line. "And even then, the supplier didn't take part in the exercise", she says.

She explains that IT security is commonly dismissed as the realm of the IT Department. But of course, if a hacking attack takes place, it will have major implications for the commercial aspects of a company. "At some time or other, the sensible option may be to close down the system in order to limit the negative consequences of an attack, and it's vital that both technical specialists and decision-makers are in very close contact during discussions about decisions of this type", she says.

Many scenarios

It isn't easy rehearsing something you know nothing about. The nature of crisis situations can vary so much that it's essential to train with flexibility in mind.

The scenario that formed the basis of this study involved an incident that evolved in five stages. It started with the identification of abnormally high levels of IT traffic from the office network out onto the internet. Two weeks later, the company was contacted by its supplier of the control systems that regulate power distribution to its customers. Contact was made in an unusual way, requesting the company to install a security update.

Three months later a power cut occurred in a residential area without activation of the control system alarm. In the period that followed,

notifications were received of several power cuts in different areas. During the final phase, both the mobile network and the internet had shut down.

"Employees are faced with the clear challenge of being able to see the connections between incidents that take place over an extended period", says Moe. "It's essential for them to carry out exercises in order to realise that such things CAN happen", he says.

Reporting and information sharing are essential in order to see the connections between isolated incidents that over time can result in a crisis situation.

"The worst thing the companies can do is to continuously repeat exercises of just a few scenarios, or not perform exercises at all", says Line. "Each scenario should only be practised once, otherwise its usefulness becomes very limited. For this reason new scenarios have to be developed all the time", she says.

Coordination in action

The researchers emphasise that their recommendations are food for thought for the future. First and foremost, it's essential to carry out the exercises. This is more important than getting things right all the time.

The most important thing of all, they say, is to carry out exercises together and to do so often. This will ensure that everyone involved can coordinate their roles effectively. In order to take effective decisions, it's important to have all the facts, and the right facts, at hand. This is why everyone involved must take part in the exercises.

Provided by SINTEF