Unheeded cybersecurity threat leaves nuclear power stations open to attack

October 19 2015, by Nasser Abouzakhar

Credit: Steag/VGB Power Tech GmbH, CC BY-SA

There has been a rising number of security breaches at nuclear power plants over the past few years, according to a new Chatham House report which highlights how important systems at plants were not properly secured or isolated from the internet.

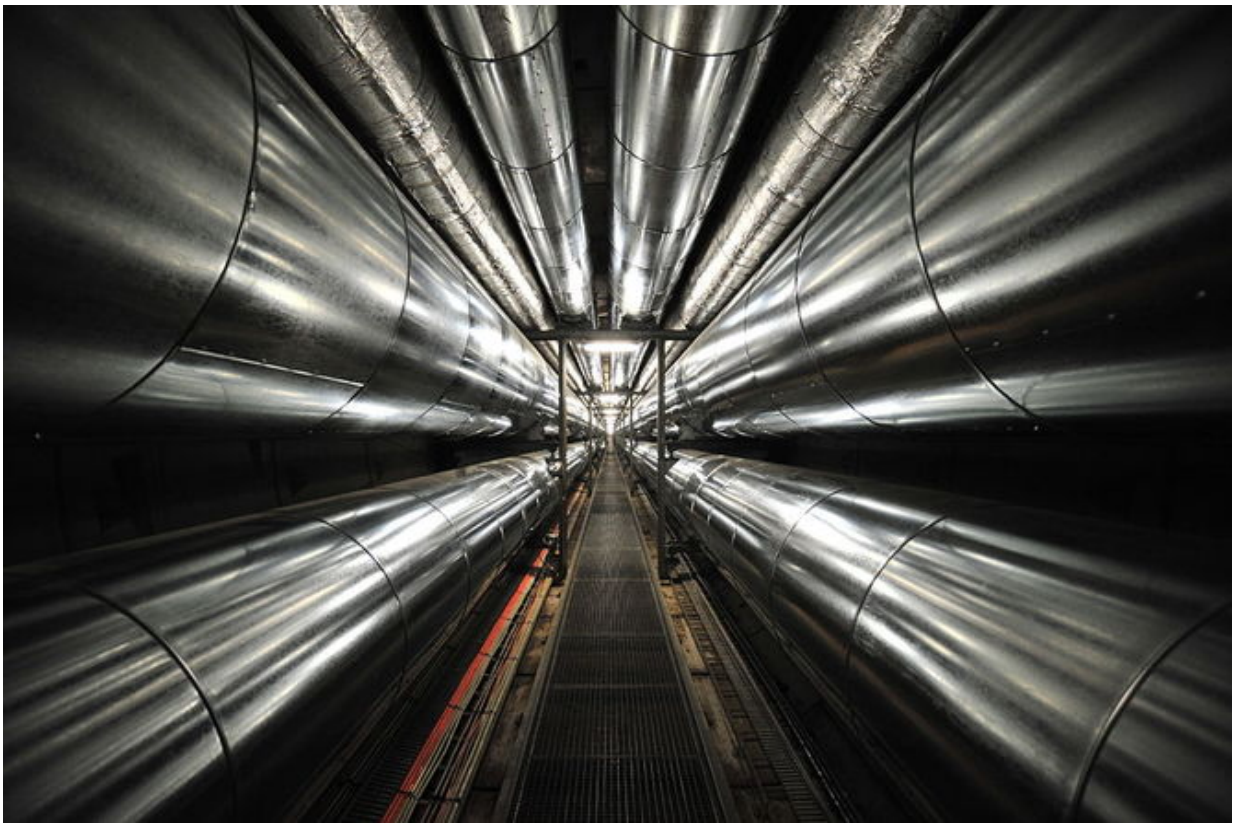
As critical infrastructure and facilities such as power plants become increasingly complex they are, directly or indirectly, linked to the

internet. This opens up a channel through which malicious hackers can launch attacks – potentially with extremely serious consequences. For example, a poorly secured steel mill in Germany was seriously damaged after being hacked, causing substantial harm to blast furnaces after the computer controls failed to shut them down. The notorious malware, the Stuxnet worm, was specifically developed to target nuclear facilities.

The report also found that power plants rarely employ an "air gap" (where critical systems are entirely disconnected from networks) as the commercial and practical benefits of using the internet too often trump security.

In one case in 2003, an engineer at the Davis-Besse plant in Ohio used a virtual private network connection to access the plant from his home. While the connection was encrypted, his home computer was infected with the Slammer worm which infected the nuclear plant's computers, causing a key safety control system to fail. A more serious incident in 2006 at the Browns Ferry plant in Alabama nearly led to a meltdown.

The report also found that there is a general lack of knowledge of cybersecurity on the part of management who have generally shown a poor understanding of good "IT hygiene" and how it relates to security. It was quite common, the report said, for factory default passwords to be left unaltered and off-the-shelf software to be used despite known issues that were left unaddressed.



There’s a lot of civil infrastructure, and a lot of it is vulnerable. Credit: Bill Ebbesen, CC BY

The problem is that the industrial communication protocols and mechanisms still commonly used in nuclear power plants were designed in an era before the internet and cyber-threats were a consideration. These are often insecure and not designed to deal with such challenges. Most of the legacy communication protocols such as Profibus, DNP3 and OPC are still vulnerable to various attacks as they lack any proper authentication techniques.

This means that all a malicious hacker might need to get inside a nuclear power station's network is Google. Using search terms relevant to the software in use in the plant, Google can turn up direct links to websites

leading into its network – with little or no security in the way.

An example of this is the technique used to hack internet-connected webcams. Searching for text used in the webcam login page, Google will turn up links to cameras all over the world. Many users fail to change the default username and password (which are easily found online), meaning that the cameras can be accessed and controlled with ease.

The same sort of techniques can be used to locate, not webcams, but web-connected industrial devices potentially providing access to important facilities. Search engines such as Shodan can identify these sorts of devices and even use geo-location to pin down their physical location.

Mind the gaps

Unauthorised access by hackers to important systems in a power plant is a serious matter: anything that damages or disturbs the balance of operations within the plant could lead to a shutdown or even dangerous situations when shutdown routines fail, while power surges within the plant could affect transmission infrastructure outside. Whether we are talking about a nuclear power plant or not, the end result is likely to be production failures or financial losses, or even injury and death in. Of course, with a nuclear power plant the risks are that much greater because of the radioactive fuel in use.

Managing cybersecurity risks is challenging – and the Chatham House report makes several recommendations: integrated risk assessments to ensure security measures are properly implemented, and penetration testing where experts attempt to pry into and circumvent security measures, to ensure that the plant's staff find any security holes before hackers do.

Organisations need to be far more aware of the potential effects of

attacks: what could happen if various control systems were used incorrectly. This way it will become more apparent where resources should be dedicated towards protecting them. Only rigorous research and testing will develop the security approaches and technologies needed to respond to this quickly-evolving cybersecurity threat, keeping the power stations running and the lights on.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation