Vital infrastructures in the Netherlands vulnerable to hackers

5 August 2019

Credit: CC0 Public Domain

Don't treat vital infrastructures in the same way one would protect a shop network, for instance, but bind them to a secure circuit that hackers cannot breach. This is one of the central recommendations in a comprehensive report entitled "Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands," based on research carried out by the University of Twente on behalf of the Scientific Research and Documentation Centre (WODC) of the Dutch Ministry of Justice and Security.

Forget the classic terrorist attack: today's newest threats come from hackers and are directed at power stations, hospitals, bridges, waterway locks and nuclear reactors. In recent years, every large international conference on cyber security has been saying the same thing. "We've spent a great deal of money on digital resilience, but it's not been working well enough. We're not winning," said Alex Dewdney, director of cybersecurity for UK intelligence services, recently.

Hackers

Are these concerns justified? Can hackers really shut down hospitals and power stations? "Definitely," says Aiko Pras, professor of internet security at the University of Twente. "There have been several comparable cases in recent years. Remember the incident in Ukraine? The east of the country was hit by a blackout that affected hundreds of thousands of people. Research showed that hackers were responsible, possibly from Russia."

The Dutch government is also taking this kind of threat seriously. Pras and his research team in Twente won a call by the Dutch government to examine vital infrastructures in the Netherlands.

"First of all we looked at whether anyone with a computer could access those sorts of vital systems in the Netherlands, of which there are about a thousand. Then we examined how many of those systems were also vulnerable—that is, which software versions they were running and how hackable they were. We found that 60 vital systems had more than one weak point and could be hacked. These were mostly relatively small systems used for control purposes; we don't know exactly what was behind them."

What Does This Mean?

In their report, Pras and his colleagues give two interpretations of this discovery. "Firstly, it's shocking. Suppose one or more of those sixty control systems was responsible for something really important, like a lock gate or a power station? At the other extreme, however, all sixty systems may have been intended to attract potential attackers: they may have been 'honeypots,' designed to protect a system by luring its attackers into a trap. This is normal practice in the cybersecurity world. Whatever the case, we're sharing our findings with the owners of these vital infrastructures."

Political Choice

For Pras, however, the most important outcome of the report is to stimulate political debate on cybersecurity for vital infrastructures in the Netherlands. "In our view, the government should say: vital systems should not be connected to an open, public internet so that malicious, possibly foreign hackers can get in. For some time now, we've seen that the Dutch government has a rather weak grasp of ICT. Only a few politicians really understand the issue, and the decision-making process is slow."

Pras argues for a 'dedicated section of internet that can be managed separately." "Nothing like this exists in the Netherlands as yet. Everything is uniform, with a few different providers who generally treat all their customers in the same way. A closed network structure would need a political decision to be taken first, and that's exactly the debate we would like to see being catalysed by this report."

Provided by University of Twente