Cybercriminals are now targeting critical electricity infrastructure

June 5 2020, by Henri Van Soest

Credit: Yuting Gao from Pexels

Amid the constant stream of news on the coronavirus pandemic, one event passed relatively unnoticed. On the afternoon of May 14, a company named Elexon was hacked. You probably haven't heard of it, but Elexon plays a key role in the UK's electricity market, and though the attack did not affect the electricity supply itself, as an academic who researches cybersecurity in the electricity system, I am worried. This

near miss reveals just how vulnerable our critical infrastructure is to such attacks—especially during a pandemic.

Elexon plays an important role in the operation of the country's electricity system. In such a system, the levels of supply and demand need to be balanced at all times. Otherwise, the system becomes unstable, which can lead to blackouts. To avoid this, Elexon compares the amount of electricity that generators promise they will produce, with the amount of electricity that suppliers say will be consumed. Where needed, the company determines the difference in price and transfers funds between the parties on either side of the transaction.

The lockdown has made Elexon's role significantly more difficult. Usually, electricity demand is pretty fixed, as people broadly go to work, return home, cook dinner and watch TV at roughly the same hour every day. However, the lockdown has ripped up the rule book on all this. Despite many people staying at home, electricity demand has also dropped by about 20% compared to this time last year due to the closure of factories and businesses. In sum, it is a lot harder to correctly predict demand.

The drop in demand also means that less electricity is needed. The drop in demand also means that less electricity is needed. Because wind and solar power are now the cheapest forms of electricity available, coal and gas plants are generating less, and there has lately been a big increase in renewable energy sources in the overall mix. However, wind and solar power experience large swings in supply, depending on whether the sun shines and the wind blows. This again makes supply and demand more complicated to manage.

Held to ransom

The Elexon attack used ransomware, in which a computer virus encrypts

the contents of a computer, and it can only be decrypted after a ransom has been paid, typically in bitcoin or another cryptocurrency. The most famous ransomware attack is no doubt the 2017 WannaCry attack, which particularly affected the UK's National Health Service.

Several reports indicate that the Elexon attack relied on REvil/Sodinokibi ransomware, the same as was used in a cyberattack on financial company Travelex on New Year's Eve 2019. The Travelex hack was traced back to a Russian hacking collective, and although it is notoriously difficult to attribute cyberattacks with certainty, it is likely that Elexon fell victim to the same hackers. On June 1, the hackers posted some of the stolen Elexon data online, in an attempt to pressure the company to pay the ransom.

A cybercrime pandemic

The attack on Elexon does not stand alone. As countries around the world have locked down, cybercriminals have launched attacks on a wide range of targets, mostly using ransomware. The lockdown-induced rise in home-working has been a big enabling factor, as lots of professional communication now takes place over the general internet, which is a lot more insecure than using a local company network with a firewall around it.

Critical infrastructures have been hit particularly hard. In recent months, cyberattacks have been launched on hospitals, coronavirus research facilities, ports, water supply infrastructure, and the Brussels-based ENTSO-E, the European Network of Transmission System Operators for Electricity.

This sort of infrastructure is in the crosshairs for two main reasons. First, cybercriminals bet that operators will be less hesitant to pay ransom than other targets, because the continued operation of electricity, water,

hospitals and so on is so important.

But it's also because their computer systems are often outdated. While it may seem paradoxical, the reason for this is the fact that critical infrastructures should always be available. When a system works fine, there is little incentive to change it, especially when changes to computer systems can easily lead to incompatibilities, errors or crashes. For instance, three years after the WannaCry attack, the NHS is once again exposed to an attack because many of its computers are still running on Windows 7, which is no longer supported.

Ransomware attacks are typically not very complicated. They make use of known software vulnerabilities that have already been patched, and the criminals specifically target those computers that have not been updated. These inherent vulnerabilities, combined with the lockdown-induced difficulties in balancing the electricity grid, mean that a more sophisticated cyberattack on Elexon could have had big consequences for the UK electricity system.

As it happens, the attack only affected Elexon's internal IT systems, and the rest of the electricity system, as well as the electricity supply itself, was not affected. But this should force us to think about how vulnerable our critical infrastructure is to cyberattacks.

What would have happened if the attack had indeed affected the electricity supply? It would have seriously hindered the UK's response to the pandemic, and it is possible that we would have struggled to get the power back up, as all resources are currently going into fighting the virus. In addition, it is unlikely that a lockdown without electricity and internet could be maintained for long. The fact that cybercriminals know this only makes our critical infrastructures more appealing targets.

Commons license. Read the original article.

Provided by The Conversation