Presented by HIROC

BRIT

writing the future

cyber-attacks and the risk to critical infrastructure

Cyber-attacks are of increasing concern

All too frequently, a new cyber breach story hits the headlines and makes us contemplate the possible consequences. Cyber-attacks are of increasing concern for operators of critical national infrastructure. Power plants, emergency services and transport systems are all attractive targets to hackers looking to hold data to ransom or disrupt services and systems.

With the pandemic prompting a shift towards more remote working, the need to maintain the highest levels of cyber security has never been greater. Last year, Dr Jessica Barker, Co-CEO and Head of Socio-Technical Security at Cygenta, discussed critical infrastructure risk in our newsletter. Now, we're revisiting the topic as new threats emerge in cyber security.

The risk of running legacy systems

In February 2021, cybercriminals attempted to poison the water supply in Florida, USA. They did so by trying to raise the sodium hydroxide content to more than 100 times its normal level, threatening human health. This attack represents a very challenging and vital area of cyber security: preventing and responding to attacks that cross the digital boundary into the physical space, to have lasting effects in the real world. The opportunity for cybercriminals is clear. As industrial systems become more standardised and are integrated more into office spaces (to provide data, safety, and remote access), those systems become part of a larger interconnected space. This is an attractive, and growing, target for criminals looking for weaknesses to exploit. Water filtration plants are part of Critical National Infrastructure systems that governments protect because the failure of one of those systems can have a devastating impact on a country and its citizens.

So how, in February 2021, did cybercriminals manage to access Florida's water filtration systems – not just once but twice – on a sunny Friday? The criminals gained access via old and unused software called TeamViewer, which allows the system's operators to connect remotely to the control computers to monitor and make changes if needed. The software was no longer used by the Florida water department but had not been removed from the computers. This kind of technical legacy is a weakness for many organisations: dormant or out-of-date and unused software is one of the largest vectors of system compromise that we see. Many companies move providers or change their ways of working – and clean-up of old software is often postponed or forgotten about.

Refreshing old systems

In many cases, these legacy systems that support old software could be removed without any impact on the business, other than reducing the threat landscape and increasing the security. Software and security move at an incredibly rapid rate; unfortunately, so do criminals. Locating and shutting down old software narrows the field of scope that attackers can leverage to gain access to your company. Further still, this is not the first time that attackers have targeted a water facility.

Further problems around the world

In April 2020, Israeli water facilities were targeted in a similar way, so much so that the Israel National Cyber Directorate is working with the FBI on the Florida case to help the US track the attackers. It was the preparedness of the local authorities that thwarted the hostile action in Florida: a worker at the treatment facility spotted the attack as it was happening and reversed the action. We can all learn

continued

from this case and heed the warnings about merging our physical and digital spaces, the need to take care of technical legacy, and the importance of being prepared for attacks – alongside preventing them in the first place.

Healthcare disruption

Beyond water facilities, there are other areas of critical infrastructure that have been left vulnerable to instances of cyber-attacks. One such instance came in May 2021 when the National Health Service of Ireland (HSE) was hit by Conti ransomware. It was found that 80% of the IT infrastructure was affected with the hackers demanding a payment of $20m worth of Bitcoin. The hack had a detrimental effect on services as vast amounts of patient data was stolen. The knock-on effect led to all areas of health services being affected, with appointments being canceled and treatments for seriously ill people being delayed.

In an unusual move, the criminal gang who initiated the hack were reported to have given the HSE access to a tool to allow it to recover the stolen data. This might have fallen into a flimsy code of ethics used by some hackers to ensure people don't come to any physical harm as a result of their clandestine activities. The Irish Health Service were naturally very wary of using software by the very hackers who'd comprised their systems. Taoiseach Micheál Martin was insistent that while access to the tool was useful, an enormous amount of work was required to rebuild the overall system.

Disruption of food supply

Beyond the world of healthcare, some ransomware attacks have affected the production and distribution of food. JBS Foods, one of the largest suppliers of meat in the world had its operations severely disrupted by a cyber attack in June 2021. The hackers were able to disrupt internal systems that led to all of the company's food plants in the USA temporarily closing, along with a further plant in Canada and beef and lamb production sites as far afield as Australia. The attack successfully ransomed JBS Food for some $11 million to bring their operations back online. Even a day's worth of disruption has the potential to affect the supply of food and drive up prices.

Looking ahead to a safer future

For many years, the UK National Cyber Security Centre has been warning that the UK will experience a Category One national cyber emergency, for example damaging infrastructure. Authorities prepare for these scenarios on the basis of 'it's not a matter of if, but when' – and this kind of approach can be beneficial for private organisations, too. Prevention and protection will always be a fundamental element of cyber security, but preparation and response are just as vital: be alert to attacks and know what to do if – or when – the worst happens.

Understanding the threat landscape for critical infrastructure is vital. As we have advanced in our capabilities to manage these systems, so have the opportunities for exploitation and vulnerability. Our knowledge of the cyber landscape gives us a deeper understanding of the different types of risk, you can find out more on our cyber page, here!