RANSOMWARE AND INDUSTRIAL CONTROL SYSTEMS

Chris van den Hooven from Hudson Cybertec explains how organisations can protect themselves against ransomware attacks

ON 7 MAY 2021 a ransomware attack took down the Colonial Pipeline infrastructure. Ransomware is a form of malicious software designed to encrypt files on a device, rendering any files and the computer systems that rely on them unusable. Attackers then demand ransom in exchange for decryption. In the case of Colonial Pipeline the attackers demanded a ransom of about US$5 million (€4.3 million).

The impact of the attack on the largest gasoline pipeline in the US was enormous. Colonial had to shut down the operations and within a day fuel shortages hit Charlotte Douglas International Airport and filling stations in Alabama, Florida, Georgia, North Carolina, and South Carolina. The restart of the pipeline operations began on 12 May and operations had returned to normal on the 15 May. Vehicle fuel supplies took some time to return to normal.

THE INCREASING RANSOMWARE PROBLEM

A ransomware attack is possible on any type of IT infrastructure. There have been many successful attacks on all kind of organisations. One of the most recent attacks took place on Kaseya, a company providing management and security software to managed service providers (MSPs). The MSPs provide IT management services to their customers. By attacking Kaseya, the attackers ended up in affecting more than 1,500 organisations.

The 'business model' of such attackers is proven to be very successful. The 'market' has become very professionalised and organised. Chainanalysis estimated that US$350 million in ransom payments were made in 2020. The ransomware groups apparently invested in even better attack tools. There are specialised criminal groups working together. Groups writing the malicious software, groups using this software against their targets, groups laundering the money, etc. In 2015 cybercrime already was more profitable than the drug trade.

A common reaction to a ransomware attack is to restore the systems from the backup. The attackers anticipated in two ways: encrypting the backups as well, and introducing the 'double extortion'. Double extortion was a new approach among ransomware groups in 2020. In this situation, data is exfiltrated to the attacker, before the ransomware software encrypts the attacked system. The attacker will threaten to leak or auction off company secrets.

PROTECTING AN ICS AGAINST RANSOMWARE

A ransomware attack can be successful against an industrial control system (ICS), but most of the attacks are targeted to business systems. However, even attacks against business systems will have an impact on the plant. In case of the Colonial Pipeline attack, cybersecurity reporter Kim Zetter suggested hackers specifically had access to the company's billing system, rather than direct control over the pipeline itself.

In its publication *Threat landscape for industrial automation systems - Statistics for H2 2020*, security firm Kaspersky published a percentage of ICS computers on which malicious software was found (and blocked). For the oil and gas industry it was an alarming 44%.

Ransomware threats for ICS are growing. In June 2021, the Cybersecurity and Infrastructure Security Agency (CISA)

released a fact sheet highlighting the ransomware threats in 2021 in relation to operational technology (OT) assets and ICS.

'Given the importance of critical infrastructure to national security and America's way of life, accessible OT assets are an attractive target for malicious cyber actors,' says CISA.

Obviously, this statement is true for many parts of the world, including Europe.

GOVERNMENTS ARE RESPONDING

In reaction to the increasing ransomware problem the US Transportation Security Administration (TSA) on 20 July 2021 issued a second security directive meant to strengthen critical pipelines against cyberattacks. In Europe there is a proposal for a revised directive on the Security of Network and Information Systems (NIS2 Directive). The NIS2 applies to many essential entities, including tank storage of oil.

Another way governments seem to respond is to attack the attackers. In case of the Colonial Pipeline US law enforcement agents successfully retrieved roughly US$2.3 million of the ransom paid. In the case of the attack on Kaseya, the ransomware group behind this attack, called REvil, seems to have vanished. The reason behind this is unknown, but the common belief is that some government forced them to disappear.

Ransomware has also become a diplomatic issue for the US, because the perpetrators of the attacks often appear to reside in countries unwilling to extradite them to the US, like Russia or North Korea. US President Joe Biden urged his Russian counterpart Vladimir Putin to 'take action to disrupt' online criminal organisations in Russia. The EU and its member states have expressed their solidarity with the US on the impact of malicious cyber activities which the US believes have been conducted by groups operating in Russia.

PROTECTING AGAINST RANSOMWARE

In order to protect an organisation, it is important to understand how a ransomware attack usually takes place. A successful cyber attack, including a ransomware attack, requires several steps. The cyber security specialists of Lockheed Martin were the first to describe these steps as The Cyber Kill Chain. The steps are similar to the steps a common burglar might take if he wanted to steal or damage goods from a big office building:

1. Learn as much as possible from the security measures in place. How do employees enter the building? Do they need badges? Is there a back door?
2. Find a way in. This could be sneaking in during broad daylight by just mingling with the employees coming back from their lunch break.
3. Organise access on demand. This could be stealing a company badge or stealing keys from a back door, by which the attacker can get access any time he wants.
4. Once in, find the room with the valuable goods. This might take some trial and error.
5. Once found, steal or damage the goods the burglar was looking for.

To prevent a scenario like this, organisations have all kinds of measures in place. Guards might notice if someone is observing the property. Badges and mantraps ensure no one without a badge can enter. Strict procedures for managing keys make it harder to steal them. A closed-circuit security camera system makes it difficult to wander around in the building unnoticed.

Preventing a successful cyber attack, including a ransomware attack, requires the cyber equivalent of these measures. One might keep an eye on the internet (including the hidden darknet) and notice the company is discussed as a potential target. Enforcing strong authentication for network access makes it harder to find a way in and makes it harder to steal a password. Segmenting the network makes it more difficult to get access to the most valuable systems. Monitoring the network and investigating any unusual behaviour makes it harder for an attacker to remain unnoticed.

WHERE TO START

The attacker has an advantage, needing only one loophole, while the defender must have everything in order. History has shown that this is next to impossible.

While preventing an attack is very hard, detecting an ongoing attack is often very well possible. It takes time, sometimes months, for an attacker to reach his goal. Every security measure will impose a delay. Once enough barriers (network segmenting, strong authentication, etc.) and monitoring are in place it becomes next to impossible for an attacker to remain unnoticed. The advantage will shift away from the attacker and performing a successful attack becomes much harder. The value of monitoring is one of the reasons Hudson Cybertec developed OT Insight, a network monitoring and compliance solution.

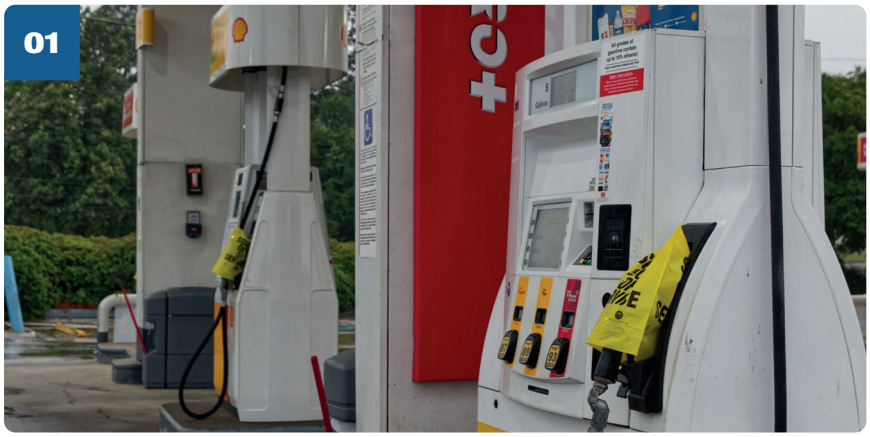
The IEC 62443 is a series of standards for protection industrial automation and control systems (IACS). This IEC 62443-2-1 describes how to establish an industrial automation and control system security programme. This standard describes three basic steps for the security programme: risk analysis, addressing risk, and monitoring and improving the programme. The various other parts focus on the development of secure components, how to perform risk analysis and building and managing IACS in a secure manner.

Applying this standard ensures a structured way in improving the cyber security of any IACS system. It will result in enough barriers to stop or slow down an attacker and monitoring to detect malicious activities.

For more information:

This article was written by Chris van den Hooven, senior cyber security consultant at Hudson Cybertec.

www.hudsoncybertec.com/tsm



01 Filling station in Georgia out of fuel with yellow bags on pumps during the Colonial Pipeline outage