Are you cyber secure?

In our latest feature on cyber security, Ever van de Weg examines how companies within the can making business are looking to become more security conscious when it comes to its IT

Computers have brought us an almost unimaginable wealth of blessings in the last 50 years. However, we all also recognise the very uncomfortable feeling when we discover our computer was hacked and we cannot reach important files.

In the world of big business, similar things are happening frequently. In fact, since the 1980s the attacks are become smarter and more devastating. Hacker groups have succeeded in penetrating huge networks of large international companies. Companies like Yahoo, CNN, but also e-commerce companies like eBay, Dell and Amazon have been brought to a complete standstill, causing considerable financial damage. In recent years the scale and the robustness of cyber attacks have increased rapidly.

In its 2018 report, the World Economic Forum observed: "Offensive cyber capabilities are developing more rapidly than our ability to deal with hostile incidents."

An often used weapon are the DoS attacks, during which huge amounts of data are sent to servers, resulting in servers getting stuck. Hackers try to make companies that they are attacking pay ransomware payments in return for lifting their blockades.

A clear example how damaging a cyberattack can be is the recent attack aluminium producer Norsk Hydro in Norway had to cope with. The extensive ransomware attack was accompanied by a ransom demand from the hackers. From the very beginning the Norsk Hydro management made clear they did not intend to pay the hackers' ransom demand and the company's IT experts restored step by step the functions to ensure stable production, to serve customers and to limit financial impact. The company had to temporarily move to manual operations.

The aforementioned case is typical in relation to the financial motives of attackers. Lesser known are attacks relating to operation ▷

technology, motivated by confiscating IP or by sabotage. A large game changer in this field was the Stuxnet attack to the Iranian nuclear plant Natanz. The Stuxnet computer worm compromised the industrial controllers brought by an insider with a USB stick. This malicious exploit was installed and caused substantial damage to the equipment.

CYBER SECURITY IN CAN MAKING

As companies worldwide have become aware of the huge risks cyber attacks present to them, specialised organisations that are able to advise how to cope with these threats have developed over the last few decades. The company aXite, based in The Hague, The Netherlands, is one such company.

Managing director Bert Willemsen, in the past sales director in the can making business at Continental Can Europe and Impress, founded this company in 2013 and has gathered a number of cyber specialists with many years of experience around him. Over the years he and his team have built a cyber security practice in operational technology and integrated control systems (ICS) for the industry.

In September 2019 Bert Willemsen was keynote speaker at a global cyber security conference in Amsterdam for the oil and gas industry.

"Of course cyber crime has become a worldwide threat against large, medium and small businesses in the can making industry," explains Willemson. "Losses of privacy and confidential data, losses of direct income and operational standstills are lurking around in the high density of digital systems and equipment at production facilities. Cybersecurity is a serious matter, and the hype around this complex subject makes a practical industrial solution necessary for can manufacturers and fillers."

Industrial control systems are used to monitor and control various systems such as can making or can filling production lines, heat ventilation air conditioning, and utility metering. Supervisory control and data acquisition, operation control systems (SCADA), process control, industrial automation, and energy management systems are all categories of industrial control systems that meet specific needs. Manufacturing sites are using different industrial control system devices.

"These types of devices increasingly rely on computer and network technology to collect data, analyse the information received, and react with corrective action," Willemson says. "Industrial control systems are also becoming increasingly interconnected and interdependent with other information systems, such as budget IOT devices to measure processes performance and share data with management , which may introduce additional risks.

"Due to this interconnectivity, these devices are exposed to similar vulnerabilities as computers and network devices. Security through the lack of external connectivity, the so-called 'air gap', is disappearing as more and more devices and sensors are being connected to the internet to generate and share data.

"In addition, insider threat, physical access or access through trusted ports creates a vulnerable environment for cybercrime, and thus a threat to business continuity."

IN PRACTICE

We asked some companies in the can making mar-

ket about their experiences around cyberattacks and their protection they have undertaken. Mark Veron, head of Technological Engineering and Development of Canline, explained its approach:

“We ourselves have had no spectacular experiences so far,” he says. “We have protected ourselves with the normal security procedures and we have not had to deal with hackers so far. Every night our systems make a back-up of all the relevant digital data that were exchanged during the day.

“One month ago a supplier of ours did have a serious problem when hackers activated ransomware on their servers and their whole company had serious trouble in its production. Only after the company paid thousands of Euros, the blockade was lifted. It is a lesson for us how important it is to keep a sharp eye on cyber security.”

Another company we asked about possible experiences in the field of cyber security was the Swiss company Can Man.

Sales manager Marianne Umbricht was kind enough, after talking to her brother and managing director Rudi Umbricht, to tell about the experiences of Can Man.

Marianne Umbricht takes up the narrative: “We foresee for our company very limited risks and we do not have any negative experience so far fortunately.

“Within our company we take the same protective measures as you take for your own personal computers, namely to use safe internet standards, firewalls, passwords and so on.

Most importantly, all our equipment is built in a way that no moving parts can be started or stopped online over the internet, this means a machine cannot be started without being physically in front of the machine. All moving parts on our machines are started and stopped physically rather than pushing buttons to avoid the risk of injuries.

“What could be done online is to change the production speed; this is for sure not nice and can harm the production, but on the other hand we have independent units which monitor the process.

“Independent units means that they are not controlled over the same login and password. So any change which is done unplanned will automatically either lead to a crash, so a production stop or to a mass-ejection of the can bodies. A ghost-change which nobody recognises is not possible.”

Managing director Jörg Höppner of the German organisation of metal packaging producers Verband Metallverpackungen in Düsseldorf, confirms that cybersecurity is often high on the agenda in meetings of the members.

“We discussed what happens when the customers of our can producing members have direct access to their order entry systems to order a certain quantity of cans, barrels, closures or so,” says Jörg Höppner. “Such an entry into the digital systems of our members could potentially be misused to get bad cans produced, also by switching off the quality checking systems. In our meetings we invited experts in cybersecurity to make our members aware of the possible threats.”

©2012 Dave Blazek · looseparts@comcast.net · Dist. by Tribune Media Services, Inc. 1-20

This may be the worst case of hard drive infestation I've ever seen.”

ADVICE FROM BERT WILLEMSEN AND THE COMPANY aXite

Based on countless experiences with cyberattacks on various companies, Bert Willemsen comes up with some clear advice.

“Checklists of cybersecurity control systems suggest to detect intrusion, protect assets from physical access and execute controllers configuration integrity,” he notes. “Manufacturers are becoming more and more aware of the threat of unauthorised access to their control systems.

“A more strict change in management procedure should make changes controllable and data should be put in specific context to monitor the operation at a specific location to monitor risk and mitigate threats.

“We developed in-line tools to execute this at shop level, next to the controllers. Programmes can be modified and tested up-front, including a Factory Acceptance Test (FAT). Followed by secured installation of the tested version also during the Site Acceptance Test (SAT).

And although operations often are running 24/7 and 365 days a year, real-time detection, prevention, neutralisation and recovery should be made available at controls level.

“The impact of intended or unintended changes to the machinery can have such a huge effect; it could put companies out of business.”