Protect your company against ransomware attacks

According to the 2019 Official Annual Cybercrime Report, a business falls victim to ransomware every 14 seconds. With employees working from home and operating outside the corporate firewall, the risk increases.

What is it?

Ransomware is malicious software that blocks the user's access to a computer system or device until a ransom has been paid. The malware finds and encrypts valuable data and locks users out of their operating systems, then demand payment, usually in the form of bitcoin or another cryptocurrency, to reveal the decryption key.

There is no guarantee that, by paying the ransom, victims will regain access to their devices and data.

Back-up and update

Use multiple back-up solutions and ensure that at least one of them is offline at any given time. Remember: cloud syncing services like Dropbox or Google Drive may synchronise after data has been encrypted, making backup pointless.

Update the company's antivirus software regularly and choose a provider that offers add-ons that spot file encryption and automatically make copies of the threatened files.

Choose a secure password and change it regularly. Remember that brute force attacks account for 31 percent of all attacks.

The human element

Train employees to recognise and report suspicious e-mails — ransomware can easily spread from spam and fishing e-mails.

Use content scanning and email filters to add an extra layer of protection. These tools can detect malicious links and delete dangerous emails before they reach staff.

Ensure a standardised security protocol throughout the company, from employees to executive-level positions.

Develop an emergency recovery plan that includes a response to a potential attack. Include technical guidelines but also strategies to mitigate legal and reputational consequences.

Check with your insurance providers whether your policy covers the costs associated with a ransomware attack.

Create a PR strategy to explain the situation to customers, investors and the press in case of an attack.

For more expert tips on cybersecurity in your smart plant,
visit www.euautomation.com