Protection for smart factories

End-to-end protection against cyber attacks – a must in connected manufacturing

These days, everyone is talking about the advantages of fully connected, automated, and self-regulating processes in Industry 4.0. When production facilities become accessible via industrial Ethernet and internet protocol (IP), however, they become vulnerable to new risks and targets – but these have proved to be a less popular topic of conversation. To prevent intrusion and extortion by cyber attackers, holistic IT security solutions are required.

Time is of the essence. Picture a facility in which production processes run at full capacity 24 hours a day. Suddenly, the touchscreens on several machines fail. When the personnel check to see what is wrong, they realize that access to the central process data is blocked. It is not long before they receive a blackmail threat by email.

This is not a made-up scenario. Since 2016, Germany has been hit by six major waves of cyber attacks. According to the Federal Office for Information Security (BSI), some of the companies affected saw their operations grind to a standstill for several weeks and re-ported losses amounting to millions of euros. The BSI reports that attacks on plant control systems and industrial computers are on the rise. This upward trend is attributable to increasing numbers of connected processes which create new targets for cyber criminals. BSI president Arne Schönbohm is understandably worried: "We're seeing an ongoing surge in IT security incidents; they are occurring with increasing frequency and reaching new levels of sophisti-cation." At the dawn of Industry 4.0, this is clearly an unsettling message.*

Industrial Ethernet offers better performance but poses new risks

Industry 4.0 promises to bring enhanced efficiency, transparency, and flexibility to production processes – but also comes with a greater number of risks. Connected environments see the field-buses used in the past replaced by Industrial Ethernet, while production systems can be accessed via internet protocol (IP). Opening the systems to the outside world in this way increases the risk of unauthorized access to the control software and to sensitive data. The recent spate of attacks – many of them success-ful – shows that even global corporations with highly advanced IT infrastructure underestimate the risks.

Small and medium enterprises do not always make the necessary investments in cyber security, either. Many falsely assume that hackers would have no interest in their production facility. They run their production IT systems non-stop and often miss updates as a result, which is precisely what makes these companies so vul-nerable to both manual and automated attacks. Even machines not connected to the smart factory are at risk from attack during maintenance, for example, or via unauthorized USB interfaces. Blackmailers can moreover target production operations as part of wider supply chains. And if that is not reason enough to take precautions against cyber criminality, new regulations such as Germany's IT Security Act stipulate that companies must imple-ment industrial IT security measures by law.

A job for the experts

The only way to reliably protect connected production facilities from the dangers of cyber criminality is to put holistic security solutions in place. It takes a deep understanding of heterogeneous IT systems in the production environment to perform the detailed status quo analyses required to systematically identify and evaluate risks, and to define security objectives. Security concepts must allow for maintenance and updates in facilities where machines run around the clock, and account for multiple operators accessing individual systems – which makes password protection a highly impractical solution. In-house IT departments – perhaps more accustomed to dealing with office IT – are rarely in a position to develop holistic security solutions for their production systems alone. This is where the experts come in.

After all, security needs to be addressed at all levels and appro-priate governance developed in order to firmly embed IT security in organizational structures, in processes, and in people's minds. Verification of the solution's effectiveness using the PDCA cycle (plan, do, check, act) is equally as important as having an information security management system in place (ISMS). Cornerstones of holis-tic protection include prevention of risks, identification of critical incidents, and initiation of quick responses to defend against such incidents. End-to-end security solutions must also enable con-clusions to be drawn about future threats. Only in this way can companies ensure the integrity, availability, and authenticity of all IT components and systems in their connected production facilities, and protect the confidentiality of the associated data.

Concrete security measures

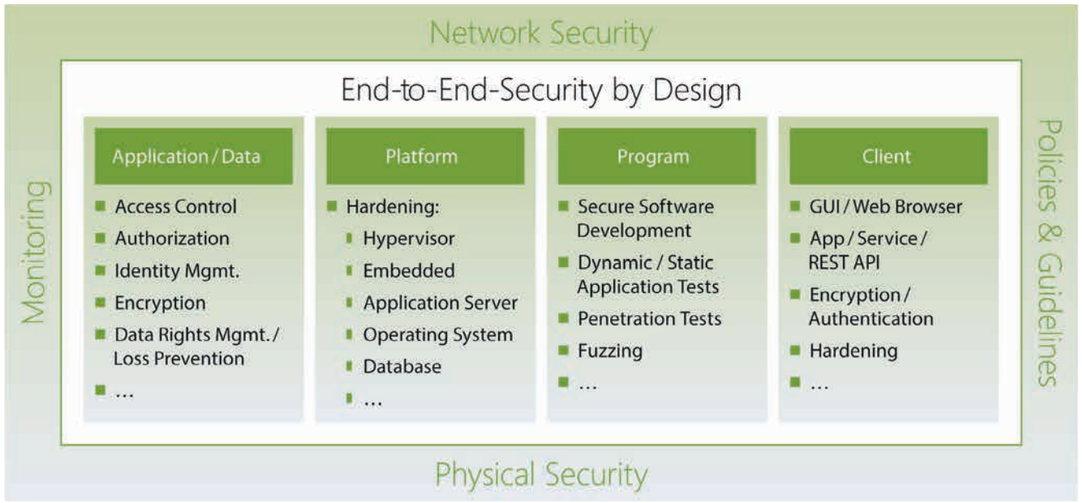
Given the heterogeneous nature of IT systems, existing production lines are difficult to protect. For this reason, it is advisable to trans-fer protection measures for individual machines or security zones to upstream systems. That, first of all, shields process communication from the outside world and filters out any suspicious network traffic. It moreover enables antivirus software, defense functions, application recognition, and user identification to be updated with-out stopping production activities. Zone models also provide pro-tection whereby firewalls monitor communication between indi-vidual production zones. Based on source and target information, they filter out unauthorized network traffic. Setting up these zones calls for IT experts to work closely with production experts. And, if a secure environment is divided up in this way, it is important to ensure that tasks such as implementing updates or changes, or legally compliant reporting, remain easy to manage.

Best practice: end-to-end security by design

The situation is different in new smart factories, however, because industrial cyber security can be integrated directly into the software and hardware control systems for the production lines in the planning stage. Security organization, continuous IT security management, and protection of components and systems can be harmonized from the outset and designed to cover the entire lifecycle of the plant and machines. This end-to-end security by design approach means that production facilities become connected IT systems in themselves, which puts security at the very heart of Industry 4.0. ■

Author

Norman Wenk is Group Manager Enterprise IT Security Consulting at **ESCRYPT**.



Best Practice – End-to-End-Security by Design

*) Source: BSI-Magazin 2018/1