Summary/Recommended action

"Industry 4.0" requires additional measures. Be aware of the fact that there are specific requirements linked with this topic.

- Take its aspects into account when designing your security architecture (security by design)
- Identify vulnerable process elements and protect each of them
- Align your security concept's technical and organisational measures with the changes going along with "Industry 4.0"
- Make sure to include binding security regulations when designing contracts relating to Industry 4.0
- Raise all staff members' awareness and train them

Do not hesitate to contact us and make an appointment for confidential awareness talks.

Your points of contact in economic security

initiative wirtschaftsschutz

Protecting values in a concerted effort

For additional information and your local contacts' communication data, please visit the website

www.wirtschaftsschutz.info

Imprint

Publisher: BfV (German federal domestic intelligence service) for the community of the domestic intelligence services of the Federation and the federal states

Pictures: © fotohansel - Fotolia.com
© magele-picture - Fotolia.com
© Nikolai Sorokin - Fotolia.com

DOI: January 2017

Domestic intelligence service

Federal Republic of Germany
Federal States

Economic Security

Challenges of a new technology

Industry 4.0

What is "Industry 4.0"?

This concept refers to connecting product development, production, logistics and customers in a smart way. The driving force behind this development is the rapidly increasing digitisation of the economy and society, which already has a lasting effect on the way companies work.

Such an integration aims at optimising corporate workflows and at developing new business models to ultimately achieve an increased added value. This opens new horizons in particular for small and medium businesses, but may also go along with additional challenges.

New opportunities

–

New risks

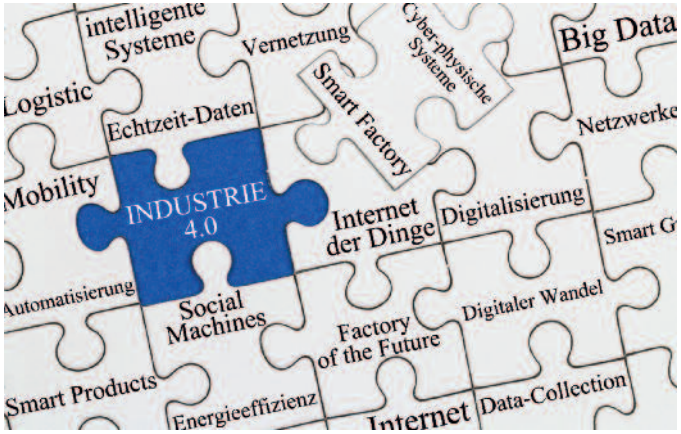
Risks

The growing digitisation and integration within the business world also increases the number of interfaces and interactions between various protagonists who seldom work with consistent security standards. This trend opens up completely new ways for attacks and, in addition, multiplies the existing risk of electronic attacks.

While, until now, only one central control system had to be protected (e.g. by means of a firewall), "Industry 4.0" requires every single smart element integrated within the system as well as the appropriate communication to be safeguarded. These so-called "cyber-physical systems" (CPS) are capable of autonomously gathering information, triggering processes, and controlling each other. Each of them should be considered an independent computer to be protected individually in order to prevent sabotage or espionage.

"Companies will have to increasingly open up to this integration. One of the essential aspects is the reliability of the systems being used. To achieve this, an effective and seamless security concept needs to be prepared."

(Michael Ziesemer, ZVEI President,
CompetenceBook, 2015)



New types of threat scenarios

- Production details being spied out through reading CPS parameters
- Sabotage through manipulation of single CPS and/or of the CPS communication
- Influencing through DoS attacks against CPS layers to the point of the stoppage of production

Outlook

Industry 4.0 will enable the economy and society to develop enormously. Furthermore, the growing integration (e.g. Smart Cities, Internet of Things) will increasingly shape our everyday lives. Everyone should be aware of this fact, considering it both in personal and in professional environments.