INFOCOM.
Shaping digitization securely.

Industry 4.0

Challenges of the networked industry

IABG

Challenges of the networked industry

Increased networking of industrial control systems provides integrators and operators with new challenges that have so far primarily been known in classic IT environments. The focus areas of **Industry 4.0, Smart Manufacturing and Internet of Things** require a high degree of networking at a high security level. Against the background of a rapidly increasing number of cyber-attacks, this is of particular relevance: Cyber criminals pose an equally imminent threat as the increasing activity of state-financed hacker groups. A modern IT and communication infrastructure protects you against brain and knowledge drain and reduces the risk of falling victim to cyber blackmail or sabotage.

Typical challenges for companies in this context are:

- Secure integration of Informational Technology (IT) and Operational Technology (OT)
- Secure integration of external partners, such as suppliers, sales partners or service providers, e.g. via cloud services
- Automated ad-hoc establishment of trust relationships to external partners (trustworthiness)
- Integration of various, partly proprietary technologies, such as different field buses
- Elimination of risks and weaknesses in existing systems
- Components of industrial facilities cannot be updated (for example, because systems are certified and accepted, operating permits would expire or manufacturer updates are missing)
- Interaction of organisational and technical security aspects
- Introduction, operation and continuous development of a comprehensive security management for office and production facilities
- Certifications as proof of your security measures to third parties, e.g. authorities, customers or partners

IABG provides advice and support when you are introducing, restructuring or redesigning your communications and information technologies, from conceptual design all the way to the implementation phase. You can hereby rely on our project experience in highly sensitive security areas. Our customers have special demands on the availability of their services as well as on the confidentiality and the integrity of their information.

2012

After an industrial control system malfunctioned: Waste water from a sewage treatment plant leaks into a Californian river.

2013

Massive damage after a German steel mill is hacked: System can no longer be shut down in a controlled manner.

Shaping digitization securely.

Our range of services

Technical infrastructure analysis

IABG supports you throughout the entire life cycle when securely networking your production. We determine your individual protection requirements, identify and assess risks to your systems. In addition, we perform penetration tests when analysing your infrastructure to identify and eliminate vulnerabilities.

We furthermore analyse your communication infrastructure and contrast your requirements – from the communication of your automation hardware at control level (e.g. **Industrial Ethernet, wireless communication**) via process control systems (e.g. **DNP3, Siemens S7 protocol**) and office communication (e.g., **IP networks, LAN**), all the way to cross-site networking (e.g., **WAN technologies, Carrier Ethernet**). The goal is ensuring secure networking of your production in line with your needs.

Development of customer-specific concepts and strategies

Together with you, our specialists define the protection goals of your company and develop operational and technical security concepts matching your needs – **security by design**. At the same time, we take into account internationally recognized standards, such as **ISO 27001 or ISA / IEC 62443** and create a catalogue of measures for you. In addition to that, we enhance the development of your network architecture, perform profitability assessments and, for larger projects, create a migration plan ensuring smooth implementation.

Providing advice and support in the implementation phase

Our experts close security gaps, eliminate vulnerabilities of your systems and identify the products required to meet your protection requirements. We are your experienced partner when it comes to the introduction and continuous development of an **Information Security Management System (ISMS)**.

We create test specifications for you allowing to verify infrastructure functionality by means of acceptance tests. We furthermore document your technical infrastructure as well as your organisational and security processes.

Supporting the operation phase

On request, our colleagues also gladly support the operation of your technical infrastructure, your ISMS or the work on the continuous improvement of your processes.

Energetic Bear / Dragonfly

Spear phishing on European and US energy sectors.

US utility companies face brute force attacks.

2014

At a security conference, researchers present a guide on how to attack a chemical factory.

Further increase in attacks on Industrial Control Systems in 2015 compared to 2014.

Cyber-attack on a control computer brings Canadian bakery factory to a standstill.

2015

AUTOMOTIVE

INFOCOM

MOBILITY, ENERGY & ENVIRONMENT

AERONAUTICS

SPACE

DEFENCE & SECURITY

About IABG

IABG offers integrated, ground-breaking solutions in the sectors Automotive • InfoCom • Mobility, Energy & Environment • Aeronautics • Space • Defence & Security. We provide independent and competent consulting. We implement with future viability and target orientation. We operate reliably and sustainably. Our success is based on an understanding of market trends and requirements, on our staff's technological excellence and a fair relationship with our customers and business partners.

For more information please contact:
infokom@iabg.de
www.iabg.de

Download this flyer

IABG
Einsteinstrasse 20
85521 Ottobrunn
Germany
Phone +49 89 6088-2030
Fax +49 89 6088-4000
info@iabg.de
www.iabg.de

Berlin Bonn Dresden Hamburg Karlsruhe Koblenz
Lathen Lichtenau Noordwijk (NL) Oberpfaffenhofen