**INFOCOM.**
Shaping digitization securely.



**IABG –
Your IT service provider for
cyber security**

**iABG**

## Cyber security

The report by the Federal Office for Information Security (BSI) on the IT security situation in Germany has shown a significant increase in the risk of cyber-attacks for several years with over 300,000 new malware programs discovered every day. The rise in national and international cyber-attacks clearly show the major challenges companies and public administrations face. In order to cope with the danger of cyber-attacks they must act in a risk-oriented manner and implement suitable security measures in time.

The risk of falling victim to a cyber-attack has become a major problem in our globally connected world. Apart from attacks on so-called office IT, where most data theft occurs, industrial production has also not been spared from hacker attacks in recent years.

The sharp increase in networking and digitization in areas such as smart homes, smart grids, autonomous driving, industry 4.0 and digital management means that the number of targets who will be open to attack in the future is constantly increasing, and this problem will have to be addressed accordingly.

Yet 70 % of companies in German-speaking regions still do not have an adequate IT security staff. Therefore, it can take months before strategic cyber-attacks are even discovered in corporate networks.

The longer an attack remains undiscovered, the greater the damage done. Since it is impossible to achieve a one hundred percent security level, it is essential to detect attacks early, evaluate them, and counter them with the right defensive measures.

Our experts help companies and public authorities alike arm themselves more effectively against cyber-attacks and protect themselves against data theft and loss as well as against financial damage.

## ISMS and risk analysis

To achieve effective protection against cyber-attacks Germany must introduce and further develop an information security management system (ISMS). An ISMS encompasses the technical and organisational aspects as well as the personnel aspects of security measures. Operators of critical infrastructures are obliged by the IT Security Act to implement an ISMS.

### Your added value
- We perform risk analyses
- We accompany you in the introduction, further development, and operation of an ISMS based on ISO 27000 native and in compliance with the IT baseline protection
- We draft tailored IT security concepts and plans of action for you
- As one of the very few IT security service providers certified by BSI (Federal Office for Information Security) we prepare audits and revisions for you or perform them for you
- We advise you on technical and organisational matters regarding information security

## Technical IT security

Protection against cyber-attacks is achieved, among other things, by implementing the technical specifications and measures of IT security concepts. Initially, these encompass the securing of your software against attacks, for example by

- Appropriately segmenting your systems and services,
- Implementing suitable security gateways like firewalls or data diodes,
- Using cryptography to encrypt and authenticate information.

For early recognition of any other cyber-attacks we recommend the deployment of sensors like virus walls, intrusion detection systems, or honeypots.

As well as the implementation of security solutions, their operation is also of key importance. Regular updates and the generation and administration of the necessary codes and certificates via a PKI are decisive here.

The information from the security sensors come together in a Security Operation Centre (SOC) and is captured, processed and evaluated onsite by a Security Information and Event Management System (SIEM). Based on this information and partially supported by a Computer Emergency Response Team (CERT), specialists activate appropriate measures to counter cyber-attacks. In this case, the SOC/CERT can either be operated independently by yourself or provided as a managed security service by an external service provider.

### Your added value

- We draft technical and customer-specific security concepts
- We identify and evaluate security solutions
- We make recommendations regarding the operation of your security solutions
- We draft statements of work and technical award documents for you
- We assist you with the awarding and the introduction of security solutions
- We perform threat analyses and verify security measures through penetration tests in selected areas



## A selection of reference projects

**We provide our services in the cyber security sector** to a vast number of public and private customers. For example, we currently support a German federal agency with the introduction, further development, and operation of its information security management system (ISMS) according to ISO 27001 based on IT baseline security, and act as its main contact for any questions in connection with information security.

**We advise German federal state authorities** on the continual optimisation of their existing security architecture and in the design and implementation of a Security Operation Centre and a Computer Emergency Response Team. This encompasses the central collection, processing, and evaluation of all the information from security sensors in an SIEM system.
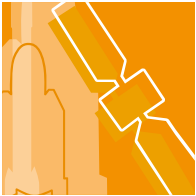
**AUTOMOTIVE**

**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