Cybersecurity is not just the keyword of the day because of the recent scandals surrounding international secret services. The threats from the internet, be they from government agents or criminal associations, should be taken seriously by all companies and present serious challenges for individual companies. Maintaining the confidentiality, integrity and availability of critical information and the information technology behind it, whether this involves research and development data or customer relationship data, should be of the utmost importance for companies in all industries and of all sizes in order to ensure their competitiveness and corporate success for the long term.

Cybersecurity expands the scope of classic IT security to include all of cyberspace. This comprises all information technology connected to the internet and similar networks and includes communication, applications and processes based on this as well as data processed through it. Thus basically all modern information and communications technology becomes part of cyberspace.

What makes cyber attacks so dangerous? They can't be seen: Cyber attacks can be launched from anywhere in the world – wherever there is access to the internet. They are dynamic: Cyber attacks compromise IT systems of any kind, are increasingly professional and continually developing, faster than the security cycle of the IT systems themselves.

Numerous private and government initiatives, such as the Alliance for Cybersecurity founded in 2012 by the German Federal Office for Information Security (BSI) and the German Federal Association for Information Technology, Telecommunications and New Media (BITKOM), provide a platform for companies to communicate with one another. In addition, steps and measures are developed here together with the companies that can be used to counter the threats from cyberspace.

Having an experienced partner is key to successfully implementing suitable measures to achieve an appropriate level of protection. These should be well-versed in industry and company-specific issues as well as the possibilities currently offered by technology. Roever Broenner Susat Mazars is your partner for cybersecurity in a wide range of application areas. For example, we took a leading role in the development of the cybersecurity check as well as the development of training measures and Cyber Security Practitioner (CSP) certification as part of an initiative of the ISACA Germany Chapter e.V. with experts from the BSI.
The cybersecurity check is a pragmatic approach to assessing the state of the security of the information at your company with analysis criteria that is also comprehensible for management. It is completed in a risk-oriented manner based on the concrete need for protection in your company. As it only takes a few days to complete, it does not involve great effort. The cybersecurity check is based on current security standards and best practice frameworks and is thus compatible with measures that are already in place at your company.

The assessment is completed using a variety of methods: Interviews with those responsible in your company, inspection of the security arrangements in place, review of documentation as well as analysis for relevant data (such as protocols and log files) Active interventions in your company’s IT systems are not necessary, which rules out the risks associated with this.

The cybersecurity check identifies weak spots and sorts these into easily understandable categories. The issues that are noted are thoroughly documented by us. Additionally, binding objectives for the improvement measures are defined. In the final assessment report, all issues and deficiencies that have been identified are listed in detail, assessed and the corresponding recommendations and measures are documented.

Our services at a glance
- Developing security guidelines
- Hosting training and awareness measures
- Building information security management systems in accordance with ISO 27001
- Creating emergency management procedures
- Information security audits and cybersecurity checks
- Analyses of the need for protection and the risks
- Preparations for information security certifications in accordance with ISO 27001
- Assistance with the implementation of measures in accordance with ISO 27001 and BSI IT-Grundschutz
- Review of the internal control systems of IT service providers

Contact

Stefan Wittjen
Diplom-Kaufmann
CISA, CIA, CISM, CRISC, QA, QAR-IT
Senior Manager
Tel: +49 30 208 88-1170
stefan.wittjen@mazars.de