



CYBER-SECURITY SERVICES – GUARDING YOU IN CYBERSPACE.

KEY COMPETENCE IN CYBER PROTECTION.

The cyber-vulnerability of globally networked companies keeps increasing, since cybercriminals, Internet activists and industrial spies have become highly professionalized. Even large corporations now need assistance in handling the many different threats that have emerged. More and more, attackers have been zeroing in on core operational assets. While cyberspies focus on the intellectual property with which companies set themselves apart in the market, cybersaboteurs seek to disrupt business processes that are critical to companies' value creation.

As a result of the growing threats, cyber protection has become a key area of competence. And such protection is not limited to the area of ITC per se; it also extends to corporate governance and corporate risk management. In practice, companies have to integrate their existing processes and mechanisms within company-wide cyber-security management frameworks. As a globally operating provider of end-to-end services, T-Systems has the know-how and the services that companies need to complete such transformation processes successfully.

IMPLEMENTATION-ORIENTED CONSULTATION.

In the basic Cyber-Security Assessment it carries out for a company, T-Systems determines what company resources and assets are at risk, and in what ways. The assessment outlines the current status of the company's protection and defines the level of security that needs to be achieved. Significantly, it focuses on protection of business-critical processes. In a next step, T-Systems then carries out Cyber-Security Architecture Consulting, in which a reference architecture for all necessary individual measures is developed. The architecture makes it possible to derive all measures in a consistent way.

Then, Cyber-Security Transformation Consulting lays out how – and when – the measures need to be implemented. Upon request, T-Systems supports all relevant implementation and backs the cyber protection with its tried-and-true Managed Services. And if attackers should nonetheless find a way to get through the company's lines of defense, a Cyber Incident Response plan is activated to guard the company's intellectual property and processes.

THE DIFFERENT CYBER-SECURITY SERVICES.

CYBER-SECURITY ASSESSMENT.

This assessment illuminates the company's specific threat situation. T-Systems' security experts determine what information, systems, processes and locations might attract attackers. In the process, they consider different types of attackers, with different types of attack agendas. The experts determine how serious the various types of potential damage would be, and they analyze the effectiveness of the company's existing defenses. In doing so, the experts think and work like attackers, applying "penetration tests" in order to try to overcome the company's protecting systems. Once they have identified and assessed the various cyber risks involved, T-Systems' consultants work with the customer to define the necessary level of protection. The result of the assessment is then a meaningful CURRENT SYSTEM/DESIRED SYSTEM model which serves as basis for deriving and prioritizing suitable measures.

CYBER-SECURITY ARCHITECTURE CONSULTING.

On the basis of the assessment results, T-Systems then develops a cyber reference architecture. The company's existing ITC infrastructure serves as a starting point, to ensure that the company's existing investments are protected to the greatest possible extent. If the company's existing security management is not adequately guarding against the identified risks, the reference architecture reveals precisely where changes are required.

CYBER-SECURITY TRANSFORMATION CONSULTING.

If the CURRENT SYSTEM/DESIRED SYSTEM comparison reveals a need for action, T-Systems prepares a "road map", with specific measures, and prioritizes the pertinent tasks. For each measure, the road map details the contribution the measure will make to the company's defenses. To ensure that the resulting benefits are measurable, the T-Systems consultants define customized performance indicators and provide the necessary measuring tools to monitor them.

CYBER INCIDENT RESPONSE.

T-Systems also develops systematic procedures for managing security incidents. Such procedures provide the basis for operational responses to attacks, and they support additional related tasks such as development of suitable information policies and preservation of evidence. In addition to meeting its own, experience-based standards, T-Systems conforms to applicable industry standards, such as ISO/IEC 27035 and NIST Special Publications 800-61 and 800-86.

CYBER INTELLIGENCE FOR ITC INFRASTRUCTURES.

Along with its consulting services, T-Systems offers a Cyber-Intelligence Service that functions around the clock. This service gathers information from a range of different relevant sources and assesses it. The information sources involved, for example, include Security Information & Event Management (SIEM), which T-Systems operates as a Managed Service. It monitors, and continually assesses, the log data for all security-relevant systems. In cases of attack, a T-Systems Cyber Incident Response Team takes the controls and wards off the attack.

CYBER-SECURITY SERVICES.

- put meaningful price tags on risks and cyber protection and provide road maps to optimal protection
- improve companies' ability to respond, and limit any damages in case of attack
- protect the availability of information, systems and processes, and thus protect companies' ongoing operations
- protect cutting-edge/innovative intellectual property against espionage
- limit the costs companies can incur via contractual penalties or sanctions, and prevent damage to a company's image
- provide a common working basis for corporate governance, risk management and ITC protection

ANY QUESTIONS?

Internet: www.t-systems.de/security
or simply e-mail to
security-info@t-systems.com

TO CONTACT EXPERTS

T-Systems International GmbH
Gerd Enste
Vorgebirgsstr. 49
53119 Bonn, Germany

PUBLISHED BY

T-Systems International GmbH
Hahnstr. 43d
60528 Frankfurt
Germany