S4T

Your Service for Information and Technology

ISN'T THE NSA
INTERESTED IN
YOUR COMPANY?

LUCKY YOU!

Industrial espionage by intelligence agencies or
other organizations can affect everyone.

How safe is YOUR business communication?

S4T

Trust is good,
Protective measures are better

Recent disclosures cause great indignation and unrest. Many companies are surprised by intelligence agencies' listening activities and their scope, however the risks and threats for companies are not new. Therefore, companies must not fear intelligence agencies as much as criminals or competitors, who want to abuse internal knowledge for their own economic interests and competitive advantages.

Industrial espionage has been a real threat for years. Required protective measures are known and appropriate solutions are available on the market.

One hundred percent security cannot be achieved, but whoever takes no action runs the risk of being spied upon as well as the disclosure of its critical business secrets. Yet periodic individual measures have no effect! Security must be considered as a whole, long-overdue measures must be implemented consistently.

Absolutely indispensable measures

Basic protection

- Educating the staff and creating security awareness in the form of company-wide information campaigns.
- Conscious communication and data economy, i.e. avoiding unnecessary communication and Internet services.
- If you want to protect your business effectively, but can't do nearly enough, additional measures must be taken.

Necessary measures

Increased protection level

- **Use of encryption technology**
  - Protected e-mail communication without technical burden on the user.
  - Use of VPNs for communicating with business partners and associated offices.
  - Implementation of integrated, end-to-end encryption.
  - Encryption of cloud contents and/or waiver of online storage, especially abroad.
- **Trusted hard- and software**
  - Use of solutions by German manufacturers that are subject to our strict legislation and controlled; the German intelligence agency has no legal mandate for economic espionage.
- **Trusted services**
  - Cooperation with German companies, which maintain the data in Germany.
  - Do not use foreign cloud services; e-mail and cloud providers resident in Germany are subject to German data protection law.
- **Technically supported data economy**
- **Technical infrastructure measures**
  - DMZ and high-security network concepts (including firewalls, IPS, etc.) with appropriate logging/alerting.
  - Strong authentication (two-factor authentication) and secure remote access (for example, SSL-VPNs).
  - Monitoring the existing security level using vulnerability scanners.
  - Current asset and Patch/Update Management.
  - Data Loss/Leakage Prevention (DLP) – protection against disclosure of sensitive data.

Recommended Actions

Highest protection level

The **most effective** protection against threats is a well-established company management system for information security. This makes it possible to maintain permanently the three pillars of information security: confidentiality, integrity and availability.

By implementing and operating an information security management system (ISMS), all significant measures of the underlying protection levels are covered. Implementing an ISMS based on the ISO/IEC 27000 standard is recommended.

With the internationally recognized standard, organizations in all industries can have their Information Security Management System (ISMS), which means their processes and measures for guaranteeing information security, certified according to ISO/IEC 27001. Thus, you can be sure that all necessary measures and activities for ensuring information security are implemented professionally in your company.

Our recommendation

There is no such thing as off-the-shelf security. Security solutions are tailor-made.

We can help you design and implement the necessary security measures for your company and its requirements.
Get in touch with us!

Your benefits

- Construction of a holistic, safety management system optimally oriented to your business processes.
- Risks are visible and minimized.
- Impartial advice for the best overall solution.
- Using the latest security methods and technologies for maximum protection.

Why IS4IT?

IS4IT's security business has been successfully established on the market for years. We provide comprehensive support based on our many years of experience and extensive knowledge. Our solutions tailored to your needs are not only reliable, but also provide significant added value and are cost effective to operate. We also assume the support and operation of your surroundings and offer flexible managed service concepts.

Our ultimate goal is the proper protection of your corporate values.

IS4IT and our staff have a broad portfolio of expertise that is supported by numerous product- and vendor-independent certifications. Well-known customers in all industries rely on our expertise.

- ISO 27000
- ITIL
- Certified Information Security Auditor according to ISACA
- Certified Information Security Manager according to ISACA
- Professional Association of EDP auditors
- CISSP – Certified Information System Security Professional according to ISC2

IS4IT ensures security – Rely on us as a security partner!