Author: Ingeborg Schlosser

Information Security: It depends on the right measure

Customers, partners, legislators and lawmakers are increasingly forcing companies to ensure IT-Security protection. While the international IT- Security standard ISO 27001 has been consistently implemented in several large companies, the complex catalogue of measures poses significant challenges for SMEs (small/medium-sized companies). However what options do SMEs have in the organisation of IT-Security? The most important principles are summarised in the CFPA "Protection of Business Intelligence" guide, which raises important aspects of Cyber-Security. VdS Guidelines 3473 go even further – developed specifically for small and medium-sized enterprises, they implement the fundamental requirements of the ISO standard at only 20% of the costs.

Nearly 60% of organisations in Germany have been victims of a cyber attack over the past two years. This was announced by “The Alliance for Cyber Security”. According to the auditing firm KPMG, the number of victims of e-crime has doubled since 2013. In companies, this risk is well known: 89% of those responsible see a high or very high risk for German companies to suffer from

a cyber attack. However, few people fear being hit themselves. They therefore only use inadequate security measures and only react when it is too late. The fact that a separate position is created that is exclusively concerned with IT security tasks is very rare – in 85% of companies with fewer than 1,000 employees this is not the case. The consequences of an attack are devastating and range from business or production losses to financial losses or image damage.

Challenge IT-Security

However whether from entrepreneurial self-interest or due to the demands of customers, contractors and legislators and lawmakers: SMEs are increasingly forced to ensure IT-Security. Against this background, a number of well-known institutions and bodies now involve themselves with the subject of Cyber-Security. One example is the CFPA Europe, which has developed a comprehensive guide with the "Protection of Business Intelligence", in which the essential parameters for the implementation of information security in companies are presented. And CFPA Europe is working on the development of further common guidelines and also on harmonized training courses on this topic. In addition, a large number of CFPA members are now discussing the topic, as a glance at various publications shows.

International standard is complex and expensive

The most widely known and probably the most extensive directive for Cyber-Security in larger enterprises is the internationally recognised standard ISO 27001. However, the expense, effort and resources required with ISO 27001 are significant – from risk analysis to the elaboration of the abstract standards contained in the standard, up to the implementation of the concrete measures. For SMEs the certification is therefore usually associated with too high a cost and is therefore hardly achievable. Against the background of this complexity, the statistics presented at the outset do not surprise us that companies know the risk of an attack but do not adequately protect themselves. The lack of security measures is not an expression of carelessness, rather a consequence of the overwhelming demands of IT security.

Free risk analysis as a first step

To encourage and help especially SMEs to deal with this complex topic, in several countries questionnaires are available to raise the awareness for the most important risks. A tool to carry out a first risk analysis has been developed for example by CEPREVEN, the Spanish CFPA Europe member, and it is offered online for free. More information is available at http://www.cepreven.com/cuestionario-ciberseguridad.

The German CFPA Europe-member VdS has also worked on the topic and developed a system to support SMEs with regard to cyber-security.

VdS 3473: The solution for the SMEs

One way to easily implement IT-Security is VdS 3473. This standard developed by IT experts, is oriented to ISO 27001 and implements 80% of the ISO standard at only 20% of the cost. The special strength of the VdS 3473 guidelines is in the consideration of the organisational level. Topics such as personnel, responsibilities, accesses, etc. are adequately covered and small and medium-sized enterprises are neither overburdened organically nor financially. It is not without reason that VdS 3473 is one of the top three standards for the implementation of an information security management system, according to a BSI Cyber-Security survey.

VdS Quick-Check

How do companies actually implement the VdS guidelines? The first step towards IT-Security is an individual risk analysis. On the basis of the guidelines 3473, VdS offers a free Quick-Check, which can be carried out online by the company without any additional preparation. The check includes 39 questions, which can be answered within 20 minutes. The aim of the test is to determine the individual degree of protection. In the end, companies receive two evaluations: a compact and a more detailed report. The special features of the Quick-Check are the concrete recommendation measures for immediate action and their implementation.

Quick-Check for production environments

The previous VdS-Quick-Check focuses on the field of office communication. With a second test, VdS offers an analysis tool for companies that use industrial control and automation systems in their production, so-called Industrial Control Systems (ICS). These are often not taken into account when dealing with Cyber-Security. They are at a high risk as a result of the rapid growth in communications connections within the scope of industrial 4.0 projects. The Quick-Check for ICS therefore focuses on criteria such as very high availability requirements, aspects of remote maintenance and cooperation with manufacturers.

VdS-Quick-Audit systematically covers existing security gaps

The test is followed by the Quick-Audit. The security measures implemented on the basis of the Quick-Check results are analysed in detail. The later report shows in detail what measures are to be taken, covers existing gaps and provides comprehensive suggestions for optimisation. These

instructions can be implemented by companies with their own professional personnel, such as IT staff or information security officers, or by the support of VdS-approved consultants.

Certificate for customers and insurance companies

If all improvement measures are successfully implemented, companies will obtain a corresponding confirmation in the form of a certificate. With this they generate trust with their customers and partners. In addition, the certificate has yet another advantage: in order to safeguard the residual risk that remains despite comprehensive measures, companies should conclude a Cyber-Policy. Cyber-Insurance is already common practice in the USA and is also gaining in importance in Germany, especially in the face of the increasing risk potential. The certificate is used by the insurance company to assess the risk and provides more favourable policies for those companies which are proven to comply with the directives.

Just like Quick-Check and Quick-Audit, the VdS certificate is also based on the guidelines 3473 and is thus tailored to the requirements of SMEs. In order to obtain the certificate, auditors examine the necessary documentation and prove for themselves on the spot of the correct implementation of the measures. The VdS certificate has a validity of three years - however, annual, less extensive re-audits are provided. The certificate can later be used as a basis for certification in accordance with ISO 27001.

VdS Cyber-Courses are positioned in line with business practice

In order to firmly establish information security within the company, qualified employees become a decisive key factor. The necessary knowledge is provided by various VdS courses, which focus on different target groups. This includes courses for the information security officer, in which the participants learn how to interlink the necessary safety and security measures in such a way that the necessary level of protection within the company is defined and achieved with as little effort as possible. The course includes the teaching of theoretical knowledge as well as practical exercises and concludes with an examination. In addition, VdS offers courses on the VdS 3473 guidelines, for first-aid in the event of IT loss or damage, as well as a course on Cyber Security for insurers.

Conclusion

When implementing an information security management system, the question now is not whether it is necessary, but rather how it can be implemented. The reason for this is the complexity of ISO 27001, which presents small and medium-sized enterprises with insurmountable challenges. The

difficulty, therefore, is to find the perfect measure of information security management. The ideal procedure takes into account the organisational business areas without overwhelming SMEs: VdS Guidelines 3473 are therefore the ideal standard for small/medium-sized businesses. The path to comprehensive protection leads through the free Quick-Check, the following audit and finally the certificate. In this way, companies achieve higher IT-Security, minimise the risk of financial losses or image damage, while still meeting the demands of customers, partners, legislators and lawmakers.

For more information on the VdS Cyber-Security standard, please visit www.vds.de/cyber
The free VdS-Quick-Check is available at www.vds-quick-check.de
The VdS courses on Cyber-Security are summarised at www.vds.de/lehrgaenge/cyber0/