Data losses plus 64 %: mobility and leased personnel as security traps

Companies in Germany and Austria are obliged to report data loss.
"Waterproof" policies acc. to ISO 27001.

(September 2009) - The risk of data losses is becoming more critical. According to "The Ponemon Institute", 53 per cent of the companies interviewed in Germany report at least one event of data theft within the last twelve months. The past year, the value had still amounted to 34 per cent (plus 64 per cent). For the study "German Enterprise Encryption Trends", 490 IT Representatives were interviewed. The legislators have already reacted and put into force a duty of companies and public institutions to report data loss in Germany in early September. A similar rule is being prepared for Austria thanks to the Amending Statute of the Data Protection Act, which is to enter into force in January 2010. Accordingly the persons concerned would have to be informed in case of data leaks. It is still being discussed whether this should be done directly or via an announcement in a newspaper. As practice shows, organizations stumble over the complexity of the topic. "Without structured personnel policies, decisive security gaps will be overlooked," explains Herfried Geyer, Auditor of the Certification Body CIS. In the interview, he discusses typical security gaps and "waterproof" controls acc. to the International Standard for Information Security ISO 27001.

Mr. Geyer, what typical risks for personnel security do you see in practice?
An important issue is mobility: confidential data on Smart Phones, the fact that updates are not made on the Teleworking PC or the use of data-sharing platforms in the web. Still another factor leading to problems is leased personnel as that on the Help Desk: paid too little, without identification with the temporary employer but with access to customer data and the intranet – this will make damaging activities more probable. Even Leasing Porters can have a surprising IT knowledge, have access to general keys and can act without being observed. This almost seems to be paranoid. However, practice speaks its own language.
What protection is offered by ISO 27001?
The complexity of the whole topic requires holistic concepts: The International Certification Standard ISO 27001 with the relevant Guideline ISO 27002 provides a framework for structured security management. This includes classification of data, persons and resources just as much risk analyses and effective policies. In the field of personnel security, the Implementation Guideline ISO 27002 places detailed requirements relating to mobile computing, teleworking, leasing personnel, subsuppliers and service providers.
What is the way to treat third companies?
Contractual securing is not sufficient. It is necessary to implement security gates on the interfaces. Otherwise it is better to use the company's own employees. At audits, CIS as an inspection and testing body will have to require relevant third companies to work on the same security level. It also is at requests for quotation that this item is being required more and more often.
And what about the company's own employees?
Leaving of employees mostly is regulated well in companies. This is not so much the case for changes of positions. Some employees can still access former projects, have writing rights or keep keys. Therefore, a personnel policy acc. to ISO 27002 covers all the phases of employment: hiring, work, change of position, termination. What is important is to verify Certificates and review extracts from the registers of convictions or indebtedness in advance. In general it is necessary to motivate the employees to sustain the security system by making trainings according to the train-the-trainer principle throughout the company.
Control always is an interesting topic …
This particularly includes technical logging. In practice, log files will be overwritten again in order to save storage space. This is a delicate issue if IT budgets are scarce. Therefore, ISO 27001 provides for risk assessment, access logs relating to security relevant information normally having to be kept longer than operational logs. For detecting fraud situations, fraud detection programmes, which will list non-plausible transactions, can be used.
And within the IT Department?
For example, a 4-eye principle used correctly is effective to protect log files from being changed afterwards. This particularly also is true for the IT Department: There people think about personnel security least. For there is the motto "It's only us anyway." Whoever takes personnel security seriously, will also encounter the requirements placed by the 8th EU Directive and the Sarbanes Oxley Act.
Many thanks for the interview!

www.cis-cert.com: CIS is the Certification Body accredited for ISO 27001 and ISO 20000.