ISSN 2055-6950 (Print)
ISSN 2055-6969 (Online)

Cyber Security Review

Winter 2014/15

CYBERCRIME AS A NATIONAL SECURITY ISSUE

CECSP: TOWARDS EFFECTIVE COLLABORATION ON CYBER SECURITY IN CENTRAL EUROPE

TECHNICAL ANALYSIS OF ADVANCED THREAT TACTICS TARGETING CRITICAL INFORMATION INFRASTRUCTURE

SecuSUITE FOR BLACKBERRY 10 REDEFINES COMMUNICATION

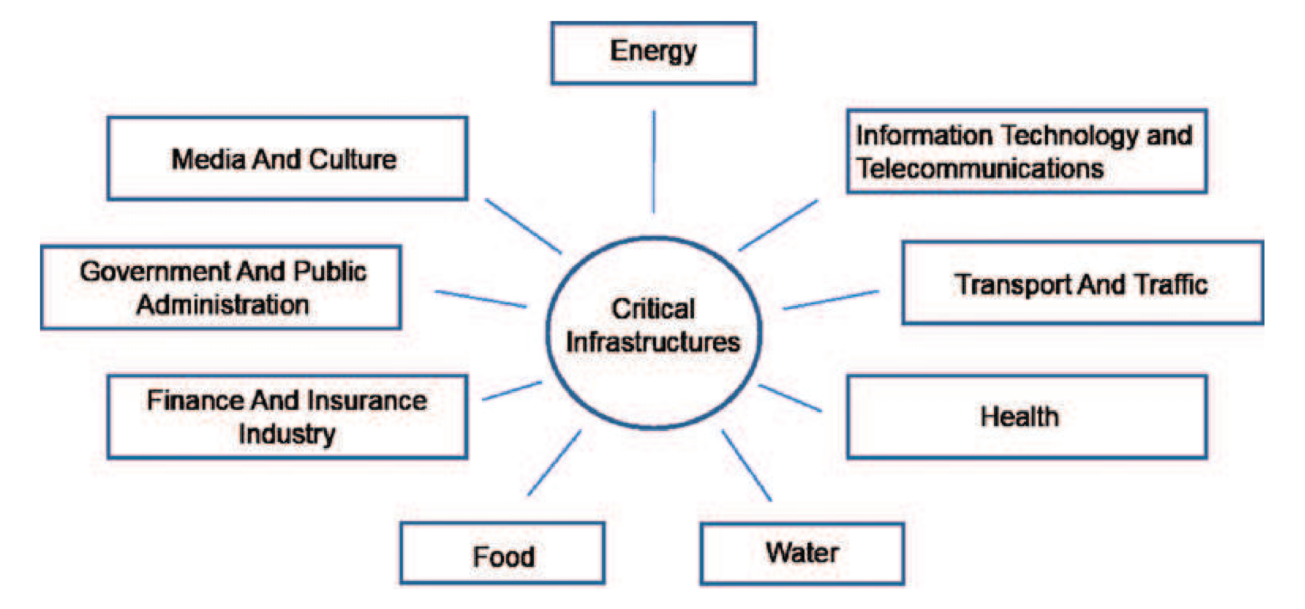
CYBER-SECURITY NEEDS FOR FUTURE CITIES

MAKING SENSE OF THREAT INTELLIGENCE

CHANGING THE APPROACH TO RESILIENCE IN CRITICAL INFRASTRUCTURE

BUILDING A SKILLED CYBER DEFENCE WORKFORCE FOR THE EU MILITARY

SO YOU WANT TO WORK IN CYBER SECURITY. CAN YOU BE TRUSTED?


Energy
Media And Culture
Information Technology and Telecommunications
Government And Public Administration
Critical Infrastructures
Transport And Traffic
Finance And Insurance Industry
Health
Food
Water

Sector overview of critical national infrastructures.

Source: Federal Ministry of the Interior, National Strategy for the Protection of Critical Infrastructures[1].

CYBER SECURITY FOR CRITICAL NATIONAL INFRASTRUCTURES — A CASE FOR HOMELAND SECURITY

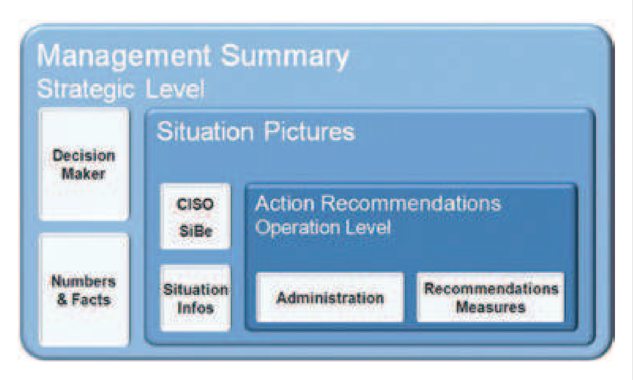
By Dr. Willi Kafitz, TeleTrusT – IT Security Association Germany

J. P. Morgan and other U.S. banks have recently become victims of professionally conducted cyber espionage. Massive amounts of customer data have been affected. Even a liquidation of customer accounts was possible. Many believe the crime took place in Russia. J. P. Morgan boss Jamie Dimon took immediate action and wants to deploy more than 1000 employees working for the IT security and to spend 250 million dollars on cyber security. A lot of damage was done, but fortunately it was not catastrophic.

Fortunately, everything also turned out all right in the energy sector. At the end of last year the IT Security-responsible individuals in over 1,000 energy-supply companies in 84 Western-oriented countries breathed a sigh of relief. A sophisticated malware named “dragonfly” in their energy control systems had been detected and cleaned. Later, a notable virus signature provider analysed the very differentiated files of the malware.

The malware´s intention was obviously to place “time bombs” instead of causing immediate damage. These time bombs could be activated by the click of a mouse. The programmers were evidently highly specialised and were certainly controlled by public authorities. The time stamp of the compilers revealed not only the crime scene to be in Eastern Europe (GMT+4 hours), but that long hours were logged in between Monday 8am and Friday 6pm: the hackers had regular working hours!

Examples such as this are becoming increasingly common. This year the senate of the city of Hamburg was hacked. Even the German federal police became a victim of cyber espionage and lost 270,000 sets of documents for manhunts. All sectors of the critical



Comprehensive situational overview for all relevant target groups as an intermediate goal

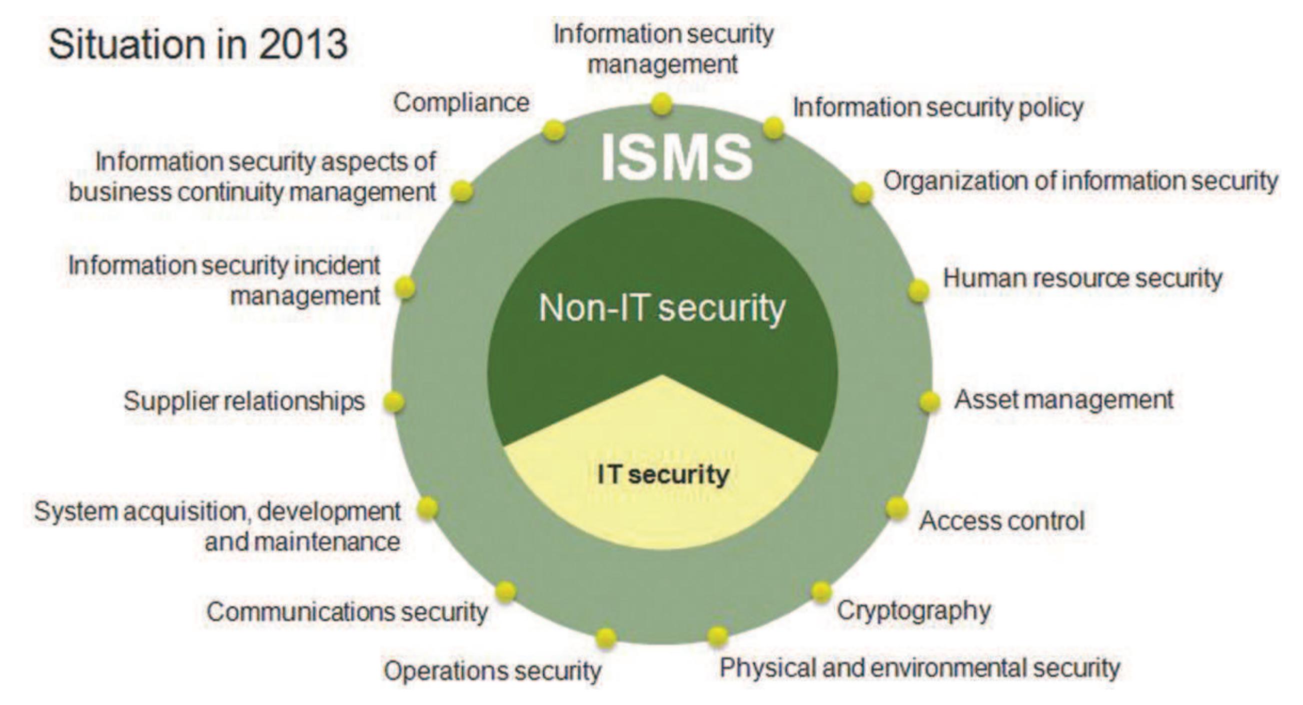
(Source: Mr. Klaus Keus, BSI).

infrastructures are potentially affected and still a lack of sufficient awareness of security persists. With the approval of authorities, security experts in Michigan showed that over 100 traffic control systems could have been acquired.

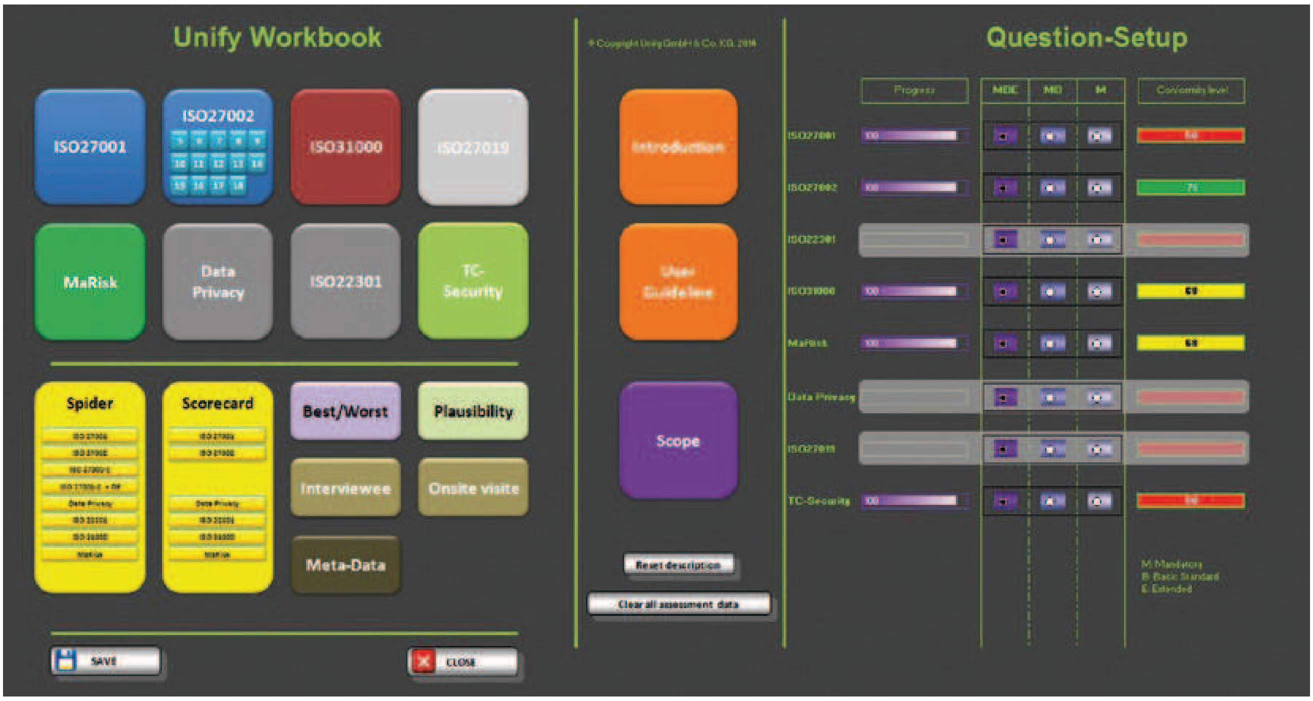
Just by the click of a mouse all traffic lights could have been switched to “red“ or “green“, which would have been even worse. Primarily, the lack of awareness regarding such an event is criticised. A cyber attack simulation called “Waking Shark II” was conducted in London´s bank district on November 12, 2013. In addition to the London Stock Exchange and the Bank of England, all relevant “High Street Banks“ and payment service providers, including the dependencies of the Deutsche Bank and Commerzbank, were represented. It was the second test of this kind after the spring of 2011. Significant progress was made, although difficulties in persistent attacks and sophisticated attacks in the Business Continuity Management (BCM) and in the exchange of information had been observed. Characteristically, institutes that had been considered as especially secure performed much worse this time. Was this a reason for complacency or decreasing effort? However, it can be said that stagnation is recession when it comes to cyber defence.

All operators of critical infrastructures are therefore particularly at risk because our modern society is very dependent on the functioning of the stated infrastructures in these sensitive areas. This applies not only to the economy but also to the media, healthcare, and food supplies. Even social structures are fragile and can collapse. Between public order and anarchy perhaps there are really only three regular meals.

Therefore, the legislator had to react. IT security has


Situation in 2013
Information security management
Information security policy
Organization of information security
Human resource security
Asset management
Access control
Cryptography
Physical and environmental security
Operations security
Communications security
System acquisition, development and maintenance
Supplier relationships
Information security incident management
Information security aspects of business continuity management
Compliance
ISMS
Non-IT security
IT security

Topics in ISO27001/2:2013.

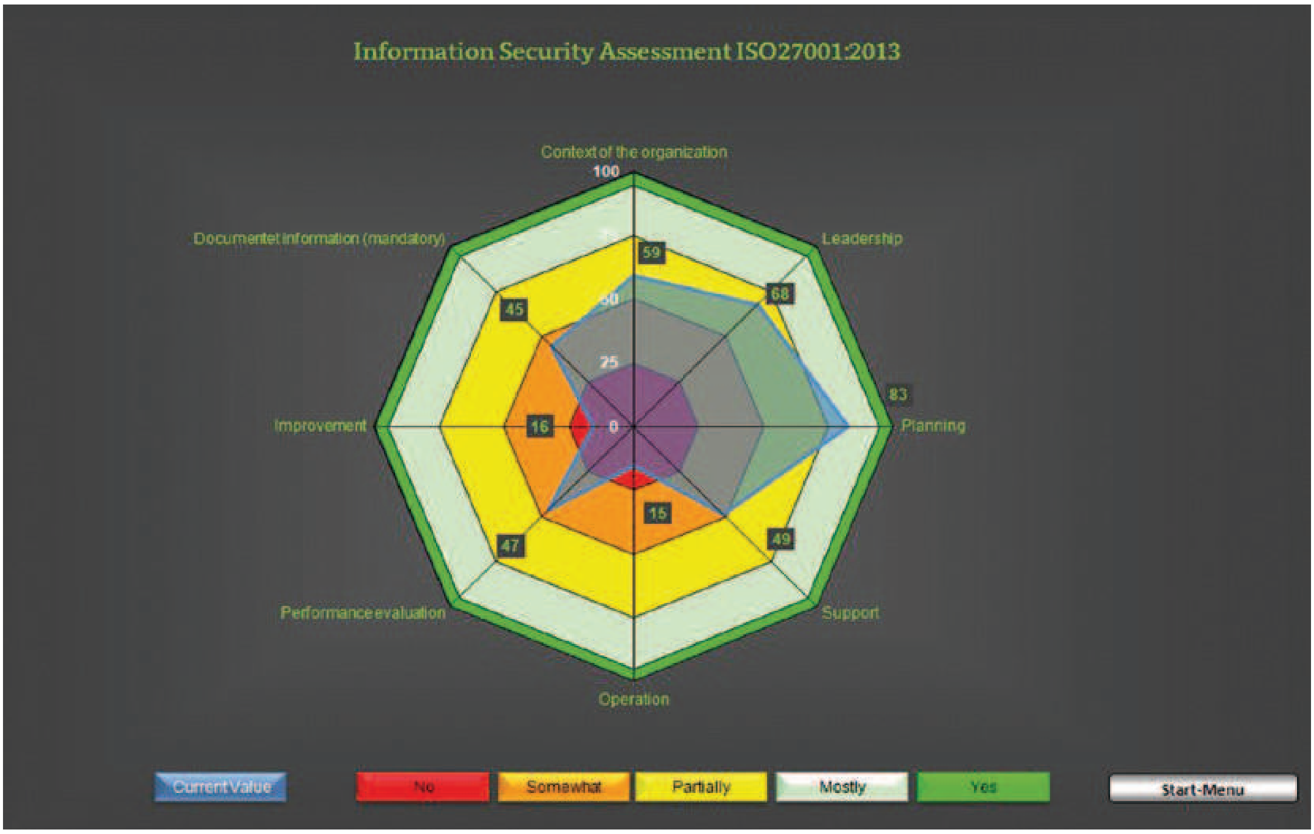


Example for a Workbook starting page to provide a gap analysis. (Source Unify).

become a case for internal security, and ever since, the Stuxnet cyber war scenarios had also become a case for external security. As early as spring 2014, the European parliament approved the EU Commission proposal for a directive on Network and Information Security (NIS). All EU member states should establish a central point for NIS reports. NIS-hotlines should be networked throughout the EU and inform each other and the competent European Agency ENISA about relevant incidents. Consequently, the Federal Ministry of the Interior (BMI) submitted a bill for an IT Security Act. The draft stipulates that key federal agencies such as the Federal Office for Information Security (BSI), the Federal Criminal Police (BKA), or the Federal Office for Civil Development and Civil Protection (BBK) should be reinforced and is set to expand and should be given additional competences. After the hearing of German associations in November 2014, the law will be approved before Christmas by the cabinet and introduced in the legislative process. The verifiable security levels and reporting of security incidents are considered binding, quite anonymously or anonymously filtered, through a single point of contact. It is about to finally receive transparency on the extent of the threats and share better information — without shaming the institution concerned.

In addition to the general law, all sector-specific regulations are intended to cover the various security requirements of enterprises and institutions in the various critical sectors. On the other hand, efforts in the public sector are thus required for the coordination, support, and monitoring of industries. There is still a considerable need for organisation at state institutions. This can go up to new-cutting of ministries and federal agencies, in which the responsibilities for cyber security are yet widely distributed. Because, "industry-specific regulations" means "sector-specific regulations," and thus a formation on the specific risks and needs in the sectors.

These days, all "critical national infrastructure" in Germany is divided into 9 sectors: energy, health, ICT, transport and traffic, media and culture, water, financial economy, nutrition, as well as state and administration. These cannot be grouped together — from different security requirements and for economic reasons. Not every organisation has to take everything into account. The bank has slightly different requirements than the energy network operators. What counts is a



Example for a spider diagram.

common, verifiable minimum security level. Equal to other security laws and their monitoring, the risk-based thinking is important, and the staff within the proper authorities must coordinate the activities accordingly.

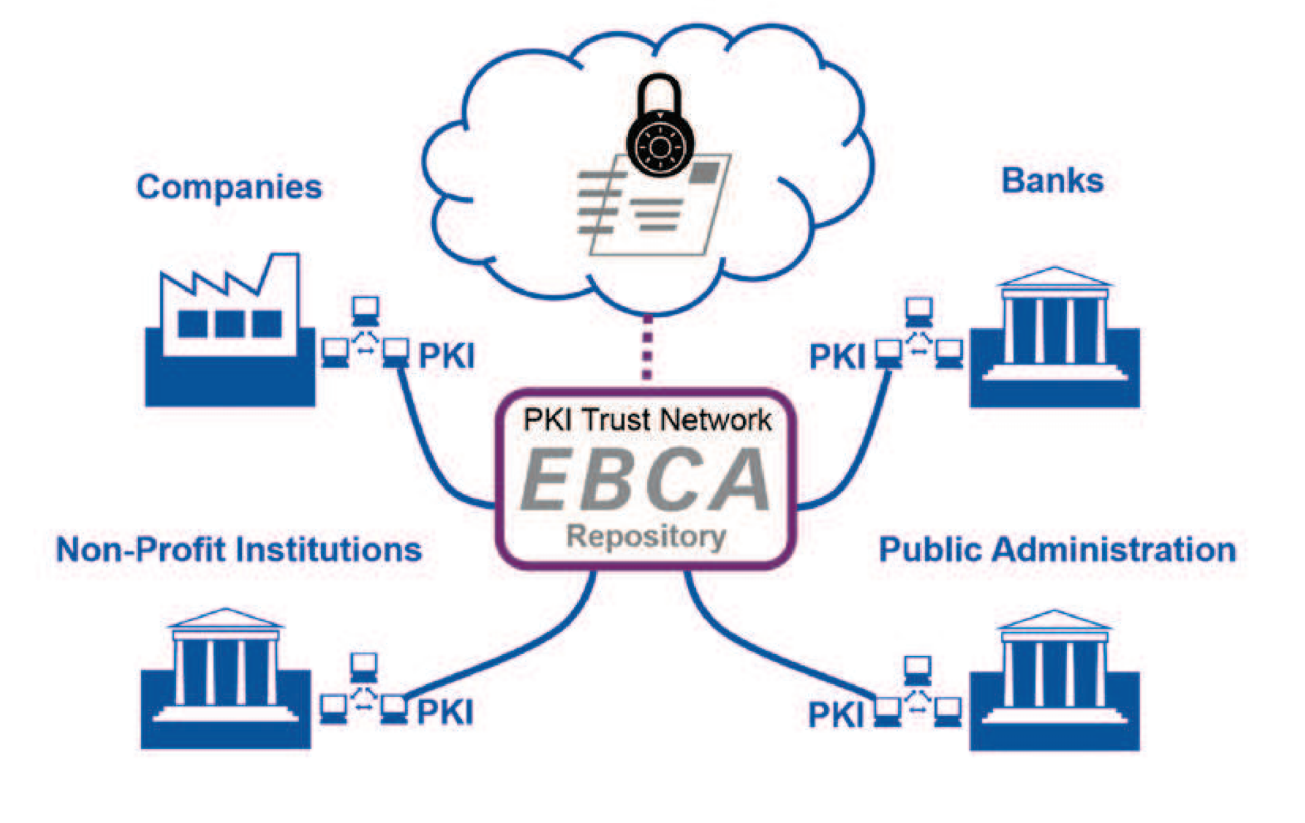
VERIFIABLE MINIMUM SECURITY LEVEL

With the standard series ISO 27000 a universally accepted international standard for information security had been established. In 2013, the standard requirements ISO 27001 and the supporting Best Practice catalog ISO 27002 were revised and harmonised (formerly issued in 2005 as BS7799 successor).

The standard series primarily aims at the development of the Information Security Management System (ISMS). This is a remarkable finding in the standardisation. Of course, extensive technical measures must be applied to succeed in the constant race between attackers and security. But the decisive factor is a powerful security organisation that strategically makes the right decisions based on operational risk management. As the name implies, the organisation establishes a management system for the area and ensures that appropriate processes are lived.

The first step in the ISMS implementation asks for the current state or, more precisely, for the difference with the target state, that the standards mentioned above prescribe. The generally accepted term is gap analysis. Actually, the gap analysis is a full audit in which no aspect of information security may be omitted.

However, this step does not decide over an ISO 27001 certificate but instead highlights and conveys a different image to all parties at the organisational and technical information security. This gap analysis is usually performed in the form of interviews, which are to be verified. For this, the interviewer must examine the standards very carefully, because several points are often required in one sentence as binding. These requirements can then be presented in different degrees of compliance that must be rated highly differentiated, to see where you stand in the required implementation. Estimates in the form of six-



Working principle of the TeleTrusT European Bridge CA. (Source: TeleTrusT – IT Security Association Germany).

stage "grades" are suitable. Bad differentiations such as "very satisfied", "partially met", "not satisfied" are unsuitable.

Guidelines appear as the following questions – may use the mnemonic term DRIVE:

- **D** Documented:
  Is this adequately documented?
- **R** Responsibility:
  Is responsibility allocated and fully accepted?
- **I** Implemented:
  Is the requested range ("control") implemented?
- **V** Verifiable:
  Could the interviewee (theoretical and practical) easily submit evidence?
- **E** Effectiveness:
  Is the effectiveness of measures evaluated?

It is not only about technical measures but rather clearly defined organisational responsibilities, demonstrable implementation, and documented processes for measured success. One cannot help but check all areas in the gap analysis. At Unify, one of the TeleTrusT members, a so-called workbook is used that covers all standard requirements. It includes approximately 2,000 questions that can be rated and graphically presented in a variety of evaluations. To some extent, information and ideas should be recorded in a comment box, so that they are not lost. Only when the gap analysis is present can one anticipate which implementation of sub-projects is necessary for each company to get a successful certification.

Given the demands of the revised ISO 27001:2013 it is apparent that the management support is very important. An external auditor will examine carefully whether the ISMS project and the ISMS idea has support from the management. But even in the technology partially different priorities had to be set. The ISO 27002:2013, compared to the standard version of 2005, enhances cryptography and even has created its own "control". Passwords still cannot be replaced, but each company must increasingly seize cryptographic requirements, specifically use them, and bindingly regulate the use of cryptographic key material in a separate set of regulations/policy labour law. An issue often being faced are the own company's borders.

Encryption and electronic signature/strong authentication are often well established only within its own network. Once cross-organisational business processes are to be protected, the application of the use of cryptographic methods, such as PKI, lacks.

New forms of cooperation in the market, such as Industry 4.0 or Smart Grid, however, are highly dependent on a smooth, secure, electronic business transaction. A central directory service for PKI certificates and public cryptographic keys is sought after by many industries, which have to work closely together in market communication or with customers and partners. So far only a few industries have successfully established such services, mainly in B2B traffic. With confidential and binding communication with smaller partners and end users, progress is still very low. Still, countless billions of unencrypted e-mails containing sensitive content are sent over public networks. There should be at least a virtual directory service, in which each organisation or company publishes its certificates independently. A prime example is the TeleTrusT European Bridge CA (EBCA), a project of the IT Security Association Germany (TeleTrusT). Participants in the EBCA form a network of trust and automatically find the key material of the communication partner.

IT has become such a central element of our national economy that modern communities are highly sensitive to disturbances or even attacks. This is particularly evident in the energy supply, but all other areas of public life are also affected by massive cyber attacks. Even short-term disruptions of the day area could cause massive economic losses. Thus, cyber ??security has actually become a question of internal and external security and must be treated with the priority corresponding to their risk potential in the various sectors of the critical infrastructure in the legislative, executive, and judicial law. In our networked world, information security has become a survival factor in the economy. ■

REFERENCE

1. KRITIS-Strategy http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/SicherheitAllgemein/kritis.html (17.06.2009).

ABOUT THE AUTOR

For 30 years, **Dr. Kafitz** has been working at Siemens or affiliated companies of Siemens. Furthermore, he has been dedicated himself to information security for over 20 years.

His work focuses primarily on Public Key Infrastructures (PKIs) and Information Security Management.

In the field of PKI, Dr. Kafitz manages, on behalf of Unify, the TeleTrusT European Bridge CA, an association of PKI-operators with well-known members, such as E.ON, the German Federal Bank, EADS, Siemens, Deutsche Bank, and not least the Federal Office for Information Security (BSI) itself.