

IT-Sicherheit als Standard

IT security as a standard

Immer mehr Vorschriften regeln die Ansprüche an IT-Sicherheitsstandards in Unternehmen. Lutz Neugebauer, Referent Sicherheit beim BITKOM, stellt die wichtigsten vor.

An increasing number of mandatory requirements are coming to determine what is expected of IT security standards in companies. Lutz Neugebauer, BITKOM Head of Security Division, gives an account of the most important ones.

D

EIN ÜBERBLICK ÜBER GELTENDE STANDARDS

Die Normen, Vorschriften und Gesetze, Verfahrensanweisungen, Vorgehensmodelle, die heute unter den Begriff Standards im Rahmen der IT-Sicherheit fallen, sind extrem vielfältig und für Einzelpersonen kaum zu überblicken. Eine grobe Einteilung lässt sich durchführen, wenn man zwischen fünf großen Gruppen unterscheidet. In der ersten Gruppe sind alle grundlegenden Standards zum IT-Sicherheits- und Risikomanagement zusammengefasst. Dazu gehören beispielsweise das IT-Grundschutzhandbuch des BSI und die bekannte Norm ISO/IEC 27001 (Anforderungen an ein Informationssicherheits-Managementsystem) oder auch die Normen für IT-Netzwerksicherheit (ISO/IEC 18028). Die zweite Gruppe umfasst heute gängige Strukturmodelle, wie beispielsweise ITIL und COBIT, die auch sehr intensiv Sicherheitsaspekte beleuchten. Die dritte Gruppe sind bekannte Vorschriften und Gesetze wie das KonTraG, Basel II, SOX und auch das Bundesdatenschutzgesetz. Eine vierte Gruppe setzt sich aus Standards für die Prüfung und Evaluation von IT-Sicherheit zusammen.

Das sind beispielsweise die so genannten „Common Criteria“, die auch als ISO-Normen beschrieben sind. In der fünften Gruppe sind schließlich die Normen für spezielle kryptographische und IT-Sicherheitsverfahren wie Verschlüsselung oder digitale Signaturen und die Standards der physischen (u.a. Brandschutz, Einbruchhemmung etc.) Sicherheitsverfahren zusammengefasst.

Die Normen, Vorschriften und Gesetze, Verfahrensanweisungen, Vorgehensmodelle sind kaum zu überblicken.

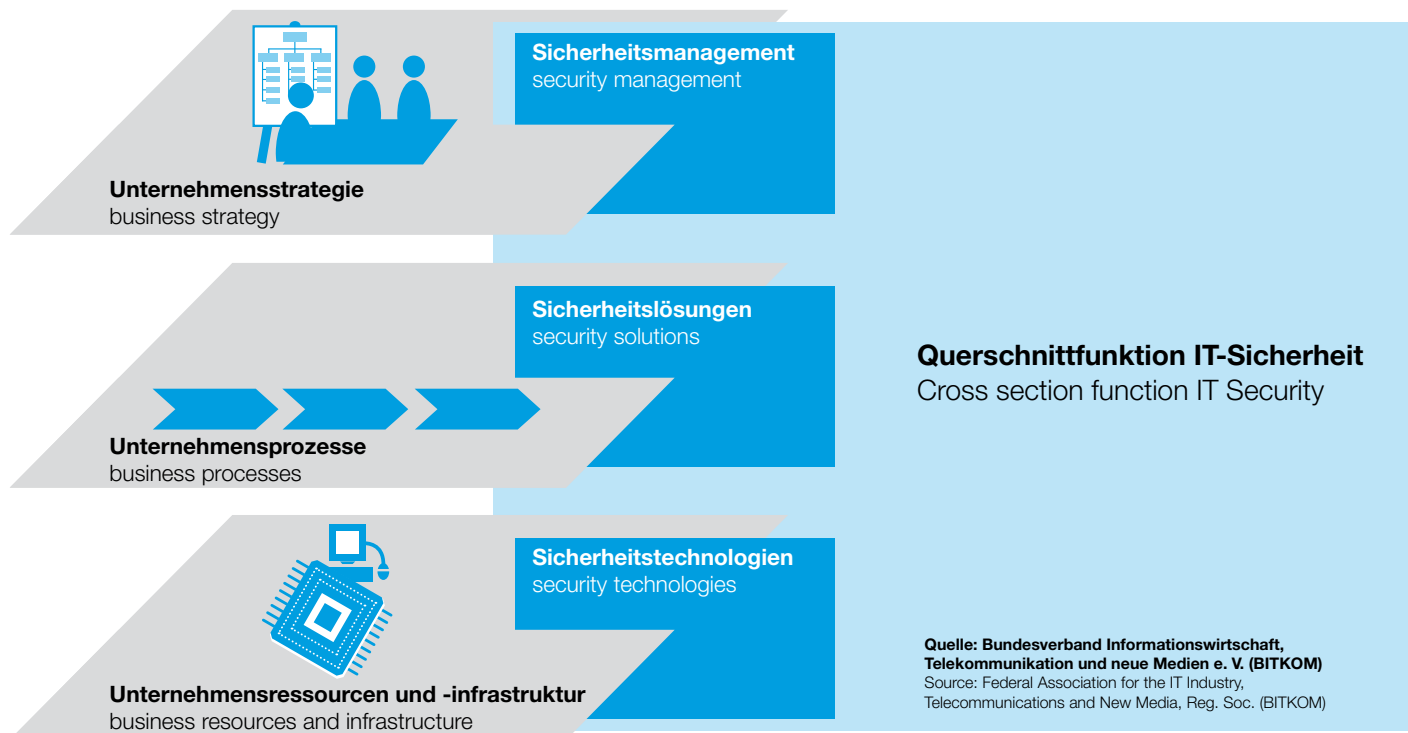
E

AN OVERVIEW OF THE APPLICABLE STANDARDS

The norms, ordinances and laws, procedural instructions and procedural models that today come under the heading of standards in the context of IT security are extremely varied, and the ordinary individual is hardly likely to have a clear view of them. We can carry out a broad classification if we divide them into five major groups. The first group comprises all fundamental standards for IT security and risk management. These include for example the BSI's Basic IT Protection Manual and the well-known ISO/IEC 27001 standard for information security management systems, as well as the ISO/IEC 18028 standards for network security. The second group consists of structural models current today, like ITIL and COBIT, which also cast a great deal of light on security aspects. The third group includes well-known ordinances and laws like KonTraG, Basel II, SOX and the Bundesdatenschutzgesetz [Federal Data Protection Act]. A fourth group consists of standards for the scrutiny and evaluation of IT security. These include for example the so-called 'common criteria', which are also embodied in ISO standards. The fifth group, finally, comprises the standards for special cryptographic and IT security procedures, like digital signatures and encryption, as well as the standards for physical security (protection against fire, deterring break-ins etc.).

LEGAL OBLIGATIONS AND COMPETITIVE ADVANTAGES

An actual obligation to comply with IT security standards can in principle only be derived from statutory prescriptions and requirements that apply to Germany. The theme of compliance – that is to say, the demonstration that certain regulations, laws and standards are being observed in the field of IT security – is however continuing to gain in importance. Alongside the legal aspects – for example, in connection with the legal liability of a company's management board – purely business management considerations also have a part to play. The use of standards – above all in the field of IT security – can contri-



RECHTLICHE VERPFLICHTUNG UND WETTBERWERBSVORTEIL

Eine tatsächliche Verpflichtung zur Beachtung von IT-Sicherheitsstandards lässt sich prinzipiell nur aus den für Deutschland geltenden gesetzlichen Vorgaben und Vorschriften ableiten. Das Thema „Compliance“, also der Nachweis, dass bestimmte Regeln, Gesetze, Standards im Themenbereich IT-Sicherheit eingehalten werden, gewinnt allerdings weiter an Bedeutung. Neben den juristischen Aspekten, zum Beispiel im Rahmen der Haftung der Geschäftsführung einer Unternehmung, spielen hier auch rein betriebswirtschaftliche Gründe eine Rolle. Die Nutzung von Standards – auch gerade im Bereich der IT-Sicherheit – kann zur Vermeidung von Kosten beitragen. Dienstleister und ihre Leistungen können so besser kontrolliert werden. Auf der anderen Seite kann die Einhaltung von IT-Sicherheitsstandards auch als ein Verkaufsargument für eigene Produkte dienen und sich damit zum Wettbewerbsvorteil entwickeln.

DER BLICK IN DIE ZUKUNFT

Mit fortlaufender technischer Entwicklung werden sich auch Normen und Standards weiterentwickeln. Dies ist für ein Einzelunternehmen zunächst kein Nachteil, da alles, was Sicherheit und Verlässlichkeit für das eigene Handeln und das von Lieferanten und Partnern verspricht, zunächst einmal positiv bewertet werden sollte. Die Entwicklung auf der Gesetzgebungsseite lässt sich an dieser Stelle nur schwer vorhersagen. Es ist nicht unwahrscheinlich, dass insbesondere bei der EU in Brüssel Gesetze und Verordnungen entwickelt werden, die zukünftig Einfluss auf die IT-Sicherheitsstandards nehmen werden. Aktuell seien die Diskussionen zum Schutz von Kritischen Infrastrukturen genannt, zu denen die EU-Kommission auch IT-Systeme und Netze zählt.

Den Leitfaden „Kompass der IT-Sicherheitsstandards“ von BITKOM und DIN finden Sie auf der Seite des BITKOM zum Download: www.bitkom.org/de/themen_gremien/36737_31037.aspx

bute to reducing costs. Service providers, and the services they offer, can also be more closely monitored on this basis. Then again, adherence to IT security standards may also serve as a sales argument in favour of a company's products, and so function as a competitive advantage.

FUTURE PROSPECTS

As a result of ongoing technical development, the relevant norms and standards are going to go on developing as well. For individual companies this is not in the first instance disadvantageous, as anything that promises better security and reliability – for a company's own activities and those of its suppliers and partners – should on the face of it be seen as a positive development. Developments on the side of the legislature are difficult to predict at this point. It is not out of the question that laws and ordinances may be developed, especially by the EU in Brussels, that will have future implications for IT security standards. We may point to the current discussions in connection with the protection of 'critical infrastructures', which in the eyes of the EU commission includes IT systems and networks.

The BITKOM / DIN guideline, 'Compass for IT Security Standards' will be found at the BITKOM website and may be downloaded: www.bitkom.org/de/themen_gremien/36737_31037.aspx



LUTZ NEUGEBAUER
HEAD OF SECURITY DIVISION, BITKOM