SPLITTER

# Informationssicherheit im ITDZ Berlin: Zentraler Bestandteil unserer Unternehmenskultur

**Die Themen Informationssicherheit und Datenschutz sind bereits seit Jahren wichtige Themenfelder für IT-Dienstleister wie das ITDZ Berlin. Sie sind auf Grund aktueller Entwicklungen sowie der damit verbundenen medialen Präsenz weiter in den Fokus gerückt. Die zentrale Herausforderung besteht darin, adäquate Maßnahmen zu definieren und umzusetzen, um die vorhandenen Informationen sowie die Systeme angemessen zu schützen. Sicherheitsvorfälle wie die Offenlegung oder Manipulation von Informationen können weitreichende, geschäftsschädigende Auswirkungen haben. Aus diesem Grund müssen Informationssicherheit und Datenschutz in Entscheidungsprozesse immer mit einbezogen werden.**

Die Bedeutung und Tragweite von Informationssicherheit und Datenschutz hat das ITDZ Berlin bereits früh erkannt und im Haus ein Informationssicherheitsmanagementsystem (ISMS) nach den Empfehlungen des BSI etabliert, um Informationssicherheit mit Hilfe des IT-Grundschutzes im ITDZ Berlin übergreifend zu steuern und weiter optimieren zu können.

Die Methodik des IT-Grundschutzes bietet eine hervorragende, standardisierte Grundlage, um (IT-)Compliance-Vorgaben, insbesondere die Vorgaben und Empfehlungen des Landes sowie die des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umzusetzen und damit zur Steigerung der Informationssicherheit beizutragen. Informationssicherheit wird im ITDZ Berlin strategisch durch den Vorstand, die Unternehmenssteuerung (durch den IT-Sicherheitsbeauftragten) und das ISMS-Team gesteuert. Die konkrete Ausgestaltung sowie die Umsetzung von Sicherheitsmaßnahmen obliegen allen, egal ob Mitarbeitende oder Führungskraft.

Mit dem Projekt „LKG-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz“ hat das ITDZ Berlin schon im Jahr 2012 ein Pilot-Projekt initiiert und gemeinsam mit den Fachbereichen wichtige Meilensteine zur weiteren Verbesserung der Informationssicherheit erreicht.

### Der IT-Grundschutz

Die Umsetzung des IT-Grundschutzes und die dazugehörige Zertifizierung in einer IT-Organisation von der Größe des ITDZ Berlin ist, wenn es sorgfältig durchgeführt wird, eine komplexe Herausforderung. Die Methodik des IT-Grundschutzes bietet jedoch die Möglichkeit, in einem standardisierten Prozess Informationssicherheit bezogen auf einen jeweils zu definierenden IT-Verbund umzusetzen. Mit Hilfe des Schichtenmodells und eines modularen Baukastenprinzips können potentielle Gefährdungen gezielt mit Maßnahmen behandelt werden.

Es empfiehlt sich zur Erstellung von Sicherheitskonzepten, insbesondere ➔

zur Abbildung aller notwendigen BSI-Anforderungen, zur nachhaltigen Dokumentation und zur Erstellung der notwendigen BSI-Referenzdokumente für eine Zertifizierung nach IT-Grundschutz ein ISMS-Tool zu nutzen. Die Nutzung des Tools ermöglicht Sicherheitskonzepte ohne großen Aufwand kontinuierlich fortzuschreiben. Dies wiederum führt mittelfristig zu einer Entlastung der Mitarbeitenden.

### Aktueller Stand des BSI-Zertifizierungsprojektes

Im Rahmen des BSI-Zertifizierungsprojektes des ITDZ Berlin soll das interne, auf SAP-basierende logistisch-kaufmännische-Gesamtsystem (LKG) nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert werden. Nach einer Bestandaufnahme notwendiger und bereits umgesetzter BSI-Maßnahmen wurden die im ITDZ Berlin geltenden Richtlinien und Vorgaben im Bereich der Informationssicherheit und des Datenschutzes weiter verbessert und aktualisiert. Anfang des Jahres 2014 fanden eine Dokumentenprüfung sowie intensive Vor-Ort-Prüfungen durch einen externen Auditor statt, bei denen die konkrete Umsetzung einzelner Sicherheitsmaßnahmen in verschiedenen Fachbereichen im ITDZ Berlin geprüft wurde. Das Audit war erfolgreich. Dem ITDZ Berlin wurde das Auditor-Testat „IT-Grundschutz Einstiegsstufe“ erteilt.

Die nächste und abschließende Phase des Projektes hat die finale Zertifizierung des definierten IT-Verbundes nach ISO 27001 auf Basis des IT-Grundschutzes zum Ziel. Gemeinsam mit den Fachbereichen werden derzeit die notwendigen Grundlagen geschaffen, um die Voraussetzungen für eine erfolgreiche Zertifizierung zu erfüllen. Der Abschluss des Projektes wird die Auseinandersetzung mit dem Thema Informationssicherheit nicht beenden, da Informationssicherheit ein kontinuierlicher und dauerhafter Prozess ist.

### Nutzung von Synergien

Das Vorgehen nach IT-Grundschutz schafft Transparenz und eindeutige Verantwortlichkeiten. Ebenso können damit auch notwendige organisatorische und technische Anforderungen bewertet und bearbeitet werden. Durch die Nutzung eines ISMS-Tools können erfasste und bewertete Komponenten sowie umgesetzte Maßnahmen in anderen Kontexten für andere, notwendige Sicherheitskonzepte und Risikoanalysen weitergenutzt werden, ohne größere Aufwände erneut zu generieren.

*Karsten Pirschel*
IT-Sicherheitsbeauftragter ITDZ Berlin und Projektleiter des BSI-Zertifizierungsprojektes

*Sven Malte Sopha*
Cassini Consulting

### Zertifizierung des logistisch-kaufmännischen Gesamtsystems

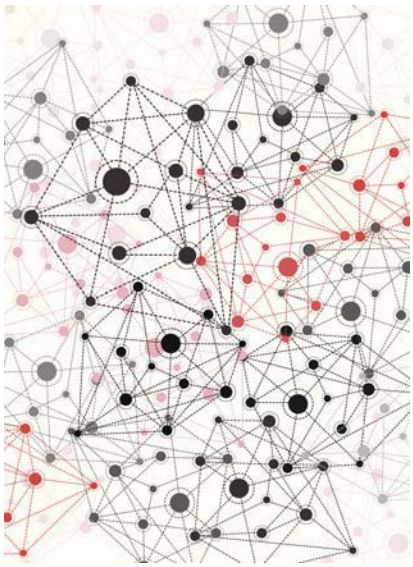
**Ziel ist die Zertifizierung des logistisch-kaufmännischen Gesamtsystems (LKG) des ITDZ Berlin nach ISO 27001 auf der Basis von IT-Grundschutz, beispielhaft für vom ITDZ Berlin betriebene Verfahren mit hohem Schutzbedarf.**

**Gegenstand der Zertifizierung ist die Unternehmens-IT des ITDZ Berlin an allen Unternehmensstandorten in Berlin inklusive des High Secure Data-Centers. Der Schwerpunkt liegt dabei auf den kritischen Geschäftsprozessen der Fachbereiche. Dazu zählen insbesondere das interne SAP-basierende logistisch-kaufmännische Gesamtsystem, sowie die zum Betrieb notwendige IT-Systeme einschließlich der Netzwerk- und Kommunikationsverbindungen. Verfahren, die von Kunden in eigener Verantwortung betrieben werden oder die das ITDZ Berlin in der Verantwortung des Kunden betreibt sowie das Landesnetz Berlin sind nicht Bestandteil des Untersuchungsgegenstandes.**

## CERT für das Land Berlin wird aufgebaut

**Das CERT des Landes Berlin wird ein Service zur Erhöhung des Informationssicherheitsniveaus in der Berliner Verwaltung und eine Antwort auf die gestiegene Gefährdungslage in der IT-Sicherheit ein.**

Ob es um den millionenfachen Identitätsdiebstahl durch Hacken von E-Mail-Konten, das Ausspähen von Bankverbindungsdaten von Telekommunikationskunden oder auch den Informationsabfluss von Fahndungsdaten aus dem Schengener Informationssystem bei der dänischen Polizei geht – die Gefährdung von schützenswerten Daten und der zuverlässigen Erbringung von IT-Services wächst ständig.



najewei/iStock/Thinkstock

Schwachstellen in der Programmierung von Systemen oder Verfahren sind aufgrund der hohen Komplexität kaum zu verhindern. So ist es Angreifern über speziell dafür angefertigte Programme, sogenannte Exploits, die im Internet quasi jedem zur Verfügung stehen, z. T. sehr einfach möglich, diese für ihre meist kriminellen Interessen auszunutzen.