ZT IT-KOLUMNE

IT-Sicherheitsmanagement nach ISO 27001 Grundschutz

Der Wunsch nach umfangreicher Sicherheit eigener IT-Infrastrukturen wächst bei Organisationen und Unternehmen. Eine Zertifizierung nach ISO 27001 Grundschutz hilft dabei, die erforderlichen Maßnahmen umzusetzen und Vertrauen bei den Kunden zu stärken. Dieser Artikel gibt einen Einstieg in die komplexe Materie.

Die Sicherheitsanforderungen an informationsverarbeitenden IT-Systemen sind in den letzten Jahren extrem angestiegen. Nicht zuletzt durch raffinierte und hochkomplexe Cyberangriffe müssen Organisationen und Unternehmen ihre Computersysteme, die immer mehr mit dem Internet verbunden sind, dagegen absichern. Da auch der Trend sehr stark zu cloudbasierten Anwendungen geht, geraten die Geschäftswerte (alles, was für die Geschäftstätigkeit relevant ist) und Prozesse, die in den informationsverarbeitenden IT-Systemen verarbeitet werden, in den Fokus von professionellen Hackern. Ziele der Hackerangriffe sind:

- Beschädigung oder Zerstörung von IT-Infrastrukturen oder Server-Systemen
- Spionage (Industrie und Militär)
- Beschädigung oder Zerstörung von Infrastrukturen von Ländern/Kommunen durch gezielte Angriffe auf deren IT-Infrastrukturen von Terroristen.

Da die Cyberangriffe immer bedrohlicher und umfangreicher werden, müssen Organisationen und Unternehmen durch Schutzmaßnahmen das Vertrauen in sich und ihre IT-Infrastrukturen weiterhin sichern. Durch eine ISO 27001-Zertifizierung auf Basis von Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) werden die IT-Infrastrukturen mithilfe von Anforderungskatalogen auf Sicherheit analysiert, geprüft und die Maßnahmen beschrieben. Die Organisationen und Unternehmen können dann mittels IT-Grundschutz der BSI die vorgegebenen Vorgehensweisen und Einzelmaßnahmen konkret umsetzen.

Ich möchte an der Stelle klar betonen, dass auch kleine Unternehmen ihre Unternehmensstruktur und informationsverarbeitenden IT-Systeme auf Sicherheit überprüfen sollten. Gerade der Mittelstand hat eine potenziell hohe Gefährdungslage und sollte entsprechende Maßnahmen ergreifen. Das BSI mit ihren Grundschutzkatalogen ist hierbei eine sehr gute Anlaufstelle.

Was ist eine Bedrohung?

Eine Begriffserklärung des BSI: „Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann.“ (Quelle: BSI)

Was bedeutet BSI-Grundschutz?

Das Ziel des BSI ist die präventive Förderung der Informations- und Cybersicherheit, um den sicheren Einsatz von Informations- und Kommunikationstechnik in Staat, Wirtschaft und Gesellschaft zu ermöglichen und voranzutreiben. Die sogenannten BSI-Standards sind im Prinzip Empfehlungen des BSI zu Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen bezüglich der Informationssicherheit. Organisationen und Unternehmen können diese Empfehlungen dann nach ihren eigenen und speziellen Bedürfnissen anpassen.

Das BSI gibt die IT-Grundschutz-Kataloge heraus, die Empfehlungen für Standardschutzmaßnahmen für typische IT-Systeme enthalten. In diesen Katalogen werden nicht nur technische, sondern auch organisatorische, personelle und infrastrukturelle Maßnahmen erörtert. Das BSI ist die zentrale Zertifizierungsstelle für die Sicherheit von IT-Systemen in Deutschland (Computer- und Datensicherheit, Datenschutz). Prüfung und Zertifizierung ist möglich in Bezug auf die Standards des IT-Grundschutzhandbuchs. Der IT-Grundschutz wurde von der BSI in einem Grundschutzhandbuch beschrieben und schildert die IT-Sicherheit einschließlich Datenschutz. Mittlerweile hat sich der IT-Grundschutz insofern weiterentwickelt, als sich das Sicherheitsmanagement an der ISO 27001 ausrichtet. Für die Maßnahmenauswahl sind weiterhin die Maßnahmenkataloge des IT-Grundschutzes und für die Gefährdungsanalysen ebenfalls die sogenannten Gefährdungskataloge zu verwenden.

Der IT-Grundschutz geht von einer für das IT-System üblichen Gefährdungslage aus und hat hierfür passende Gegenmaßnahmen parat. So kann ein Sicherheitsniveau erreicht werden, das in den allermeisten Fällen ausreicht und damit die viel teurere Risikoanalyse vollständig ersetzt. Sollte der Sicherheitsbedarf größer sein, kann der IT-Grundschutz als Grundlage für weitere Maßnahmen genutzt werden.

Vorbereitung auf die Zertifizierung

Sollte sich ein Unternehmen für eine ISO 27001 Grundschutz-Zertifizierung entschieden bzw. für die Zukunft geplant haben, sollten unbedingt folgende wichtige Forderungen vorab schon mal geprüft werden:

- Eine gelenkte Dokumentation (ist bewertet, genehmigt, lesbar, ...).
- Sicherung von beweiserheblichen Aufzeichnungen.
- Die Organisation von internen Audits.
- Verbesserung von eingeführten Prozessen.

Wie im IT-Grundschutzhandbuch beschrieben, werden zuerst alle zu prüfenden „Gegenstände“ in einem Datenschutz-/Datensicherheitskonzept vorgestellt. Ein Sicherheitscheck vervollständigt dann die erstellten Konzepte. Folgende entscheidende Themen sollten hierbei berücksichtigt werden:

Datensicherheitskonzept

- Organisation und Regelungen
- Gebäude und Räume
- Architektur der IT-Infrastruktur bzw. Systeme
- Anwendungen
- Personal sowie Datenschutz- und Sicherheitsmanagement

Istzustand Analyse und Verbesserung

- Ist der Umgang mit personenbezogenen Daten gesetzeskonform?
- Sind die Ziele der Sicherheit angemessen bzw. adäquat?
- Sind die im Datensicherheitskonzept beschriebenen Maßnahmen zur Sicherheit der IT-Infrastruktur ausreichend?
- Sind Internetzugang und Server der IT-Infrastruktur sicher?

Zur Durchführung einer Analyse werden Standard-Informationen aus dem IT-Grundschutzhandbuch verwendet. Das Ergebnis der Analyse sind Verbesserungsvorschläge, die mit den Auftraggebern zusammen diskutiert werden, sodass dann die erstellten Datenschutz- und/oder Datensicherheitskonzepte geändert bzw. angepasst werden können.

Ablauf der Zertifizierung

Eine Zertifizierung nach ISO 27001 auf Basis des IT-Grundschutzes durch das BSI liefert den Nachweis, dass die Organisation oder das Unternehmen organisatorischen, infrastrukturellen und technischen Maßnahmen der Informationssicherheit für einen definierten Geltungsbereich oder für ihr gesamtes Unternehmen getroffen hat. Ein sogenannter „BSI lizenzierter IT-Grundschutz bzw. ISO 27001 Auditor“ führt die Umsetzung der in den Standards beschriebenen Maßnahmen durch. Das Ergebnis des Auditors ist ein Prüfbericht. Sind alle Maßnahmen umgesetzt, kann der Bericht an das BSI gesendet und eine Zertifizierung beantragt werden. Das BSI erteilt dann ein „ISO 27001 Zertifikat auf Basis von IT-Grundschutz“. Dieses Zertifikat ist international anerkannt und aussagekräftiger als ein reines ISO 27001 Zertifikat, da in diesem Fall – zusätzlich zu den allgemeinen Anforderungen der ISO/IEC 27001 auch – die konkreten Anforderungen des Grundschutzes eingehalten werden müssen.

Fazit und Ausblick

Die Gefährdungslage für informationsverarbeitende Systeme und somit auch für ganze Organisationen und Unternehmen wird auch in Zukunft weiter ansteigen. Es sei den Organisationen und Unternehmen angeraten, sich für die Sicherheit ihrer IT-Systeme zu interessieren. Ob eine Sicherheitszertifizierung notwendig ist, muss individuell entschieden werden. Auch die vorgeschlagenen Maßnahmen dienen nur als Orientierung und sind ebenfalls individuell an die Gegebenheiten anzupassen. Auch jede einzelne Person in einer Organisation/Unternehmen, ja, sogar in der Gesellschaft, hat die Pflicht, sich mit der Sicherheit für informationsverarbeitende Systeme auseinanderzusetzen. Ebenfalls ist das Verhalten jeder einzelnen Person im Hinblick auf Datensicherheit sehr wichtig. Man denke nur an den Umgang mit Passwörtern und vertraulichen Dokumenten. ZT

ZT Adresse

Thomas Burgard Dipl.-Ing. (FH)
Softwareentwicklung & Webdesign
Bavariastraße 18b
80336 München
Tel.: 089 540707-10
info@burgardsoft.de
www.burgardsoft.de