IT-Sicherheit mit BSI-Grundschutz

Eduardo Isaac Soto Barrera, Abogado (Mexiko)
Mag. iur. (Mx), Mag. iur. (D), Hannover

Juni 2021

Für Geschäftsführer kann mangelnde IT-Sicherheit ein erhebliches Haftungsrisiko darstellen: Beeinträchtigungen der IT oder der Verlust von Daten führen zumindest zu Betriebsunterbrechungen, oft aber auch zum Verlust von wichtigen Geschäftsinformationen und in manchen Fällen im Ergebnis zum Zusammenbruch des Unternehmens.

Dabei begehen Unternehmen typische Fehler, die ihre Sicherheit gefährden. Fehlendes Backup, fehlenden Updates bei Viren, falsche Dokumentation von Administrator-Passwörtern bis hin zu internen Angriffen sind dies nur einige Beispiele aus dem Bereich der Informationssicherheit.

Aus diesem Grund bietet das Bundesamt für Informationssicherheit (BSI) seit 2006 Methoden und eine Zertifizierung nach dem BSI-Grundschutz an, auf Grundlage der ISO 27001 und als Umsetzung der Standards 200-1 (Vorgehensweise) und 200-3 (Risikoanalyse). Das BSI-Grundschutz-Kompendium stellt auf über 800 Seiten (ohne Parallelnormen) einen umfassenden Katalog mit konkreten Maßnahmen für spezifische Risiken bereit.

Die Norm ISO 27001 zur IT-Sicherheit

Das IT-Grundschutz-Kompendium (2021) ist für Behörden, Dienstleister, Unternehmen und sonstige Institutionen entwickelt. Eine entsprechende Zertifizierung wird dabei von einem vom BSI zertifizierten externen Auditor vorgenommen. Das Programm umfasst zwei Bereiche:

Prozessbausteine

Die Prozessbausteine betreffen das gesamte IT-System oder Teile davon und umfasst

ORP Organisation und Personal:
Sensibilisierung und Schulung zur Informationssicherheit, Compliance Management

CON Konzeption und Vorgehensweise:
Verschlüsselungskonzepte, Datenschutz, Datensicherungskonzepte, das Löschen und Vernichten von Daten, Informationsaustausch und Datensicherheitsprobleme

OPS Betrieb:
interne und externe betriebliche Aspekte der Organisation, einschließlich Dritter, z.B. Schadprogrammschutz und Outsourcing für Kunden, Telearbeit, Cloud-Nutzung,

ISMS Managementsystem für Informationssicherheit

DER Detektion und Reaktion:
Reaktion auf Sicherheitsvorfälle, Notfallmanagement

Systembausteine

Systembausteine behandeln einzelne Objekte oder individualisierbare Gruppen.

APP Anwendungen:
Allgemeine Regeln zu E-Mail-Client und -Server, Office-Produkte, Webserver und Relationale Datenbank-Systeme

SYS IT-Systeme:
Sicherheitsfragen von Endgeräten wie Smartphones und Tablets sowie Druckern, Kopierern und Multifunktionsgeräten, auch systemspezifische Aspekte von Servern und Desktop-Systemen

IND Industrielle IT:
Prozessleit- und Automatisierungstechnik, Allgemeine ICS-Komponente und Speicherprogrammierbare Steuerung (SPS), Maschine

NET Netze und Kommunikation:
Netz-Management, der richtigen Implementierung von Firewalls, der Nutzung des firmeneigenen WLANs, VPN, VoIP, Faxgeräte und Faxserver, alles im Bereich der Kommunikation und nicht nur auf zentralen IT-Systemen

INF Infrastruktur:
Gebäude, Rechenzentrum, Serverräume, Büro- und mobile Arbeitsplätze, Besprechungs-, Veranstaltungs- und Schulungsräume, Fahrzeuge, Allgemeines

BSI Standards

Für eine effektive Anwendung des IT-Grundschutz-Kompendiums werden die folgenden Standards verwendet:

BSI-200-1: bestimmt, wie ein ISMS zu entwickeln ist. Es richtet sich an die Verantwortlichen für die Informationssicherheit, Sicherheitsexperten, Sicherheitsbeauftragte, etc.

BSI-200-2: setzt auf der Initiierung bzw. Ergänzung eines ISMS auf und beschreibt die verschiedenen Arten der Sicherheit: Standard-, Basis- und Kern-Absicherung, einschließlich ihrer Geltungsbereiche.

BSI- 200-3: bezieht sich auf die Risikoanalyse mit der Erstellung einer Gefährdungsübersicht, Risikoeinschätzung, Risikobehandlung, etc.

BSI-200-4: zielt auf die Entwicklung des sogenannten "Business Continuity Model" (BCM). Es richtet sich an BCM-Beauftragte, Krisenstabsmitglieder, Sicherheitsverantwortliche und andere, die mit dem Management von Notfällen und Krisen technischen und nicht-technischen Ursprungs betraut sind.

Risikoeinstufung

Für eine zutreffende Problemdiagnose muss das Unternehmen seine Risiken richtig einschätzen. Dazu dient eine Methodik zur Einschätzung der Bedrohungen, Schadenspotenziale, Eintrittshäufigkeiten und der daraus resultierenden Risiken.

Risikoeinstufung

Die Risikoeinstufung erfasst die Eintrittswahrscheinlichkeit von Risikoereignissen

- Selten alle fünf Jahre
- mittel alle fünf Jahre bis 1x im Jahr
- häufig einmal im Jahr bis 1x pro Monat
- sehr häufig mehrmals im Monat

Ein anderer Risikoparameter ist die potenzielle Schadenshöhe, klassifiziert als:

- vernachlässigbar
- begrenzt
- beträchtlich
- existenzbedrohend.

Die Parameter Eintrittswahrscheinlichkeit und Schadenshöhe werden miteinander kombiniert, um das Risiko im Ergebnis einzuordnen.

Dabei sind bestimmte Risiken nicht mit bestimmten Grundsätzen vereinbar, z.B. der Verfügbarkeit (Feuer, Naturkatastrophen, Zerstörung von Geräten oder Datenträgern, Personalausfall, Sabotage, Datenverlust etc.), der Integrität (Manipulation von Informationen, Integritätsverlust schützenswerter Informationen, etc.), der Vertraulichkeit (Ausspähen von Informationen/Spionage, Abhören, Missbrauch personenbezogener Daten, etc.) oder einer Mischung aus einem oder mehreren dieser Prinzipien.

Risikobehandlung

Nach der Identifizierung und Klassifizierung eines Risikos stellt sich die Frage nach der Risikobehandlung durch

- Vermeidung (Ursachenfindung),
- Reduzierung (Änderung der Umstände),
- Verlagerung (Outsourcing, Versicherungen)
- Inkaufnahme (Positionierung am Markt)

Seine Entscheidung muss das Management dokumentieren und überwachen.

Verfahrensarten

Mit der Richtline 200-2 bietet das BSI drei Verfahrensarten zur Wahl, die sich je nach Unternehmensgröße unterschiedlich eignen:

Basis-Absicherung

Die Basis-Absicherung analysiert analog zu den BSI-Mindeststandards alle für das Unternehmen relevanten Prozesse pauschal, aber auch alle „Assets" (alles was für das Unternehmen einen Wert darstellt), für den Fall, dass sie beschädigt oder zerstört werden. Zu dieser Analyse gehören auch Sicherheitsrisiken, solange sie kein existenzielles Risiko für das Unternehmen darstellen. Diese Methode ist ein Einstieg für kleine Unternehme und kann auch von nicht spezialisierten Mitarbeitern durchgeführt werden. Die Aktionsfelder bei der Basis-Absicherung sind kein geschlossener Zyklus, sondern eine Einstiegsvorgehensweise.

Kern-Absicherung

Die Kern-Absicherung entspricht im Grundsatz der Basis-Absicherung, bietet aber die Möglichkeit einer ISO-27001-Zertifizierung.

Standard-Absicherung

Dieses Level bietet ebenfalls eine Zertifizierung und umfasst das ISMS. Die Standard-Absicherung ist ein geschlossener Zyklus. Es sollte in allen Abteilungen des Unternehmens eingesetzt werden, da jede ihre eigenen Merkmale hat, und die Verfahren individualisiert werden müssen.

In der Praxis werden für kleine Bereiche "mit besonders gefährdeten Assets" Sicherheitskonzepte (Kern-Absicherung) erstellt, während für die anderen Bereiche nur die Mindeststandards umgesetzt werden, die eine "Basis-Absicherung" gewährleisten. Es ist wichtig, alle technischen und organisatorischen Aspekte zu berücksichtigen. Diese sind von großer Bedeutung, um Verantwortlichkeiten und zuständige Personen zu bestimmen - unter Berücksichtigung der Informationen selbst, der spezifischen Aufgaben und betroffenen Prozesse.

BSI-200-4: Schutz von Geschäftsprozessen

Diese Norm ersetzt die bisherige BIS 100-4 und ist relativ neu (Januar 2021). Sie ist für Unternehmen zum Schutz der Verfügbarkeit der Geschäftsprozesse oder Fachaufgaben konzipiert, um das Unternehmen finanziell vor existenziellen Risiken zu schützen. Diese Prozesse sind wichtig für funktionierende Lieferketten und Leistungen Dritter, z.B. Dienstleister, Lieferanten und Versorger. Die Risiken bestehen zunehmend durch Cyber-Angriffe, insbesondere Ransomware-Angriffe, und extreme Naturereignisse. Die meisten Vorfälle sind nicht durch entsprechende Sach- und Cyberversicherungen gedeckt.

Allgemeine Aufbauorganisation (AAO)

Die AAO ist die ständige Organisationsform für die Aufgaben des täglichen Geschäftsbetriebs. Die Zuständigkeiten, der hierarchische Aufbau sowie die Kommunikations- und Entscheidungswege müssen festgelegt werden.

Besondere Aufbauorganisation (BAO)

Bei schwerwiegenden Einschränkungen, Unterbrechungen oder Ausfällen des Geschäftsbetriebs kann das Unternehmen eine BAO als zeitlich begrenzte Organisationsform einrichten und damit auf außergewöhnliche Situationen angemessen und schnell reagieren. Die BAO umfasst drei Stufen mit Reaktiv-BCMS, Aufbau-BCMS und Standard-BCMS.

Vor massiven Schadensereignissen müssen sich Unternehmen durch Prävention schützen oder angemessene Reaktion nach einem Ausfall.

Störung ist eine Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen. Sie wird von der AAO beseitigt.

Notfall ist eine aktuelle oder drohende Unterbrechung des Geschäftsbetriebs, die mindestens einen zeitkritischen Geschäftsprozess betrifft und nicht im Normalbetrieb innerhalb der maximal tolerierbaren Ausfallzeit beseitigt werden kann. Ein Notfall wird von der BAO behandelt.

Krise ist eine Situation, bei der massive Konsequenzen für das Unternehmen bestehen und die die BAO nicht mehr alleine bewältigen kann.

Diese drei Situationen können schrittweise oder aber plötzlich auftreten, so dass das Riskmanagement stets das Szenario einer Eskalation vor Augen haben und in seine Planungen und Maßnahmen einbeziehen muss.

IMPRESSUM

HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-30756-0 Fax 0511-30756-10
Mail info@herfurth.de, Web www.herfurth.de
Hannover · Göttingen · Brüssel
Member of the ALLIURIS GROUP, Brussels

REDAKTION

Leitung: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantw.)

Mitarbeit: Angelika Herfurth, Rechtsanwältin, FA Familienrecht; Sibyll Hollunder-Reese, M.B.L. (HSG), Rechtsanwältin; Günter Stuff, Steuerberater; Xiaomei Zhang, Juristin (China), Mag. iur. (D); Thomas Gabriel, Rechtsanwalt; JUDr. Yvona Rampáková, Juristin (CR); Dr. Jona Aravind Dohrmann, Rechtsanwalt; Prof. Dr. jur. Christiane Trüe LL.M. (East Anglia); Dr. jur. Reinhard Pohl, Rechtsanwalt; Konstantin Kuhle, Rechtsanwalt; Antonia Herfurth, Rechtsanwältin; Eduardo Isaac Soto Barrera, Master of Law (Mexiko); Tobias Wundram, Rechtsanwalt; Stephanie Reese, Rechtsanwältin

VERLAG

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511 - 30756-50 Fax 0511 - 30756-60
Mail info@caston.info; Web www.caston.info