IT-Sicherheitsmanagement

Ulrich Herfurth, Rechtsanwalt in Hannover und Brüssel
Eduardo Soto Barrera, Abogado (Mexiko)
Mag. iur. (Mx), Mag. iur. (D), Hannover

Juni 2021

Die Sicherheit des IT-Systems und der Schutz von Unternehmensdaten hat für jedes Unternehmen essenzielle Bedeutung. Der Totalverlust von Daten führt nach Branchenerkenntnissen in 90% der Fälle innerhalb von 12 Monaten zur Insolvenz des betroffenen Unternehmens, entweder weil die Unternehmensprozesse massiv beschädigt sind oder weil wesentliche Datenbestände zu Produktion und Kunden verloren gingen. Die Ursachen kann man einfach unterscheiden: es sind stets Unglücke oder Angriffe. Bei den Unglücken führen die stark gestiegene Komplexität und Vernetzung der IT-Systeme zu einer immer breiteren Wirkung und zu höheren Schäden. Angriffe unterscheiden sich wiederum nach Innentätern und Außentätern. Gerade die Zahl und Wucht der Außenangriffe ist in den letzten Jahren massiv gestiegen: in IT-Systemen finden sich immer wieder Sicherheitslücken, dies nutzen Angreifer inzwischen im Rahmen organisierter Kriminalität mit rasant steigendem Zuwachs aus. Cybercrime ist inzwischen, wie klassische Industrie organisiert: die Täter können Standardsoftware für maliziöse Verschlüsselungen nutzen, aufbereiten und in regelrechte Vertriebssysteme einschleusen. Das erfolgreichste Modell ist die Erpressung mit Random Software: der erste Schritt ist Sabotage, durch Verschlüsselung der Dateien sind diese nicht mehr nutzbar. Der zweite Schritt ist die Erpressung: zahlt das Unternehmen kein Lösegeld (meist in Kryptowährung), bleiben die Dateien unzugänglich. Dieses Konzept wird hunderttausendfach eingesetzt, angefangen bei massenweise kleinen Nutzern gegen Lösegeld von unter tausend Euro bis hin zu großen Unternehmen, die nicht selten mehrere Millionen Lösegeld zahlen. Viele Angriffe und Zahlungen bleiben unbekannt, weil die Opfer keine Nachahmungen provozieren wollen.

Die Sicherheit von IT-Systemen und Unternehmensdaten ist daher essenziell und eine hochrangige Aufgabe für die Unternehmensleitung.

Für Geschäftsführer bedeutet die Vernachlässigung der gebotenen IT- Sicherheit regelmäßig eine Sorgfaltspflichtverletzung und damit ein Haftpflichtrisikogegenüber dem Unternehmen.

Die Anforderungen an die notwendige IT-Sicherheit beinhalten das technische IT-System selbst (inkl. Server, Cloudsysteme, etc.), aber auch den IT-Betrieb (operativen Teil) und das IT- Sicherheitsmanagement (Risikoerkennung, Richtlinien und Überwachung).

Ein sicheres IT-System

Das IT-System umfasst alle Computer (Clients und Server), industrielle Steuerungen (Produktionsanlagen, Mobiltelefone, Smartphones, Tablets, Endgeräte wie Scanner oder Drucker, die an diese PCs angeschlossen sind), IoT-Komponenten (Webcams, Smart-

Home-Komponenten oder Sprachassistenten), Router, Switches und Firewall, und mehr.
Jedes dieser Systeme muss vollständig erfasst und beschrieben werden, insbesondere wo und wie es genutzt wird und welche Personen in welchem Umfang zugriffsberechtigt sind.
Die Geschäftsleitung muss dazu Organisationsrichtlinien aufstellen, das BSI (Bundesamt für IT-Sicherheit) bietet entsprechende Informationen zu Maßnahmen, zumindest

- Kriterien für Anschaffung und Nutzung von Soft- und Hardware
- Zugriff über nicht vernetzte Systeme
- Nutzung, Konfiguration und Entsorgung von mobilen Systemen (BYOD), ISO-27002 für Mobilgeräte und Telearbeit.
- Authentifizierung und Authentisierung
- Protokolle zum Starten und Beenden einer Sitzung
- automatische Bildschirmsperren
- Zugriff auf Managementinformationen
- Einsatz von Verschlüsselungen
-

Bei den Zugriffs- und Kontrollrechten sollte jeder Benutzer nur die unbedingt notwendigen Rechte haben. Das Unternehmen muss klar definieren, wer Administrator und wer Benutzer ist.

Prozesse im IT-Betrieb

Im Betrieb des Systems müssen möglichst alle Anwendungen und Systeme dokumentiert und durch Passwörter geschützt sein. Es muss auch eine Kontrolle der Protokolldateien, regelmäßige Backups usw. geben.
Viele dieser Anforderungen sind durch BSI-Richtlinien behandelt, insbesondere durch das inzwischen umfangreiche BSI Grundschutzkompendium noch umfassender ist die Norm ISO 27001.
Wichtig ist die Umsetzung von Richtlinien (auch für die IT-Systeme), die die Sicherung der verarbeiteten Informationen ermöglichen.

Die Richtlinien für die Infrastruktur umfassen die verschiedensten Bereiche:

- Gebäudesicherheit einschließlich der Klimatisierung von Servern.
- Stromversorgung als lokale und zentrale unterbrechungsfreie Versorgung mit Reserven bis zur Wiederherstellung für bis zu 6 Tagen
- Brandschutz mit Brandmeldeanlage, Rauchverbot und Videoüberwachung mit entsprechendem Alarm- und Überwachungssystem (kooperativ mit Datenschutzbeauftragtem und Betriebsrat)

Organisation und Governance betreffen verbindliche Richtlinien für das Verhalten der Mitarbeiter und anderen Personals. Dazu gehören

- Sicherheit, Datenschutz, Datensicherung, Datenübertragung, Datenträgervernichtung,
- Wartungs- und Reparaturarbeiten,
- Notfallvorsorge, Handhabung technischer Schwachstellen
- Recht zu Zutritt, Zugang und Zugriff und zur Vernichtung von Dokumenten

Weitere Richtlinien richten sich auf den Schutz vor Bedrohungen, sowohl durch die Nutzung von Computern als auch durch externe Bedrohung der physischen Infrastruktur selbst. Zur Abwehr ist eine kontinuierliche Schulung und Weiterbildung der Mitarbeiter unabdingbar.

Maßnahmen im IT-Sicherheitsmanagement

Das IT-Sicherheitsmanagement identifiziert potenzielle Risiken in den betrieblichen Prozessen und trifft Maßnahmen zur Systemüberwachung, Erkennung von Störungen und Schadensminimierung.

Das BSI prüft die Bundesbehörden auf IT-Sicherheit, seine sogenannten *Mindeststandards* sind aber auch für Unternehmen Maßstab, insbesondere zu den für sie relevanten Themen wie Web-Browser oder Mobile Device Management, externe Cloud-Dienste, Pro-

tokollierung und Detektion, Schnittstellenkontrollen, Transport Layer Security (TLS) und mehr. Weiter Standards befinden sich in Vorbereitung

Informationssicherheits-Managementsystem (ISMS)

Mit einem Informationssicherheitsmanagementsystem (*ISMS*) bestimmen Unternehmen unter anderem Maßnahmen, Regeln und Verfahren zur Sicherung und Kontrolle des Informationsflusses und zur Identifizierung der Verantwortlichen für die Ausführung sowie deren Überwachung.
Unternehmen können ihr ISMS selbst entwickeln oder im Rahmen eines Zertifizierungsverfahrens dessen Regeln oder auf Grundlage von Richtlinien, z.B. vom BSI.

Sicherheitsmanagement nach ISO 27001

Unternehmen können ihr System nach der Norm ISO 27001 einrichten - und zertifizieren lassen.
Zertifikate sind bis zu drei Jahre gültig, nach Ablauf dieser Zeit ist eine Verlängerung möglich. Es kann sogar vorkommen, dass die Zertifizierung nur für ein, zwei Jahre verlängert wird, vorausgesetzt, dass in bestimmten Fällen jährliche Audits durchgeführt werden. Diese Norm umfasst 11 Kapitel und einen Anhang A. Insgesamt enthält es 32 Pflichtblätter, 250 Optionsblätter und 114 Kontrollen, die eine internationale Anerkennung haben. Ihr Schwerpunkt liegt auf Organisationsumfeld, Planung, Implementierung, Unterstützung, Betrieb, Leistungsbewertung und Verbesserungsmaßnahmen.

Echtzeit-Erkennung

Neben einem ISMS kann ein Unternehmen auch ein *Security Information and Event Management* (*SIEM*) einrichten.

Das SIEM hat u. a. die Aufgabe, Daten und Protokolle zu analysieren, Warnungen an die Zentrale zu geben, Sicherheitslücken oder Bedrohungen in Echtzeit zu erkennen, z. B. durch Zugriffsversuche auf ein Benutzerkonto durch Eingabe falscher Passwörter usw.
Allerdings ist der Einsatz eines solchen Systems für Unternehmen mit hohen Kosten verbunden. Diese Investitionen haben jedoch zu einer neuen Art des Umgangs mit Cybersicherheit geführt: dem Einsatz von Künstlicher Intelligenz. Sie ermöglicht eine noch schnellere, genauere und effektivere Erkennung von Bedrohungen in Echtzeit. Dieses System "lernt" das Verhalten der Benutzer, indem es Benutzerprofile, Systemzugriffspunkte usw. erstellt, um ungewöhnlich Verhaltensweisen zu erkennen, die mit traditionellen Mitteln nicht entdeckt werden würden. Diese Art von Technologie schützt auch die sogenannte "Cloud" und trifft sofort Entscheidungen, um die Integrität der IT-Systeme zu gewährleisten. Diese Systeme werden in vielen verschiedenen Branchen eingesetzt (Restaurants, Krankenhäuser, Flughäfen, Kreditinstitute, Versicherungsagenturen usw.). Innovative Beispiele sind das Airport Profiling, bei dem das System das Verhalten von Touristen analysiert. In Infrastruktursystemen steuert manchmal ein einziger Computer online zahlreiche Prozesse, z.B. in der Gasversorgung oder im Umgang mit gefährlichen Stoffen, die KI-Systeme vor möglichen Cyberangriffen isolieren können. Eine weitere Anwendung ist die Überwachung von Mailsystemen gegen Angriffe am Wochenende.

Unternehmensintern können KI-gestützte Systeme überwachen, ob Mitarbeiter interne Richtlinien verletzen, etwa zum Herunterladen von Dateien oder Programmen. KI-gestützte Abwehrsysteme "lernen" die Realität und den Zustand des Unternehmens und seine ständige Weiterentwicklung, und suchen dann nach Anomalien, bevor diese einen Schaden verursachen.

Kritische Infrastrukturen - KRITIS

Für Kritische Infrastrukturen (*KRITIS*) sieht Die KRITIS-VO besondere Anforderungen vor, zusammengefasst in Sektoren und Branchen. Diese sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie,

Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Indirekt betrifft
Zwar richtet sich die KRITIS-Verordnung unmittelbar an Infrastrukturunternehmen, indirekt sind aber auch fast alle Unternehmen mit Geschäftsbeziehungen zu KRITIS-Unternehmen betroffen, wenn sie mit diesen im Datenaustausch oder in online Verbindung stehen – die KRITIS Unternehmen beziehen solche Geschäftspartner regelmäßig über ihre AGB (meist Einkaufs AGB) in ihre Sicherheitskonzept und Verpflichtungen mit ein.

Verträge mit Providern und Plattformen

Weil die Verflechtung von IT-Leistungen beständig zunimmt, ist oft bereits ein großer Teil der Funktionalität im Unternehmen ausgelagert, externe Services sind schon von Anfang an Standard. Das Sicherheitsmanagement für Cloud, Saas, IaaS usw, Backup Hosting, Outsourcing, Services und Maintenance muss zwingend vertragliche Verpflichtungen der Provider umfassen, welche Standards zu gewährleisten sind, wie diese überwacht werden und wie der Provider bei Verletzungen gegenüber dem Unternehmen als Auftraggeber oder Nutzer haftet.

Cyberversicherungen

Letztlich können sich Unternehmen gegen finanzielle Schäden auch versicherungstechnisch absichern. Elektronikversicherungen (insbesondere mit Software-Klausel) sichern das System ab, Betriebsunterbrechungsversicherungen die Einbußen aufgrund des Systemausfalls und Cyberpolicen bestimmte Angriffsrisiken. Allen Policen ist aber gemeinsam, dass der Versicherungsschutz umfangreiche betriebliche Sicherungsmaßnahmen voraussetzt – wegen des massiven Anstiegs der Angriffe im letzten Jahr sind auch die Prämien extrem gestiegen.

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

KORRESPONDENTEN

u.a. Amsterdam, Athen, Brüssel, Budapest, Helsinki, Istanbul, Kopenhagen, Lissabon, London, Luxemburg, Mailand, Madrid, Moskau, Oslo, Paris, Stockholm, Warschau, Wien, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, New Delhi, Peking, Tokio.

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