MANAGEMENTKOMPASS

02
2017

Cyber Security

TREND
Cyber Security
ist geschäftskritisch

THINK TANK
Mit SIEM for Business
Angriffe gezielt aufhalten

PRAXIS
Zahlungsverkehr: Betrugs-
prävention nicht nur Kür

F.A.Z.-INSTITUT

sopra steria
CONSULTING

Urs M. Krämer
CEO
Sopra Steria Consulting

„WannaCry hat einmal mehr gezeigt, wie verwundbar eine digitalisierte Gesellschaft ist. Die Bedrohungslage erfährt durch das Internet of Things einen neuen Schub. Spätestens jetzt gehört das Thema IT-Sicherheit ganz oben auf jede Management-Agenda – sie ist Pflichtdisziplin der digitalen Transformation. Ein rein technischer Ansatz greift jedoch zu kurz. Ohne die kontinuierliche Sensibilisierung der Mitarbeiter bleibt der Wirkungsgrad intelligentester Security-Lösungen eingeschränkt."

VORWORT

Jens Weidmann
Präsident der
Deutschen Bundesbank

„Cyber-Attacken können potenziell das Vertrauen der Öffentlichkeit in das Finanzsystem aushöhlen. Um die positiven Effekte einer digitalen Finanzwelt nicht zu gefährden, wird es entscheidend darauf ankommen, solche Cyber-Attacken ins Visier zu nehmen."

Torsten Jüngling
General Manager DACH,
Nordics and East Europe,
BT Security

„Cyber-Angriffe können unabsehbare Folgen für ein Unternehmen haben – von Geschäftsausfällen aufgrund einer DDoS-Attacke über Imageschäden durch den Verlust von Kundendaten bis hin zur persönlichen Haftung des Managements. Die IT-Sicherheit ist deshalb ein strategisches Unternehmensziel und muss Chefsache sein."

Mit der Digitalisierung steigt die unternehmerische Verletzlichkeit. Datendiebstahl, Spionage, Sabotage und Erpressung bedrohen alle Branchen, öffentliche Einrichtungen und Kritische Infrastrukturen. Doch viele Organisationen treiben die Digitalisierung ihrer Geschäfts-und Produktionsprozesse voran, ohne dabei dem Thema Security ausreichende Aufmerksamkeit zu widmen. Während kreative Hacker und andere Kriminelle ein beliebig vielschichtiges Arsenal für ihre Angriffe auf die Daten- und Betriebssicherheit einsetzen, beschränken sich der Schutz und die Abwehr unbefugten Eindringens vielerorts weiterhin auf altbekannte Security-Maßnahmen, die heute nicht mehr ausreichen.

Das Internet der Dinge bringt nicht nur neue Möglichkeiten, sondern auch unsichere Schnittstellen und Anwendungen mit sich. Zudem begünstigen systemische Schwachstellen und arglose Mitarbeiter die Cyber-Kriminalität und andere Angriffe auf den Motor des modernen wirtschaftlichen und gesellschaftlichen Lebens: die Daten. Um diese bestmöglich und gesetzeskonform zu schützen, müssen Unternehmen ihre IT-basierten Abläufe und Aktionen durchgängig überwachen. Ziel sollte sein, in den Datenströmen selbst kleinste Abweichungen zu erkennen, diese zu analysieren und flexibel reagieren zu können. Wichtig sind nicht nur technische Lösungen, sondern auch das Wissen um und das Bewusstsein für die Risiken.

Welche technischen, organisatorischen und mitarbeiterbezogenen Herausforderungen die aktuellen Spielarten des Cybercrime für Unternehmen mit sich bringen, beleuchtet dieser Managementkompass ebenso wie rechtliche Implikationen und wirksame Maßnahmen zur Prävention, Erkennung und Reaktion.

Sopra Steria Consulting

F.A.Z.-Institut

MEHR SCHUTZ DURCH CYBER SECURITY

In Zeiten fortschreitender Digitalisierung und Vernetzung hat die Reaktionsfähigkeit hinsichtlich Datendiebstahl und -missbrauch eine ebenso hohe Priorität wie die Prävention. Viel steht auf dem Spiel, wenn Cyber-Kriminelle Unternehmen erpressen, geistiges Eigentum abgreifen oder produktions- und geschäftskritische Abläufe lahmlegen. Unternehmensentscheider müssen sich fragen, ob ihre vorhandenen Systeme und Schutzmaßnahmen für den stetigen Wettlauf zwischen Cybercrime und Cyber Security ausreichend gerüstet sind und wo Handlungsbedarf besteht. Eine technische Lösung allein reicht jedoch nicht aus, denn Cyber-Kriminelle setzen oft gezielt bei der Schwachstelle Mensch an. Daher sollte jedes Unternehmen seine Mitarbeiter über die Risiken aufklären und regelmäßig schulen.

1 | » MANAGEMENTEMPFEHLUNG

Nehmen Sie zunächst die vorhandene IT und Anwendungslandschaft gründlich unter die Lupe, und spüren Sie unsauber aufgesetzte Prozesse auf. Betriebs- und Datensicherheit sind die Grundvoraussetzungen für die erfolgreiche Digitalisierung jedweder Produktions- und Geschäftsprozesse. Bevor Sie Entscheidungen zur Vernetzung (etwa zur Einbindung von Maschinen, Geräten und Abläufen in das Internet of Things, IoT) treffen, vergegenwärtigen Sie sich, dass die Modernisierung durch Digitalisierung auch neue Angriffsflächen schaffen kann.

Die Nachrüstung und Integration bestehender (Legacy-)Systeme mit modernen, Cloud-basierten Lösungen kann oft Sicherheitslücken entstehen lassen oder bereits vorhandene vergrößern, die für Datendiebstahl und -missbrauch dann ebenso zum Einfallstor werden wie für Sabotage oder Erpressung. Eine mangelnde Anwendungssicherheit, veraltete Betriebssysteme und unzureichend programmierte Schnittstellen zum IoT begünstigen IT-Ausfälle und damit Betriebsunterbrechungen. Viele Mankos im technischen Innenleben von Unternehmen machen Angriffe aus dem sogenannten Cyberspace erst möglich.

Wo Produktionsanlagen und Lieferketten immer stärker vernetzt sind und direkt miteinander agieren, können die Folgen eines technischen Fehlers oder menschlichen Versagens dramatischer denn je sein. Nicht korrekt verarbeitete, falsch formatierte oder missinterpretierte Daten können beispielsweise in Versorgungsnetzen, smarten Fabriken und anderen Industrie-4.0-Umgebungen zu schwerwiegenden Fehlleistungen, Ausfällen oder Stillstand führen.

Die eigene digitale Transformation sollte daher nicht im Hauruckverfahren erfolgen, sondern schrittweise, sorgsam und mit Blick auf eine umfassende Sicherheit. Dabei ist gut beraten, wer sich nicht allein auf die eigene IT-Abteilung verlässt, sondern bereits vor der unabdingbaren Schwachstellenanalyse ausgewiesene Modernisierungs- und Security-Experten hinzuzuzieht.

2 | » MANAGEMENTEMPFEHLUNG

Machen Sie Cyber Security zur Chefsache und die Widerstandsfähigkeit (Resilience) zum Schwerpunkt der Sicherheitsstrategie. Angriffe von innen und außen wird es immer geben, also sind Reaktionsbereitschaft und -fähigkeit das oberste Gebot. Die Kontinuität Ihres Geschäftsbetriebes muss auch bei schwerwiegenden Sicherheitsvorfällen gewährleistet bleiben.

Führungskräfte sollten sich fragen, wie es um das Risikomanagement, Notfallpläne und die Verantwortlichkeiten bestellt ist und sich zumindest einen Überblick über die aktuellen Grundvoraussetzungen verschaffen. Um Fehlinvestitionen zu vermeiden und zielführend auf die (Neu-)Gestaltung der unternehmensweiten Sicherheitsrichtli-

nien einzuwirken, gilt es, die Aussagen interner Mitarbeiter zur Sicherheitslage realistisch einschätzen zu können. Selbstüberschätzung in Sachen IT- und Cyber Security ist eine der größten Gefahren für die Betriebs- und Datensicherheit und noch immer weitverbreitet.

Etliche Studien belegen, dass gerade Geschäftsführer ihr Unternehmen häufig deutlich besser gegen interne Sicherheitsverstöße und externe Angriffe gerüstet sehen, als es tatsächlich ist. In vielen Unternehmen klafft eine breite Lücke zwischen der realen Widerstandsfähigkeit und einer Bedrohungslage, die immer ernster wird – sowohl mit Blick auf die Schwere der Angriffe als auch mit Blick auf die Art der Angreifer.

Abhilfe schaffen gezielte Investitionen in intelligente Bedrohungserkennung, prädiktive Datenanalysen und Incident-Response-Lösungen. 100-prozentige Sicherheit bieten zwar auch diese Ansätze nicht, aber sie tragen ganz wesentlich zu einer signifikanten Verringerung des Schadensrisikos und der Folgen gravierender Sicherheitsvorfälle bei.

3 | » MANAGEMENTEMPFEHLUNG

Stellen Sie sich auf strengere Datenschutzregeln ein. Zum 25. Mai 2018 wird die bereits heute geltende EU-Datenschutz-Grundverordnung (DSGVO) verbindlich. Nutzen Sie die Übergangsfrist bis zum Mai 2018, um Compliance mit den neuen EU-Richtlinien herzustellen, und bedenken Sie, dass eine Verletzung der Sorgfaltspflicht bei Datenschutz und Systemsicherheit nach deutschem Recht (Stichwort: Kontroll- und Transparenzgesetz, KonTraG) bereits heute als Straftatbestand geahndet werden kann.

Die EU-DSGVO schreibt das Grundrecht auf Datenschutz fest. Damit wächst nicht nur die Verantwortung, sondern auch das Haftungsrisiko – sowohl für das Unternehmen als auch für Geschäftsführer, IT-Verantwortliche und interne Datenschutzbeauftragte. Zudem drohen erhebliche Bußgeldforderungen. Die Höchstgrenze soll bei 20 Millionen Euro beziehungsweise 4 Prozent des Jahresumsatzes der betroffenen Unternehmen liegen.

Verschärfungen sieht die EU-DSGVO bei personenbezogenen Daten vor. Deren Definition ist deutlich strenger gefasst als bisher. Deshalb müssen Unternehmen letztlich nahezu alle Prozesse, Produkte, Dokumentationen und Verträge gründlich unter die Lupe nehmen und gegebenenfalls anpassen, um den gesetzlichen Anforderungen nach den Prinzipien „Privacy by Design“ und „Privacy by Default“ zu genügen. Besondere Aufmerksamkeit sollte hierbei auch den vertraglichen Vereinbarungen (Service Level Agreements/SLAs) zur Auftragsdatenverarbeitung gelten, die zwischen einem Unternehmen und dessen ITK- und Cloud-Dienstleistern bestehen.

4 | » MANAGEMENTEMPFEHLUNG

Sensibilisieren Sie sich und Ihre Mitarbeiter für wachsende Bedrohungen und Cyber Security. Als Führungskraft sollten Sie die Sicherheitsmankos der „Schwachstelle Mensch“ sowohl offensiv als auch methodisch angehen.

Laut der „Potenzialanalyse Digital Security 2017“ von Sopra Steria Consulting führen inzwischen fast alle Unternehmen mit mehr als 500 Mitarbeitern Maßnahmen zur Security Awareness für ihre Mitarbeiter durch. Aber nur knapp die Hälfte bietet dies regelmäßig allen Mitarbeitern an.

Schulungen zum Datenschutz und zur IT-Sicherheit sind wichtig: Denn neben Problemen in der vorhandenen IT-Basis und Anwendungslandschaft oder unsauber aufgesetzten Prozessen stellen nicht zuletzt die Arbeitsweisen und Gewohnheiten der Mitarbeiter ein Sicherheitsrisiko dar. Hier befinden sich in der Regel etliche Schwachstellen, die Cyber-Kriminelle aufspüren und nutzen, um ihr digitales Werkzeug in die (grundsätzlich recht gut abgesicherten) Netzwerke einzuschleusen.

Erpressungen mit Ransomware etwa, mit der Cyber-Kriminelle Daten und Anwendungen verschlüsseln und diese erst nach Zahlung eines Lösegeldes wieder freischalten, „funktionieren“ unter anderem deshalb so gut, weil viele Unternehmen kein systematisches Back-up betreiben. Für die Erpresser ist das ein lohnendes Geschäft. Eine Entschlüsselung der Blockade-Codes ist kaum möglich, der Geschäftsbetrieb muss weitergehen, und wer einmal für die „Freilassung“ seiner Daten zahlt, wird es wieder tun. Statistisch betrachtet, soll jedes vierte Unternehmen, das zum Erpressungsopfer wird, mindestens dreimal Lösegeld gezahlt haben. Ihren Weg in die Unternehmenssysteme nehmen solche und andere schädliche Codes häufig über Mitarbeiter, die E-Mail-Anhänge oder präparierte Links arglos öffnen. Die Herausforderung besteht darin, Sicherheitsbewusstsein und standardisierte Abläufe überall im Unternehmen zu verankern.

BUCH & WEB

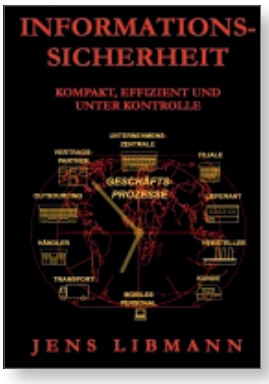
FACHLITERATUR

Ferri Abolhassan:
Security Einfach Machen: IT-Sicherheit als Sprungbrett für die Digitalisierung. Springer Gabler 2017

Autoren aus Politik, Wirtschaft und Forschung beleuchten in diesem Sammelband die Digitalisierung, insbesondere mit Blick auf die Sicherheit und die Konsequenzen für verschiedene Bereiche: Sicherheitspolitik, Management, IT-Recht und Datenschutz, neue Sicherheitsdienstleistungen und -konzepte, neue Berufsbilder, Nutzerverhalten. Der große Appell: Security muss in Zukunft selbstverständlicher Bestandteil von Anwendungen sein – und eben ganz einfach zu bedienen sein.

Jens Libmann:
Informationssicherheit – kompakt, effizient und unter Kontrolle. Praxisorientierte Prinzipien für ein profitables und effizientes Security-Management und -Controlling für Unternehmen. epubli 2016

Der Experte für Security Management Jens Libmann hat selbst feststellen müssen, dass Sicherheitskonzepte, wie sie in der Literatur oder in Weiterbildungen behandelt werden, aus den verschiedensten Gründen oftmals in der Praxis nur schwer umzusetzen sind. Als Quintessenz aus der Standardliteratur und der eigenen Erfahrung entwickelt er in seinem Buch praxisorientierte Prinzipien für ein profitables und effizientes Security Management und Security Controlling für Unternehmen.



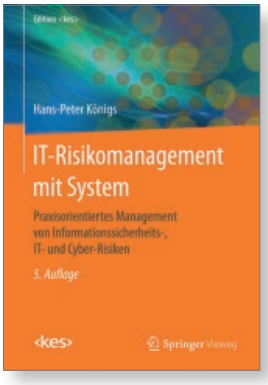
LINKS

» **www.bsi.bund.de**
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht Meldungen, Studien, Veranstaltungshinweise sowie Tipps und Empfehlungen zur Sicherheit im Internet für Bürger und Unternehmen.

» **www.cert-bund.de**
Auf der der Website des CERT-Teams des BSI finden sich Meldungen zu aktuellen Bedrohungen. Registrierte Benutzer können personalisierte Warn- und Informationsdienste nutzen.

» **www.heise.de/security**
Portal des Heise-Verlags mit Nachrichten, Hintergrundinformationen, Foren und Veranstaltungen zum Thema IT-Sicherheit.

» **www.searchsecurity.de**
Portal für IT-Security-Profis mit aktuellen Industrienachrichten, Meldungen über Hackerangriffe, Studien, Ratgebern, Softwaretipps sowie Informationen über Trainingsmöglichkeiten.

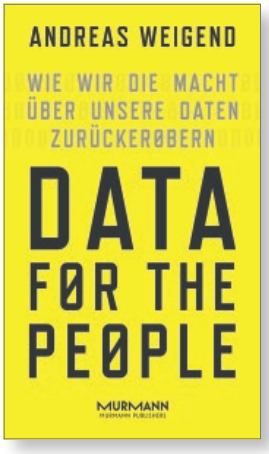


Hans-Peter Königs:
IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken. Springer Vieweg (5. Aufl., 2017)

Das Buch versteht sich als Leitfaden für das Informationssicherheits-, IT- und Cyber-Risikomanagement in Unternehmen. Ausgehend von allgemeinen Betrachtungen zum Risikomanagement und der Governance, geht der Autor auf IT-Risiken ein und vermittelt dem Leser Methoden, wie er diese beurteilen, damit umgehen und kontrollieren kann. Die 5. Auflage ist an den Stand der Compliance-Anforderungen und der Standardisierung angepasst und enthält ein Kapitel speziell über Cyber-Risiken und deren Besonderheiten.

Andreas Weigend:
Data for the People. Wie wir die Macht über unsere Daten zurückerobern. Murmann Publishers 2017

Der ehemalige Chefwissenschaftler von Amazon Andreas Weigend gibt sich zwar überzeugt, dass der Mehrwert aus der Preisgabe von Daten die Risiken überwiegt. Dennoch formuliert er sechs Grundrechte für Daten, die Bürger und Kunden einfordern sollten, um die Macht über ihre Daten zurückzuerlangen. Er zeigt, wie Google, Facebook und Co. arbeiten und wie viel unsere Daten wert sind, und klärt über den Umgang mit personenbezogenen Daten im Internet auf.



Nitesh Dhanjani:
IoT-Hacking: Sicherheitslücken im Internet der Dinge erkennen und schließen. dpunkt.verlag 2016

Der IT-Sicherheitsexperte Nitesh Dhanjani beschreibt, wie Geräte im Internet of Things von Angreifern missbraucht werden können. Mit seinem Buch präsentiert er einen Leitfaden für die Erkennung und Behebung von Sicherheitslücken. Er erklärt, wie sich Schwachstellen in IoT-Systemen identifizieren lassen, und gibt einen Einblick in die Taktiken der Angreifer.

GLOSSAR

Advanced Persistent Threat (APT)
Gezielter Netzwerkangriff über einen längeren Zeitraum. Der Angreifer will möglichst lange unentdeckt bleiben, um über einen längeren Zeitraum sensible Daten zu stehlen.

Botnet/Botnetz
Menge aktiver Schadsoftwareprogramme (Bots), die über das Internet überwacht und ferngesteuert werden können. Bots infizieren zunächst ungeschützte Rechner, gliedern diese ins Botnet ein und nutzen deren Ressourcen, etwa für Spam-Versand, ohne Wissen des Eigentümers.

CERT
Ein Computer Emergency Response Team wirkt an der Lösung von konkreten IT-Sicherheitsvorfällen mit, befasst sich mit IT-Sicherheit, gibt Warnungen vor Sicherheitslücken heraus und bietet Lösungen an.

Disaster Recovery (DR)
Wiederherstellung der Datenbestände nach einem Katastrophenfall oder einem Absturz zur kurzfristigen Wiederaufnahme der Geschäftstätigkeit. Eine wichtige Kennzahl ist das Recovery Time Objective (RTO), die Zeit bis zum Wiederanlaufen.

Distributed Denial of Service (DDoS)
„Denial of Service" (DoS) steht für die Nichtverfügbarkeit eines Internetdienstes, ausgelöst durch eine Überlastung des Datennetzes, entweder unbeabsichtigt oder durch einen konzentrierten Angriff. Im Fall eines „Distributed Denial of Service" fällt ein Dienst infolge einer Unmenge von Anfragen aus einer Vielzahl von Quellen aus.

Exploit
Mittel, um sich über Sicherheitslücken und Fehlfunktionen Zugang zu bestimmten Systemen (Betriebssystemen, Anwendungssoftware, Smartphones) zu verschaffen.

Incident Response Plan (IRP)
Ein Vorfallreaktionsplan enthält Anweisungen, um Sicherheitsvorfälle zu entdecken, und definiert Reaktionen, um die Auswirkungen eines Vorfalls zu begrenzen.

Information Security Management System (ISMS)
Verfahren und Regeln, um die Informationssicherheit in einem Unternehmen zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Keylogger
Hard- oder Software, mit der sich die Eingaben auf der Tastatur eines Computers protokollieren und damit überwachen oder rekonstruieren lassen, um etwa Passwörter oder PINs aufzuzeichnen.

Malware
Oberbegriff für Computerprogramme, die entwickelt wurden, um unerwünschte/schädliche Funktionen auszuführen.

Managed Security Service (MSS)
Auslagerung der IT-Sicherheit an einen externen Dienstleister, der den Betrieb und die Überwachung von Security-Lösungen übernimmt.

Privacy by Default
Datenschutz als Standardeinstellung. Prinzip, wonach Produkte oder Dienstleistungen standardmäßig datenschutzfreundlich eingestellt sind. In der EU-DSGVO verankert.

Privacy by Design
Datenschutz durch Technik. Prinzip, wonach Technik so angelegt ist, dass die Privatsphäre von Nutzern geschützt wird und Anwender die Kontrolle über die eigenen Informationen haben. In der EU-DSGVO verankert.

Ransomware
Schadsoftware, die den Zugriff auf das Betriebssystem blockiert beziehungsweise potenziell wichtige Dateien verschlüsselt, verbunden mit einer Lösegeldforderung, meist über das digitale Bezahlsystem Bitcoin.

Security Awareness
Bewusstsein und Wissen (der Mitarbeiter) über Risiken für die IT-Sicherheit und für einen verantwortungsvollen Umgang mit Daten und Technik.

Security by Design
Integrierte Softwaresicherheit. Prinzip, wonach Sicherheit als explizite Anforderung in den Entwicklungsprozess aufzunehmen sowie ganzheitliche Sicherheitsmaßnahmen von der Initialisierung an zu berücksichtigen, umzusetzen und zu testen sind.

Security Information and Event Management (SIEM)
Automatisierte Detektion von Angriffen, basierend auf Protokolldaten von Anwendungen, Infrastruktur und Netzwerkkomponenten. Dadurch ermöglicht ein SIEM-System eine schnellere Identifikation, Analyse und Wiederherstellung bei sicherheitsrelevanten Zwischenfällen.

Supervisory Control and Data Acquisition (SCADA)
Überwachen und Steuern technischer Prozesse mittels eines Computersystems.

Threat Intelligence
Intelligente Bedrohungserkennung. Frühwarn- und Erkennungssysteme mit Informationen über Bedrohungen wie Schadprogramme oder Tätergruppen.

AKTUELLE STUDIEN

Managementkompass
Künstliche Intelligenz

Lernende, sich selbst optimierende Systeme sind die Grundlage für die nächsten Entwicklungsstufen der Automatisierung. Welche Potenziale Künstliche Intelligenz kurz- und mittelfristig erschließen kann und welche Vorteile Unternehmen jetzt schon realisieren, zeigt dieser Managementkompass ebenso wie nötige Maßnahmen und Implikationen für die Arbeitswelt.

Branchenkompass
Banking

Der Branchenkompass Banking steht auf neuen Füßen. Praktiker aus der Finanzbranche haben sich getroffen, um die wichtigsten Herausforderungen und mögliche Lösungen zu diskutieren. Die herausgearbeiteten Themen wurden durch eine Online-Befragung von Führungskräften der Branche quantifiziert. Klares Fazit: Der Anpassungsdruck durch Regulierungsmaßnahmen auf nationaler, europäischer und internationaler Ebene bleibt hoch und auch Datensicherheit und Datenschutz stehen auf der Agenda weit oben.

Studie
Datengetriebene Agilität

Sopra Steria Consulting sowie Wissenschaftler der Universität Hamburg und der Leuphana Universität Lüneburg haben das Phänomen der datengetriebenen Agilität in Unternehmen untersucht und zeigen, dass sich diese Arbeitsweise digital exzellenter Unternehmen auch für Organisationen mit gewachsenen Strukturen und IT-Systemen eignet.

IMPRESSUM

Sopra Steria GmbH
Hans-Henny-Jahnn-Weg 29, 22085 Hamburg

F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH
Frankenallee 68–72, 60327 Frankfurt am Main

Verlag: FRANKFURT BUSINESS MEDIA GmbH – Der F.A.Z.-Fachverlag
Bismarckstraße 24, 61169 Friedberg
Geschäftsführung: Dr. André Hülsbömer, Hannes Ludwig

Titelfoto: © solarseven/iStock/Thinkstock/Getty Images

ISBN: 978-3-945999-48-6

Redaktion: Jacqueline Preußer (verantwortlich), Andrea van Baal, Juliane Streicher
Gestaltung und Satz: Christine Lambert
Lektorat: Vera Pfeiffer

Druck und Verarbeitung: Boschen Offsetdruck GmbH
Alpenroder Straße 14, 65936 Frankfurt am Main
www.boschendruck.de

Mit Ökofarben auf umweltfreundlichem Papier gedruckt.
Diese Studie wurde klimaneutral hergestellt. Der CO_2-Ausstoß wurde durch Klimaschutzprojekte kompensiert.

klimaneutral
natureOffice.com | DE-644-419329
gedruckt

Ansprechpartner

Sopra Steria GmbH
Corporate Communications
Birgit Eckmüller
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
Telefon: (040) 22703-5219
E-Mail: birgit.eckmueller@soprasteria.com

F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH
Jacqueline Preußer
Postfach 20 01 63
60605 Frankfurt am Main
Telefon: (069) 7591-1961
E-Mail: j.preusser@faz-institut.de

ISBN: 978-3-945999-48-6