MANAGEMENTKOMPASS 03 2018

Unternehmen schützen – Risiken minimieren

F.A.Z.-INSTITUT

sopra steria CONSULTING

Urs M. Krämer
CEO
Sopra Steria Consulting

„Unternehmenslenker können der Informationssicherheit nicht genug Bedeutung beimessen. Sie ist obligatorisch für den Geschäftserfolg in der digitalen Ära, denn die fortschreitende Digitalisierung zieht immer perfidere Cyber-Attacken nach sich. Unternehmen wie Behörden benötigen heute neue Verteidigungsstrategien, um ihre Systeme und ihre Reputation nicht aufs Spiel zu setzen."

Andreas Berger
Vorstandsmitglied und CEO für Zentral- und Osteuropa bei der Allianz Global Corporate & Specialty SE

„Das neue Gold der digitalen Ökonomie sind immaterielle Werte wie Daten, Plattformen, Netzwerke oder der Ruf des Unternehmens. Damit wird deren Schutz in Deutschland immer wichtiger. Betriebs- und Lieferkettenunterbrechungen sowie Cyber-Bedrohungen gehören heute zu den größten Risiken."

EXECUTIVE SUMMARY

TREND

THINK TANK

PRAXIS

THINK TANK

PRAXIS

© Bitkom

Achim Berg
Präsident des Bitkom e.V.

„Infrastrukturen, Behörden und Unternehmen stehen zunehmend unter Beschuss international tätiger Cyber-Krimineller. Eine verbesserte Zusammenarbeit im Bereich Cyber-Sicherheit ist dringend nötig. Allein der deutschen Wirtschaft entsteht durch Cyber-Angriffe ein Schaden von 55 Milliarden Euro pro Jahr."

VORWORT

Je mehr der Geschäftserfolg von Vernetzung und digital gesteuerten Prozessketten abhängt, desto umfassender müssen sich Unternehmen schützen – vor dem Diebstahl und dem Missbrauch von Daten ebenso wie vor Sabotage und kostspieligen Betriebsunterbrechungen. Die zunehmende Digitalisierung erfordert von Führungskräften wie von Mitarbeitern ein deutlich höheres Maß an Sicherheitsbewusstsein als bisher.

Heute gehören Cyber-Attacken zu den größten Risiken für geregelte, gesetzeskonforme Geschäftsabläufe, für Infrastrukturen und für den Datenschutz und somit auch für die Reputation und die Erlöse von Unternehmen. Allen Prognosen zufolge dürften die Angriffe in den kommenden Jahren weiter zunehmen, in ihrer Zahl ebenso wie in ihrer Komplexität. Entscheider sind daher doppelt gefordert: Sie müssen dafür Sorge tragen, dass Mitarbeiter von arglosen Gefährdern zu Sicherheitsverteidigern werden. Gleichzeitig gilt es, organisatorische Strukturen (Stichwort: Schatten-IT), Arbeitsweisen und Zugriffsrechte zu hinterfragen. Vor allem aber müssen Unternehmen ihre traditionell reaktiven Abwehrmaßnahmen durch intelligente, agile Lösungen ergänzen.

Wie Unternehmen ihre Sicherheitskultur verändern, auf welche Bedrohungen sie sich einstellen und wie Automatisierung und Künstliche Intelligenz zu ganzheitlicher Prävention und Widerstandsfähigkeit beitragen, zeigt dieser Managementkompass.

Sopra Steria Consulting
F.A.Z.-Institut

Sicherer wirtschaften

Durch die digitale Vernetzung steigt für Unternehmen das Risiko, Opfer von Sabotage, Erpressung und Spionage zu werden. Gegen manche Infiltrationstechniken können vorhandene Sicherheitssysteme kaum etwas ausrichten. Um Schäden für Unternehmen, aber auch für vernetzte Partner, Lieferanten und Kunden zu vermeiden, sollte die Security-Strategie laufend optimiert werden. In einer ganzheitlichen Betrachtung von Betriebs-, Prozess- und Datensicherheit sind mehrschichtige Schutzmechanismen mit intelligenten Erkennungs-, Abwehr- und Reaktionssystemen empfehlenswert.

1. Selbst Unternehmen, die den Schutz ihrer IT und ihrer Daten seit Jahren mit hohem Aufwand betreiben, sind nicht gänzlich unangreifbar. Deshalb ist es besser, sich von der Vorstellung zu verabschieden, umfassende Sicherheit sei ein Dauerzustand. Es ist realistischer zu akzeptieren, dass jedes Unternehmen zum Opfer von IT-Angriffen werden könnte – auch Ihres.

Doch viele Manager sind anderer Meinung, wie eine aktuelle Untersuchung des Digitalverbands Bitkom bei 752 Firmen mit mehr als 50 Mitarbeitern zeigt. So ist die Hälfte der Befragten davon überzeugt, dass sich IT-Angriffe komplett verhindern ließen. Genau das aber ist aus Sicht neutraler Sicherheitsexperten wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) schlicht ausgeschlossen. Möglich ist es jedoch, die Widerstandsfähigkeit der IT zu erhöhen und Erkennungs- und Reaktionsmuster kontinuierlich zu verfeinern. Hierzu ist eine umfassende, anpassungsfähige Sicherheitsarchitektur erforderlich, die alle bekannten neuralgischen Punkte abdeckt und von vernetzten Kleinstgeräten bis zum Cloud Computing reicht.

Wirksamer Schutz und Risikominimierung entstehen in einem Kreislauf aus Erkennen, Lernen und optimierter Vorsorge – und im Zusammenspiel fortschrittlicher Security-Lösungen. Diese müssen Angriffe auf Unternehmensdaten schnellstmöglich entdecken und eindämmen können.

2. Sicherheit ist ein Managementthema: Um Mitarbeiter und Dienstleister in diesem Bereich führen zu können, benötigen Sie keine tiefgreifenden technischen Kenntnisse. Die gesetzlichen Bestimmungen zur Haftung für Sicherheitsvorfälle, etwa im Rahmen der Datenschutzgrundverordnung (DSGVO), sprechen für eine prominente Platzierung des Themas.

Verschaffen Sie sich eine Übersicht über die Sicherheitslage im Unternehmen: Welche Daten sind besonders sensibel, welche erfolgskritisch? Wo entstehen neue Daten, wozu dienen diese, wo werden sie gespeichert und wie verwendet? Wer darf, wer kann auf welche Daten zugreifen? Wer bewegt sich in den Unternehmensnetzwerken, und wer kann systemische Änderungen vornehmen? Fragen wie diese sind alles andere als trivial. Häufig fällt es auch den dafür verantwortlichen Mitarbeitern nicht leicht, sie umfassend zu beantworten.

Angesichts zunehmender Bedrohungen und Angriffe sollte auch die Führungsebene möglichst genau wissen, was mit den Daten im Unternehmen geschieht. Letztlich kann fast jeder vernetzte Punkt zum Angriffsziel gegen die Betriebssicherheit und Handlungsfähigkeit werden. Eine kontinuierliche, bereichsübergreifende Analyse möglicher Schwachstellen und Sicherheitslücken ist unabdingbar.

3. Je mehr Ihr geschäftlicher Erfolg von digitalen Technologien abhängt, desto höher der Schaden bei Datendiebstahl und IT-Sabotage sowie durch Betriebsunterbrechungen. Leider ist mit bewährten Security-Produkten allein kaum etwas gegen die Taktiken und Techniken der aktuell fünften und sich ankündigenden sechsten Generation von Cyber-Bedrohungen auszurichten. Ermitteln Sie, auf welchem Stand Ihre Schutz- und Abwehrmaßnahmen sind.

Wie hoch die Schäden von Cyber-Erpressung, Datendiebstahl und Wirtschaftsspionage sind, hat Bitkom Research im Auftrag des Digitalverbands Bitkom

jüngst in einer Befragung von 500 Industrieunternehmen ermittelt: In den vergangenen beiden Jahren sollen Sicherheitsvorfälle das deutsche verarbeitende Gewerbe 43 Milliarden Euro gekostet haben.

Zwar sind Firewalls, Virenschutz, Sicherheits-Gateways, Intrusion Detection usw. nach wie vor wesentliche Komponenten einer Schutz- und Abwehrstrategie. Doch sie reichen nicht aus. Je mehr Prozesse, Datenquellen und Endgeräte in einem Unternehmen vernetzt sind, desto wichtiger sind ein umfassendes, intelligentes Monitoring, kontinuierliche Abweichungsanalysen und mehrschichtige Abwehrlösungen.

4. Das wachsende Internet der Dinge (IoT) umfasst Liefer- und Produktionsketten der Industrie 4.0, aber auch Gegenstände wie Klimaanlagen, Kameras und Kaffeemaschinen. Dazu können Steuerimpluse und Transaktionen kommen, die per Smartphone erfolgen. Machen Sie sich und Ihren Mitarbeitern die mannigfaltigen Verknüpfungen und Abhängigkeiten bewusst, und achten Sie auf die Gefahr durch ältere Geräte.

Laut Untersuchungen von Vanson Bourne und Trend Micro ist die durch das IoT begründete Angriffs- und Penetrationsgefahr vielen IT-Entscheidern (47 Prozent) gar nicht klar. Eine Sensibilisierung für Security auf Seiten der Mitarbeiter in Fachabteilungen und auf der Geschäftsleitungsebene ist notwendig.

Auch aus Gründen der Haftung und des Versicherungsschutzes sollte Führungskräften wie Mitarbeitern klar sein, dass Compliance mit gesetzlichen Vorgaben nur dann gegeben ist, wenn umfassende Maßnahmen für die IT-Sicherheit ergriffen werden – technisch und organisatorisch. Geschäftsgeheimnisse und -prozesse müssen geschützt werden, und der Schutz muss lückenlos dokumentiert sein.

5. Cyber-Bedrohungen nehmen nicht nur quantitativ, sondern auch an Raffinesse zu. Während brachiale Angriffsformen wie ein Distributed Denial of Service (DDOS) sofort spürbar sind, liegt die Gefährlichkeit von zum Beispiel Advanced Persistent Threats (APTs) in ihrer Unauffälligkeit. Sie sind ganz auf die im Vorfeld sorgfältig recherchierte Sicherheitsarchitektur des betroffenen Unternehmens zugeschnitten.

APT-Angreifer sind in der Regel nicht darauf aus, ein Unternehmen sofort zu schwächen. Vielmehr geht es darum, möglichst lange unentdeckt zu spionieren, Daten abzugreifen oder diese diskret zu manipulieren. Dazu schreiben Hacker ihren Code immer wieder um und setzen verschiedene Umgehungs- und Ausweichtechniken ein. So segeln sie unter dem Radar herkömmlicher Detektionssysteme.

Abhilfe gegen solche Lücken kann laut BSI nur selbstlernende Security-KI (Künstliche Intelligenz) schaffen. Deren verhaltensbasierter Ansatz soll ermöglichen, kleinste Abweichungen im Datenverkehr eines Netzwerks zu erkennen. In vorhandene Sicherheitsprozesse integriert, könnte KI dabei helfen, schnellere Sicherheitsentscheidungen zu treffen und agil auf Bedrohungen zu reagieren. Im Augenblick rät das BSI allerdings dazu, die rein technisch-automatisierte Risikoeinschätzung noch durch die Überprüfung von Spezialisten zu ergänzen.

Auch um regulatorischen Anforderungen gerecht zu werden, rückt in kritischen Prozessen der Ansatz „Man in the Loop" für selbstlernende Systeme in den Fokus. Bei diesem Ansatz trifft das selbstlernende Modell Entscheidungen nicht selbst, sondern macht dem Anwender Vorschläge für gute Entscheidungen. Derzeit werden neue Tools entwickelt, die das Verhalten Künstlicher Intelligenz besser nachvollziehbar machen.

Wer wissen will, wie es um die grundsätzliche Angreifbarkeit seines Unternehmens bestellt ist, kann sich durch reguläre Audits und Zertifizierungen, durch die Risikoermittlung im Vorfeld von Cyber-Versicherungen oder durch den Einsatz eines professionellen „White Hacker" ein klareres Bild davon verschaffen. Voraussetzung für ein Höchstmaß an Schutz ist jedoch, Cyber Security nicht als Kostentreiber, sondern als existenzielle Notwendigkeit zu betrachten. «

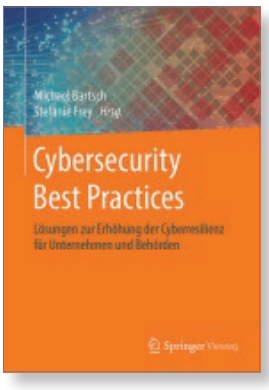
kurz & knapp

Jedes **3.** Unternehmen war in den vergangenen zwölf Monaten Ziel eines **CYBER-ANGRIFFS.**

Quelle: Potenzialanalyse Unternehmen schützen – Risiken minimieren (Sopra Steria Consulting), 2018

Buch & Web

FACHLITERATUR



Michael Bartsch und Stefanie Frey (Hrsg.):
Cybersecurity Best Pratices. Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Springer Vieweg 2018

Wie kann IT-Sicherheit gewährleistet werden? Und wie sollte man im Fall eines Cyber-Angriffs reagieren? Ein einheitliches Regelwerk dafür gibt es nicht. Deshalb haben Bartsch und Frey in ihrem Herausgeberwerk Best Practices und Strategieansätze renommierter, internationaler IT-Sicherheitsexperten zusammengetragen. Die Autoren aus unterschiedlichen Institutionen, Behörden und Unternehmen erläutern grundlegende Überlegungen und Ziele ihrer jeweiligen IT-Sicherheitsstrategie. Das kann Lesern dabei helfen , eigene Lösungsansätze zu entwickeln und umzusetzen.

Matthias Knoll und Susanne Strahringer (Hrsg.):
IT-GRC-Management – Governance, Risk und Compliance. Grundlagen und Anwendungen. Springer Vieweg 2017

Stetig komplexere IT-Systeme durchdringen alle Lebens- und Geschäftsbereiche. Deshalb müssen Governance, Risiken und Compliance im IT-Umfeld eines Unternehmens heute mehr denn je ganzheitlich gemanagt werden. Neben einer theoretischen Einführung in das Thema zeigt das Buch auch die Wechselwirkungen zwischen diesen drei Faktoren auf. Anhand praxisorientierter Fragestellungen wird die Notwendigkeit eines systematischen IT-GRC-Managements erläutert. Die Botschaft der beiden Herausgeber: Als Dreiklang innerhalb des IT-Managements ermöglichen Governance, Risk und Compliance Management eine nachhaltige Wertschöpfung.

LINKS

» **https://www.security-insider.de**
Online-Magazin mit aktuellen Nachrichten zu IT-Sicherheitsthemen, Fachartikeln, Ratgebern und Webcasts.

» **https://www.allianz-fuer-cybersicherheit.de**
Website der vom Bundesamt für Sicherheit in der Informationstechnik ins Leben gerufenen Allianz für Cyber-Sicherheit in Deutschland mit einem umfangreichen Informationsangebot und der Möglichkeit zur Meldung von Cyber-Angriffen sowie zum Austausch zwischen Unternehmen und Institutionen.

» **https://www.golem.de/specials/security**
Online-Nachrichtenportal, das mit Hintergrundberichten, Tests, Interviews und Analysen des Marktgeschehens Informationen zum Thema IT-Sicherheit liefert.

Constanze Kurz und Frank Rieger:
Cyberwar – Die Gefahr aus dem Netz. Wer uns bedroht und wie wir uns wehren können.
C. Bertelsmann 2018

Die IT-Sicherheitsexperten Kurz und Rieger warnen vor den Gefahren eines Cyber-Kriegs. Anlass dazu geben ihnen die immer zahlreicheren großangelegten Hacker-Angriffe der vergangenen Jahre. Diese werden durch die zunehmende Vernetzung in allen Lebensbereichen begünstigt. Die Autoren weisen auf das grundlegende Dilemma einer digitalisierten Gesellschaft hin: Bei den rapiden technologischen Veränderungen und dem wachsenden Druck auf Herstellerseite, stets der Erste sein zu wollen, werde die Systemsicherheit zunehmend vernachlässigt. Kurz und Rieger wollen dafür sensibilisieren, dass adäquater Schutz nur möglich ist, solange wir die Konsequenzen und Risiken unseres digitalen Handelns noch verstehen.

Kevin D. Mitnick mit Robert Vamosi:
Die Kunst der Anonymität im Internet. So schützen Sie Ihre Identität und Ihre Daten.
mitp 2017

Der eigenen Angaben zufolge „berühmteste (ehemalige) Hacker der Welt", Kevin Mitnick, zeigt zusammen mit Co-Autor Robert Vamosi, wie User mehr Privatsphäre im Internet erlangen. Die grundlegende Botschaft ihres Buchs: Jeder Mensch wird in jeder Situation beobachtet. Um diese These zu untermauern, verweisen die Autoren auf ihre eigenen Erfahrungen, und sie beschreiben reale Sicherheitsvorfälle und deren Konsequenzen für die Privatsphäre des Einzelnen. Mit praktischen Tipps zur Verschlüsselung von E-Mails, zum anonymen Surfen im Internet und mit einer Anleitung zum Passwortmanagement klären die Autoren ihre Leser über Sicherheitslücken auf und zeigen, wie ein individuell regulierbarer Grad an Anonymität erreicht werden kann.

Glossar

» Client
Computerprogramm, das auf dem Endgerät eines Netzwerks ausgeführt wird und mit einem Zentralrechner (Server) kommuniziert. Auch Endgeräte, die Dienste von einem Server abrufen, werden Clients genannt.

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

» Content-Filter
Ein System, das Webseiten oder E-Mails nach einzelnen Wörtern, typischen Phrasen, Bildern oder Links filtert.

» Digitale Forensik
Teilgebiet der Forensik, auch IT-Forensik, Computer- oder Netzwerkforensik genannt, das sich auf dolose Handlungen, die mit IT-Systemen und Datenträgern durchgeführt werden, fokussiert.

» Firewall
Sicherungssystem, das ein Netzwerk oder Computer vor unerwünschten Netzwerkzugriffen schützt.

» Flow Record Fingerprinting
Passives Verfahren, das die Metadaten des digitalen Kommunikationsflusses, die sogenannten Flow Records, analysiert. Diese erlauben es, anhand der IP-Adresse, des verwendeten Protokolls und des übertragenen Byte-Volumens Rückschlüsse auf die eingesetzte Software zu ziehen.

» Hack Back
„Digitaler Gegenangriff": Seit dem Angriff auf die IT-Systeme des Deutschen Bundestags im Jahr 2015 beschäftigen sich deutsche Behörden mit der Frage, wie man offensiv auf Cyber-Angriffe reagieren kann.

» Hash
Hash-Funktionen reduzieren große Datenmengen auf kleine Werte (Hashs), um durch einen Wertevergleich – auch absichtlich herbeigeführte – Integritätsverletzungen von großen Datenmengen feststellen zu können.

» IKT
Informations- und Kommunikationstechnik. Auch: ITK.

» Industrie 4.0
Die intelligente Vernetzung von Maschinen und Abläufen in der Industrie.

» Internet der Dinge
Vernetzung und Interaktion von Maschinen, Geräten und Anwendungen über digitale Plattformen. Auch: Internet of Things (IoT). Das IoT ist Treiber für die Digitalisierung der Logistik und Basis für die Industrie 4.0.

» Intrusion-Detection-System
System zur Erkennung von Angriffen gegen Computer oder Rechnernetze.

» Inventarisierung
Bestandsaufnahme von Hardware, Software und Lizenzen in einer Organisation.

» Kryptotrojaner
Software, die getarnt auf den Rechner gelangt und dort die Festplatte verschlüsselt. Damit wird die Festplatte unbenutzbar und kann erst nach Zahlung eines Lösegeldes wieder verwendet werden. Auch: Ransomware.

» Live-Forensik
Der Fokus liegt auf der Sicherung und Analyse flüchtiger Daten, wie dem Arbeitsspeicher, gestarteten Prozessen und bestehenden Netzverbindungen.

» Log-Einstellungen
Einstellungen für das Protokoll von Ereignissen eines Computerprogramms, das in einer Log-Datei oder einer Log-Datenbank gespeichert wird.

» Malware-Schutz
Schutz vor schädlicher Software, die Computer infizieren und Schaden anrichten kann. Malware sind zum Beispiel Viren, Würmer, Trojaner oder Spyware.

» „Man in the Loop"
Verfahren, dass die Interaktion eines Menschen erfordert. Auch: „Human in the Loop".

» Network Mapper (nmap)
Werkzeug zum Scannen und Auswerten von Zentralrechnern in einem Computernetzwerk.

» Post-mortem-Analyse
Forensische Analyse nach dem Ende eines Cyber-Angriffs.

» Proxy
Kommunikationsschnittstelle in einem Netzwerk.

» Quantenkryptografie
Einsatz quantenmechanischer Effekte in kryptografischen Verfahren.

» Security Incident Management
dient der angemessenen Bewältigung von IT-Sicherheitsvorfällen.

» Social Engineering
Psychotechniken, die das Verhalten von Menschen beeinflussen sollen, zum Beispiel um in IT-Systeme einzudringen.

» Speicher-Dump
Kopie oder Auszug eines Speicherinhalts. Auch: Speicherabbild.

» Explainable Artificial Intelligence (XAI)
Technische Disziplin, die nachvollziehbar macht, auf welche Weise Künstliche Intelligenz zu ihren Ergebnissen kommt.

Aktuelle Studien

Managementkompass
flexibel wachsen

Der wirtschaftliche, technische und gesellschaftliche Wandel vollzieht sich mit rasanter Geschwindigkeit. Damit Wachstum unter diesem Eindruck stattfinden kann, müssen sich Unternehmen flexibel aufstellen, Strategien miteinander kombinieren und Synergien aus altem und neuem Geschäft erzeugen. Dieser Managementkompass zeigt, dass das Strategieportfolio eines Unternehmens erst seinen Zweck erfüllen kann, wenn die dafür nötigen innerbetrieblichen Voraussetzungen geschaffen beziehungsweise interne Wachstumshürden abgebaut werden.

Branchenkompass
Banking

Um im Zuge der Digitalisierung konkurrenzfähig zu bleiben, müssen die Kreditinstitute ihre internen Prozesse und Geschäftsmodelle überdenken und modifizieren. Und ganz entscheidend: Die digitale Transformation muss von den Banken als Ganzes akzeptiert und umgesetzt werden. Wo stehen deutsche Banken in diesem Prozess? Wie gehen sie mit dieser Herausforderung um? Die Ergebnisse der Befragung von 109 Führungskräften aus der Finanzwirtschaft und die vertiefenden Interviews mit Spitzenvertretern aus der Branche geben hier Aufschluss.

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. Die Studie zeigt, dass sich die Arbeitsweise digital exzellenter Unternehmen auch für Organisationen mit gewachsenen Strukturen und IT-Systemen eignet.

IMPRESSUM

Sopra Steria SE
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: Dominik Heyer, Hannes Ludwig

Titelfoto: beanimages/Shutterstock.com

ISBN: 978-3-945999-71-4

Redaktion: Andrea van Baal, Eric Czotscher, Jacqueline Preußer, Georg Poltorak
Gestaltung und Satz: Christine Lambert
Lektorat: Juliane Streicher

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 SE
Corporate Communications
Birgit Eckmüller
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
Telefon: (040) 2 27 03-52 19
E-Mail: birgit.eckmueller@soprasteria.com

F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH
Jacqueline Preußer
Frankenallee 68–72
60327 Frankfurt am Main
Telefon: (069) 75 91-19 61
E-Mail: j.preusser@faz-institut.de

ISBN: 978-3-945999-71-4