Ferri Abolhassan *Hrsg.*

Security Einfach Machen

IT-Sicherheit als Sprungbrett für die Digitalisierung

Springer Gabler

Security Einfach Machen

Ferri Abolhassan (Hrsg.)

Security Einfach Machen

IT-Sicherheit als Sprungbrett für die Digitalisierung

Springer Gabler

Ferri Abolhassan
T-Systems International GmbH
Saarbrücken, Deutschland

ISBN 978-3-658-14944-4 ISBN 978-3-658-14945-1 (eBook)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler

Redaktion: Gina Duscher, Gerd Halfwassen, Albert Hold, Beatrice Gaczensky, Dominique-Silvia Kemp, Thomas van Zütphen.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Gabler ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH

Geleitwort

Vertrauen ist die Basis der Digitalisierung

Wenn es um die weitere Entwicklung unserer Gesellschaft und Wirtschaft geht, dominiert ein Wort die Debatte: Digitalisierung. Dass Menschen, Maschinen und Geräte zunehmend miteinander vernetzt werden, ist Konsens. Diskutiert wird allerdings, ob das gut oder schlecht ist. Sorgt die Digitalisierung dafür, dass die Menschen entlastet werden, und damit für Fortschritt, Komfort und Freiheit? Oder sorgt sie dafür, dass unser Gesellschafts- und Sozialsystem kollabiert und wir zum gläsernen Bürger werden, der die Kontrolle über die eigenen Daten verloren hat und dessen Arbeit kaum mehr benötigt wird? Die Antworten kann keiner alleine kennen. Vermutlich werden sie nicht schwarz oder weiß ausfallen, sondern irgendwo dazwischenliegen. Sicher ist allerdings: Wir können diese Entwicklung nicht verhindern, nur gestalten. Experten gehen davon aus, dass bis zum Jahr 2020 mehr als 50 Milliarden Geräte miteinander vernetzt sein werden: von Smartphones über Autos bis hin zu Industriemaschinen. Dadurch entsteht eine unvorstellbare Menge an Daten, die gespeichert und verarbeitet werden. Diese Daten werden zum wichtigsten Rohstoff unserer digitalen Gesellschaft, zum Öl unserer Wirtschaft.

Digitalisierung bietet großartige Chancen

Zweifellos ergeben sich durch die Digitalisierung großartige Chancen: mehr Sicherheit im Straßenverkehr zum Beispiel durch selbststeuernde Autos. Oder die Übernahme von lästigen Aufgaben durch Maschinen, die direkt miteinander kommunizieren können. Oder gar ein längeres und gesünderes Leben durch telemedizinische Anwendungen sowie neue Forschungsergebnisse durch die Auswertung großer Datenmengen. Eine entscheidende Voraussetzung für die erfolgreiche Digitalisierung ist allerdings das Vertrauen der Menschen in Datenschutz und Sicherheit der neuen Dienste. Ohne Vertrauen werden die Menschen die neuen Dienste nicht nutzen. Im Gegenteil: Es wird eher der Reflex entstehen, die Entwicklungen der Digitalisierung verhindern zu wollen.

Das ist aber nicht möglich: Untergraben wir die Entwicklung der Digitalisierung in Europa, entstehen die neuen Dienste eben weiterhin vor allem an der Westküste der USA. Den Europäern bliebe nur die Möglichkeit, ihre Daten dorthin zu geben und veredelte

Produkte zurückzuerhalten – Europa als digitale Kolonie sozusagen. Im Bereich der Dienste für Endkunden ist das überwiegend schon heute der Fall: An Facebook, Google und Co. kommt niemand vorbei. Besser sind die Chancen im Markt für Geschäftskunden-Lösungen: Das Internet der Dinge und die Industrie 4.0 bieten den Europäern die Chance, bei der Digitalisierung aufzuholen.

Datenschutz und digitale Geschäftsmodelle sind kein Gegensatz

Politik, Wirtschaft, Wissenschaft und Gesellschaft sind deshalb in der Verantwortung, die richtigen Leitplanken zu entwickeln, damit die Menschen den neuen Diensten vertrauen können. Dabei muss die digitale Souveränität der Menschen im Vordergrund stehen. Sie wird gewährleistet durch ein hohes Maß an Transparenz, Entscheidungsfreiheit der Kunden und die Entwicklung von datenschutzfreundlichen Lösungen. Dafür müssen Datenschutzexperten von Anfang an in die Entwicklung neuer Produkte und Dienste einbezogen werden, in denen personenbezogene Daten verarbeitet werden. Kunden müssen einfach verstehen können, wofür ihre Daten genutzt werden sollen, und dann bewusst darüber entscheiden können. Zudem braucht es für digitale Geschäftsmodelle effektive Methoden der Anonymisierung und Pseudonymisierung, die sicherstellen, dass einzelne Personen ohne ihre Zustimmung nicht identifizierbar sind.

Wir haben in Deutschland und Europa traditionell ein hohes Datenschutzniveau. Es ist gut, dass wir mit der Datenschutzgrundverordnung einheitliche Regeln in ganz Europa bekommen, die gleichzeitig ein hohes Datenschutzniveau garantieren und dennoch neue digitale Geschäftsmodelle ermöglichen. Es kann nicht darum gehen, einzelne Branchen oder Modelle der Datenverarbeitung zu regulieren. Vielmehr benötigen wir klare und einheitliche Leitplanken für den Umgang mit Daten, die sowohl für die Kunden als auch die Unternehmen Sicherheit und Vertrauen schaffen. Zudem brauchen die Menschen Bildung und Informationen zum Umgang mit Technologien und den eigenen Daten – und das von Kindesbeinen an.

Sicherheit muss einfach sein

Mit der Digitalisierung steigt aber auch das Risiko für Verbraucher und Unternehmen, Opfer digitaler Angriffe zu werden. Die wirtschaftlichen Schäden durch Cyberangriffe schätzt das Center for Strategic and International Studies (CSIS) weltweit auf mehr als 400 Milliarden Euro pro Jahr. Täglich gibt es bis zu 400.000 neue Viren, Würmer und Trojaner im Netz. Hinzu kommt, dass Cyberkriminelle Schwachstellen inzwischen innerhalb von wenigen Stunden ausnutzen können und täuschend echte Mails versenden, um Schadcodes einzuschleusen. Vom befallenen Rechner aus kapern die Kriminellen weitere Rechner im Unternehmensnetz und suchen sich die Informationen, die sie haben möchten. Oft dauert es Monate, bis die betroffenen Unternehmen merken, dass sich ein Angreifer im Netz befindet oder befunden hat.

Sicherheitsbehörden, Unternehmen und Privatpersonen müssen deshalb ebenfalls aufrüsten, um sich besser zu schützen. Verhaltensbasierte Analyse und Analyse von Systemzuständen heißen die Schlüsselwörter aktueller Cyberabwehr. Prävention durch Schutzwäl-

le um die IT-Systeme alleine genügt nicht. Häufig sitzen die Kriminellen – etwa durch ausgefeilte Social-Engineering-Maßnahmen – bereits im Netz. Dann geht es darum, sie möglichst schnell zu entdecken. Aufgespürt werden können diese Angreifer durch Beobachtung von Anomalien in Netzen. Für die Entwicklung solcher Lösungen bündelt die Telekom ihre Expertise derzeit in einer neuen Organisationseinheit, der „Telekom Security".

Bei den neuen Sicherheitsprodukten steht eines im Vordergrund: Sicherheit muss einfach sein. Bisher war die Sicherheit von Lösungen und Produkten eher eine Zusatzfunktion, die ins fertige Produkt integriert wurde. Zunehmend wird sie von Anfang an mitgedacht und so besser integriert.

Aus Perspektive des Anwenders gilt aber auch: Vier von fünf Angriffen sind bereits durch einfache Schutzmaßnahmen aufzuhalten. Deshalb ist es so wichtig, dass Nutzer beispielsweise einen aktuellen Virenschutz verwenden und das Betriebssystem immer auf dem aktuellen Stand halten. Smartphones sind übrigens Hochleistungsrechner, die genauso geschützt werden müssen. Auch diese Eigenverantwortung gehört zur digitalen Souveränität.

Sie sehen: Die Debatte über die Digitalisierung hat viele Aspekte, und Sicherheit ist ein entscheidender Erfolgsfaktor. Ich freue mich, dass der Cyber Security mit diesem Buch die nötige Aufmerksamkeit gegeben wird, und wünsche Ihnen eine spannende Lektüre!

Ihr
Dr. Thomas Kremer
Vorstand Datenschutz, Recht und Compliance der Deutschen Telekom

Autor

Dr. Thomas Kremer ist seit Juni 2012 Vorstand für Datenschutz, Recht und Compliance bei der Deutschen Telekom AG. Im September 2013 wurde er darüber hinaus in die Regierungskommission Deutscher Corporate Governance Kodex berufen. Seit November 2015 ist er zudem Vorsitzender des Vereins „Deutschland sicher im Netz". Vor seiner Tätigkeit bei der Deutschen Telekom arbeitete Kremer für die ThyssenKrupp AG. Nach seinem Eintritt in die Rechtsabteilung im Jahr 1994 übernahm er dort 2003 als Chefjustitiar die Leitung der Holding-Rechtsabteilung der ThyssenKrupp AG, die im weiteren Verlauf auch das Compliance-Programm entwickelte. 2007 wurde er zusätzlich zum Chief Compliance Officer des Konzerns ernannt. Im Jahr 2009 übernahm er die Leitung des neu gegründeten Corporate Centers Legal & Compliance, 2011 erfolgte die Ernennung zum Generalbevollmächtigten.

Zu den weiteren Stationen in seinem beruflichen Werdegang zählt die Arbeit als Rechtsanwalt in der Sozietät Schäfer, Wipprecht, Schickert in Düsseldorf (heute CMS Hasche Sigle). Nach seinem Studium der Rechtswissenschaften war Thomas Kremer als wissenschaftlicher Mitarbeiter an der Rheinischen Friedrich-Wilhelms-Universität in Bonn tätig. 1994 promovierte er zum Doktor der Rechte.

Inhaltsverzeichnis

Security: Die echte Herausforderung für die Digitalisierung

1

Ferri Abolhassan

1.1 Intro

Zugausfälle vorhersehen und so Schäden bis in sechsstelliger Höhe pro Ausfall vermeiden. Oder heute dem Einkauf schon sagen können, welche Artikel übermorgen von Kunden bestellt werden. Das ist schon Realität. Warum weiß der CIO meist sogar mehr und schneller über das Kerngeschäft Bescheid als der CEO oder die Fachbereiche? Weil er dank Digitalisierung mit IoT & Co. Unmengen von Informationen zu Kunden, Maschinen und Prozessen gewinnt. Und das ist neu. Damit ist er in der Lage, besser und vor allem schneller – idealerweise in Echtzeit – Entscheidungen vorzubereiten und zu treffen. Damit wird der CIO mehr denn je zum wichtigsten Sparringspartner und Impulsgeber für den CEO.

Doch um dieser Rolle gerecht zu werden, muss die Technik hundertprozentig funktionieren. Um dem CIO den Rücken freizuhalten, bedarf es dreierlei. Erstens: Die IT muss stabil laufen. Zweitens: Die eingesetzten Lösungen müssen zuverlässig zusammenspielen. Und drittens: Neben höchster Qualität muss vor allem ein Maximum an Sicherheit gewährleistet sein. Das ist die absolute Voraussetzung. Denn mit zunehmender Digitalisierung hängt die Geschäftsfähigkeit von Unternehmen zunehmend von der IT ab. Erst wenn Qualität, Zuverlässigkeit **und** Sicherheit nachhaltig stimmen, gewinnt der CIO die notwendigen Freiheitsgrade für Innovationen. Und erst dann kann er wirklich Fahrt in Sachen Digitalisierung aufnehmen. Das Rückgrat dafür ist die Cloud. Denn nur sie kann die Masse an strukturierten und vor allem unstrukturierten Daten zentral sammeln, speichern und auswerten und so maximalen Nutzen aus digitalen Technologien ziehen – selbst wenn der Datenberg weiter wächst.

Daten und die Erkenntnisse daraus werden immer wertvoller. Und sind zu schützen. In jeder Hinsicht – physisch, technisch und rechtlich. Das wissen wir. Und doch tun wir zu wenig dafür. Weil Sicherheit komplex, unbequem und langsam ist. Das muss sich ändern. Security muss einfach sein, damit sie genutzt wird. Das heißt: einfach zu beziehen, einfach zu betreiben und einfach zu bedienen. Denn Sicherheit ist kein Selbstzweck – sondern

F. Abolhassan (Hrsg.), *Security Einfach Machen*,
DOI 10.1007/978-3-658-14945-1_1,