

Management for Professionals

Ferri Abolhassan *Editor*

Cyber Security. Simply. Make it Happen.

Leveraging Digitization
Through IT Security



Springer

Management for Professionals

More information about this series at <http://www.springer.com/series/10101>

Ferri Abolhassan
Editor

Cyber Security. Simply. Make it Happen.

Leveraging Digitization Through IT
Security

Editor
Ferri Abolhassan
Telekom Deutschland GmbH
Bonn, North Rhine-Westphalia
Germany

Editing: Gina Duscher, Gerd Halfwassen, Albert Hold, Beatrice Gaczensky,
Dominique-Silvia Kemp, Thomas van Zütphen, Martin Farrent
Translation: Dr. Edward M. Bradburn, Daina Jauntirans, Stephen McLuckie, Niamh
Ruddy and Jessica Spengler for Malinowski & Partner

ISSN 2192-8096 ISSN 2192-810X (electronic)
Management for Professionals
ISBN 978-3-319-46528-9 ISBN 978-3-319-46529-6 (eBook)
DOI 10.1007/978-3-319-46529-6

Library of Congress Control Number: 2016958508

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Cover illustration: eStudio Calamar, Berlin/Figueres

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

Trust Is the Basis of Digitization

Thomas Kremer

When it comes to the future development of our society and economy, one word dominates the discussion: digitization. The consensus is that people, machines, and devices will become increasingly networked. The debate, however, is whether this is something good or bad. Will digitization unburden people and bring progress, comfort, and freedom? Or will it bring about the collapse of our social and welfare systems, turning us into transparent citizens who have lost control of their own data and whose labor is no longer needed? No single person can answer these questions – and the answers will probably not be black or white but rather somewhere in between. One thing is certain, however: we cannot prevent this development; we can only influence it. Experts predict that by the year 2020, more than 50 billion devices will be connected to one another, from smartphones to cars to industrial machines. This will generate an unimaginable amount of data to be stored and processed. And this data is going to be the most important resource for our digital society, the oil of our economy.

Digitization Offers Great Opportunities

Digitization undoubtedly promises great opportunities: safer road traffic thanks to self-driving cars, for example. Or the prospect of cumbersome tasks being handled by machines that can communicate directly with one another. Or even a longer and healthier life thanks to telemedicine applications and new research results emerging from the analysis of large volumes of data. But for digitization to succeed, it is critical for people to trust in data protection and the security of these new services. Without trust, people will not use the new services. On the contrary: Their knee-jerk reaction will be to try to prevent digital developments.

This is not possible, however. If we undermine the development of digitization in Europe, the new services will be created anyway – mostly on the west coast of the USA. Then, the only option for Europeans would be to send their data there and get modified products in return. Europe would become a kind of digital colony. In the

area of services for end customers, this is already largely the case. No one can get around Facebook, Google and Co. The chances are better in the market for business customer solutions. The Internet of Things and Industry 4.0 offer Europeans an opportunity to catch up with digitization.

Data Protection and Digital Business Models Are Not in Opposition

Politics, business, science, and society therefore have a responsibility to establish the right guide rails so that people can trust the new services. The digital sovereignty of the individual must be the priority here. This can be guaranteed by a high degree of transparency, freedom of choice for customers, and the development of solutions amenable to data protection. For this to be possible, data protection experts must be involved right from the start in the development of new products and services that handle personal data. Customers must be able to easily understand how their data will be used so that they can make informed decisions about it. Furthermore, we need effective methods of anonymizing and pseudonymizing data for digital business models so that individuals cannot be identified without their consent.

We have traditionally had a high level of data protection in Germany and Europe. It is good that the EU's General Data Protection Regulation will establish standardized rules throughout Europe which guarantee a high degree of data protection while at the same time enabling new digital business models. The focus cannot be on regulating individual industries or data processing models. Instead, we need clear, standardized guidelines for handling data, which create security and trust for customers and companies alike. People also have to be educated and informed about the use of technologies and their personal data – from an early age.

Security Has to Be Simple

Digitization additionally increases the risk of consumers and companies falling victim to digital attacks. The Center for Strategic and International Studies (CSIS) estimates that the economic damage from cyberattacks amounts to more than 400 billion euros per year worldwide. Up to 400,000 new viruses, worms, and Trojans are found in the network every day. What's more, cybercriminals can now take advantage of vulnerabilities within just a few hours and send deceptively realistic emails in order to sneak in malicious code. These criminals can then use the infected computers to hijack other machines in a corporate network and search for the information they want. It often takes months for the affected companies to notice that there was – or is – an attacker in their network.

Security authorities, companies, and private individuals therefore also have to upgrade in order to protect themselves better. Behavior-based and system-status

analyses are the keywords in cyberdefense today. Merely placing firewalls around IT systems is not enough. In many cases, the criminals have used sophisticated social-engineering mechanisms – so they are already in the network. The task then is to find them as quickly as possible. These attackers can be detected by monitoring anomalies in the network. To develop solutions such as this, Deutsche Telekom is currently pooling its expertise in a new organizational unit, “Telekom Security.”

There is one principle at the forefront of these new security products: Security has to be simple. Until now, the security of solutions and products has tended to be a supplementary function added to a finished product. But it is increasingly being incorporated right from the start, thus ensuring better integration.

From the user’s perspective, too, it is important to remember that four out of five attacks could be prevented using simple security measures. This is why it is so critical for users to always keep their virus protection and operating systems up to date, for example. Incidentally, smartphones are powerful computers that require just as much protection. This personal responsibility is yet another aspect of digital sovereignty.

As you can see, there are many facets to the digitization debate, and security is a critical factor for success. I am delighted that this book is giving cybersecurity the attention it demands, and I hope you enjoy reading it!

Yours,
Dr. Thomas Kremer

Member of the Board of Management for Data Privacy, Legal Affairs and Compliance of Deutsche Telekom



Dr. Thomas Kremer has been Member of the Board of Management for Data Privacy, Legal Affairs and Compliance at Deutsche Telekom since June 2012. He was appointed to the Government Commission on the German Corporate Governance Code in September 2013. He has also been Chairman of “Making Germany Safe on the Net” (DSiN) since November 2015. Before moving to Deutsche Telekom, Kremer worked for ThyssenKrupp AG, joining the company’s legal department in 1994. In 2003, as General Counsel, he took over the management of ThyssenKrupp’s Holding legal department, which also subsequently went on to develop the

company’s Compliance program. After taking over the management of the newly formed Corporate Center Legal and Compliance in 2009, Kremer was then appointed Executive Vice President in 2011.

Among other positions held prior to ThyssenKrupp and Telekom, Kremer also was an attorney at law firm Schäfer, Wipprecht, Schickert in Düsseldorf (now CMS Hasche Sigle). After graduating in law, Thomas Kremer worked as a research assistant at the University of Bonn in Germany before receiving his doctorate in law in 1994.

Contents

1	Security: The Real Challenge for Digitalization	1
	Ferri Abolhassan	
1.1	Introduction	1
1.2	Status Quo: The Cloud Is the Backbone of Digitalization	2
1.3	Data Security: Only a Secure Cloud Will Lead to Secure Digitalization	3
1.3.1	Risk Transformation: It Has to Be Easy to Get into the Cloud	4
1.3.2	Risk of an Incident: Making Sure the Cloud Doesn't Crash	5
1.3.3	Risk of Technical/Physical Attack: A Castle Wall Alone Isn't Enough	6
1.3.4	Risk of a Cyberattack: Ensuring Data and Devices Aren't Casualties	7
1.4	Looking to the Future	9
1.5	Conclusion	9
	References	10
2	Security Policy: Rules for Cyberspace	13
	Wolfgang Ischinger	
2.1	Taking Stock: Digital Warfare in the 21st Century	14
2.2	Challenges for the Political Sphere: Rules, Resources and Expertise	15
2.3	Outlook: A Strategy for the Digital Age	18
	References	19
3	Data Protection Empowerment	21
	Peter Schaar	
3.1	Code Is Law	22
3.2	Empowerment	23
3.3	Information Technology and Social Values	26
	References	26

4	Red Teaming and Wargaming: How Can Management and Supervisory Board Members Become More Involved in Cybersecurity?	27
	Marco Gercke	
4.1	Cybersecurity: A Management Board Issue	27
4.2	Integrating the Management Board into Existing Cybersecurity Strategies	28
4.3	Red Teaming and Wargaming	28
4.3.1	Red Teaming Defined	29
4.3.2	Wargaming Defined	29
4.3.3	Differences Compared with Methods Currently in Use	29
4.4	Use of Red Teaming in Combination with Wargaming at Companies	30
4.4.1	Classification	31
4.4.2	Definition of a Target	31
4.4.3	Composition of the Teams	32
4.4.4	Analysis: Data Collection and Evaluation	32
4.4.5	Wargaming	33
4.4.6	Report	34
4.5	Conclusion	34
	References	34
5	The Law and Its Contribution to IT Security: Legal Framework, Requirements, Limits	37
	Klaus Brisch	
5.1	Key Features of the Existing Legal Framework	38
5.1.1	IT Compliance: A Challenge for Management Boards and Executives	38
5.1.2	Who Is Responsible?	39
5.1.3	Regulation on Determining Critical Infrastructure	41
5.1.4	Controversial: Changes Affecting Telemedia Services	42
5.2	International Issues: The European Union's Directive on Security of Network and Information Systems (NIS Directive)	42
5.3	Data Protection and Data Security in the United States	43
5.4	Data Exchange Between EU and US Companies	43
5.4.1	Safe Harbor	44
5.4.2	Privacy Shield	44
5.5	Conclusion: Many Legal Issues to Consider	44
	References	45

6	IT Security: Stronger Together	47
	Ralf Schneider	
6.1	The Trinity of IT Security	48
6.2	CSSA – Security Through Collaboration	49
	6.2.1 Targeted Interaction	50
	6.2.2 Network of Trust	50
6.3	The Six Elements of an Integrated Defense Strategy	51
	6.3.1 Prevention Is Better Than the Cure	52
	6.3.2 Knowledge Is Power	53
	6.3.3 IT Security Is Not an End in Itself	54
	6.3.4 It’s Only a Matter of Time: Incident Management	55
	6.3.5 Fitness Training: Prepare for Emergencies	56
	6.3.6 Stronger Together	56
6.4	Conclusion	56
	References	57
7	The German Security Market: Searching for the Complete Peace-of-Mind Service	59
	Markus a Campo, Henning Dransfeld, and Frank Heuer	
7.1	Challenges for IT Security Managers	59
7.2	Choosing the Right Protection in a Fragmented Market	61
	7.2.1 Data Leakage/Loss Prevention (DLP)	61
	7.2.2 Security Information and Event Management (SIEM)	61
	7.2.3 Email/Web/Collaboration Security	61
	7.2.4 Endpoint Security	62
	7.2.5 Identity and Access Management (IAM)	62
	7.2.6 Mobile Security – Are Employees Really the Biggest Risk?	63
	7.2.7 Network Security	64
	7.2.8 Conclusion	65
7.3	Security from a Single Source: Managed Security Services	65
	7.3.1 Managed Service or Cloud Solution?	66
	7.3.2 Selection Criteria	67
	7.3.3 Assessment of Deutsche Telekom/T-Systems as a Managed Security Services Provider	67
	7.3.4 Specialized Managed Security Services	69
8	CSP, not 007: Integrated Cybersecurity Skills Training	71
	Rüdiger Peusquens	
8.1	The New Profession of Cybersecurity Specialist: From IT Worker to IT Security Expert	71
8.2	Hands-on Experience in All-Round Security	72
8.3	Cybersecurity Expertise for Managers, too	73
8.4	Conclusion	73
	Reference	74

9	Human Factors in IT Security	75
	Linus Neumann	
9.1	IT Security Is Just Not Very People-Centric	75
	9.1.1 The Thing with Passwords	76
	9.1.2 The “Security versus Productivity” Dilemma	77
9.2	Social Engineering	77
9.3	Human “Weaknesses” Are Often Social Norms or Simple Instincts	79
	9.3.1 Would You Mind Installing This Malware on Your Computer?	79
	9.3.2 Excuse Me, What Exactly Is Your Password?	81
9.4	Would You Please Transfer Me a Few Million?	82
9.5	Defensive Measures	83
	9.5.1 Recognizing Social Engineering	84
	9.5.2 The Learning Objective: Reporting Suspicious Activity	84
	9.5.3 Practice Makes Perfect	85
9.6	Conclusion: IT Must Work for and Not against Users	86
	Reference	86
10	Secure and Simple: Plug-and-Play Security	87
	Dirk Backofen	
10.1	Data Security in the Danger Zone	88
10.2	Digitalization Needs New Security Concepts	91
10.3	Digital Identity Is the New Currency	92
10.4	Does Absolute Protection Exist?	93
10.5	This Is What Attack Scenarios Look Like Today	94
10.6	In Need of Improvement: Security at SMEs	95
10.7	Expensive Does Not Necessarily Mean Secure: Gaps in Security at Large Companies	96
10.8	The “Made in Germany” Stamp of Quality	96
10.9	Companies Want the Cloud – But Securely	97
	References	98
11	Cybersecurity - What’s Next?	101
	Thomas Tschersich	
11.1	The Motives of Attackers Are Becoming More Malicious with Each Passing Generation	101
11.2	Cybersecurity – The Sleeping Giant in the Company	106
11.3	What Will Protect Us?	108
11.4	Conclusion	111
	References	111
12	Conclusion	113
	Ferri Abolhassan	
12.1	The Internet Has Become Ubiquitous	113
12.2	Good Internet, Bad Internet	114