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

Springer

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

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