
Data Security

Thomas H. Lenhard

Data Security

Technical and Organizational
Protection Measures against Data
Loss and Computer Crime

 Springer

Thomas H. Lenhard
Comenius Universität
Bratislava, Slovakia

ISBN 978-3-658-35493-0 ISBN 978-3-658-35494-7 (eBook)
<https://doi.org/10.1007/978-3-658-35494-7>

This book is a translation of the original German edition „Datensicherheit“ by Lenhard, Thomas H., published by Springer Fachmedien Wiesbaden GmbH in 2020. The translation was done with the help of artificial intelligence (machine translation by the service DeepL.com). A subsequent human revision was done primarily in terms of content, so that the book will read stylistically differently from a conventional translation. Springer Nature works continuously to further the development of tools for the production of books and on the related technologies to support the authors.

© Springer Fachmedien Wiesbaden GmbH, part of Springer Nature 2021

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 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, expressed 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.

This Springer imprint is published by the registered company Springer Fachmedien Wiesbaden GmbH part of Springer Nature.

The registered company address is: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Contents

1	Introduction	1
2	Data Protection and Data Security	3
3	How Computers Communicate with Each Other	5
4	What Can Happen to Data?	15
5	Hazards in the Technical Environment	17
6	Dangerous Software	25
6.1	The Trojan Horse	27
6.2	The Virus	31
6.3	The Logical Bomb	34
6.4	The Keylogger	35
6.5	The Sniffer	35
6.6	The Back Door	39
7	Removable Media, USB Devices, Smartphones and Other Mobile Devices	41
8	Telephone Systems	45
9	The Greatest Danger in a Digitalized World	51
10	Data Destruction	55
11	Data Backup and Restore	61
12	Encryption	65
13	Website Hacking	69

14	Common Security Problems	73
14.1	Working Consoles that Are Not Locked	73
14.2	Printer Stations and Multifunction Devices	74
14.3	Working with Administrator Privileges	74
14.4	The Internet of Things and Industrial Control Systems	75
15	Identification of Computers and IP Addresses	77
16	The Firewall	81
17	The Router	85
18	Configuration of Security Systems	87
19	The Demilitarized Zone	93
20	Organizational Data Security	99
21	Notes	101
	Closing Words	105
	Literature	107
	Index	109

Abbreviations

Cat-7	Cable Category 7
CCC	Chaos Computer Club
CRM	Customer relationship management
CTI	Computer telephony integration
DBMS	Database management system
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized zone
DNS	DNS
DVD	Digital Versatile Disc
EN 50173-1	European Normative 50173-1:2011 about Information technology—Generic cabling systems—Part 1: General requirements
ERP	Enterprise resource planning
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
LLC	Logical link control
MAC	Media access control
NAS	Network attached storage
NTFS	New technology file system
NTP	Network Time Protocol
OSI	Open System Interconnection
PBX	Private branch exchange (telephone system)
PGP	Pretty Good Privacy
POP	Post Office Protocol
RFID	Radio-frequency identification

RJ45	Registered jack 45
SFTP	Secure File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSD	Solid-State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transaction Control Protocol
Telnet (TNP)	Telecommunication Network Protocol
TLS	Transport Layer Security
UNC	Uniform Naming Convention
USB	Universal Serial Bus
UPS	Uninterruptible power supply
VoIP	Voice over IP (Internet Protocol)
VPN	Virtual private network
WEP	Wired Equivalent Privacy
WLAN	Wireless local area network
WPA	Wi-Fi Protected Access

List of Figures

Fig. 3.1	The OSI model	7
Fig. 3.2	Additional information in the address field of the browser	12
Fig. 3.3	Ping	13
Fig. 5.1	A server cabinet in the deepest cellar of the building	18
Fig. 5.2	A steel tray to protect IT equipment from pipes	20
Fig. 5.3	Chaos in a part of a clinical “computer centre”	22
Fig. 6.1	Wireshark analyzing database queries	36
Fig. 8.1	Separation of IT and telephone network	48
Fig. 10.1	Calibre .44 Magnum and other creative ideas are not suitable as a secure method of data destruction	58
Fig. 19.1	Positioning of a DMZ network	94

List of Table

Table 3.1 Services and port numbers 10