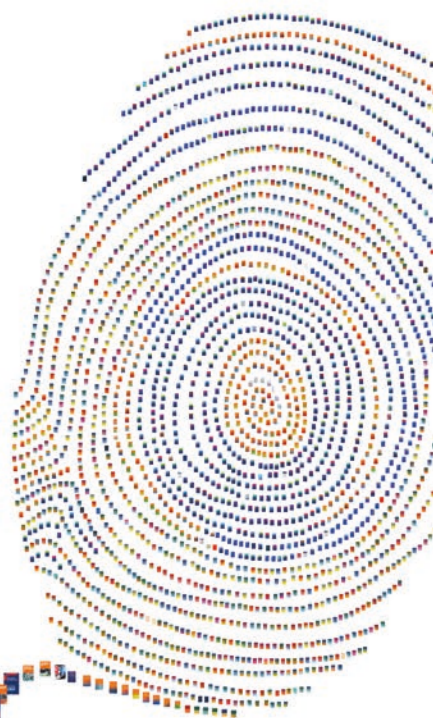

Datenschutz – Konzepte, Algorithmen und Anwendung

Lizenz zum Wissen.

Sichern Sie sich umfassendes Technikwissen mit Sofortzugriff auf tausende Fachbücher und Fachzeitschriften aus den Bereichen: Automobiltechnik, Maschinenbau, Energie + Umwelt, E-Technik, Informatik + IT und Bauwesen.

Exklusiv für Leser von Springer-Fachbüchern: Testen Sie Springer für Professionals 30 Tage unverbindlich. Nutzen Sie dazu im Bestellverlauf Ihren persönlichen Aktionscode **C0005406** auf www.springerprofessional.de/buchaktion/



Jetzt
30 Tage
testen!

Springer für Professionals.
Digitale Fachbibliothek. Themen-Scout. Knowledge-Manager.

- 🔍 Zugriff auf tausende von Fachbüchern und Fachzeitschriften
- 📄 Selektion, Komprimierung und Verknüpfung relevanter Themen durch Fachredaktionen
- 🔗 Tools zur persönlichen Wissensorganisation und Vernetzung

www.entschieden-intelligenter.de

Springer für Professionals

 Springer

Markus von Rimscha

Datenschutz – Konzepte, Algorithmen und Anwendung

Werkzeuge zum Datenschutz im Alltag

Markus von Rimscha
Fürth, Deutschland

Das in diesem Werk enthaltene Programm-Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor übernimmt infolgedessen keine Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

ISBN 978-3-658-22045-7 ISBN 978-3-658-22046-4 (eBook)
<https://doi.org/10.1007/978-3-658-22046-4>

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

Springer Vieweg

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2018

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

„Datenschutz ist Verbrecherschutz.“ Ja, das stimmt. Datenschutz schützt *auch* die Daten von Verbrechern. Datenschutz ist also im gleichen Maße Verbrecherschutz wie Autos Verbrechertransportmittel sind und Brot Verbrechernahrung.

Hat denn der brave, unbescholtene Bürger etwas zu verbergen? Ja, hat er. Ja, habe ich. Das nennt man Privatsphäre. Oder Betriebsgeheimnisse. Vielleicht tausche ich mit meinem Steuerberater Daten aus? Verschicke einen Krankenbericht? Arbeite an einer Erfindung? Schreibe in freudiger Erwartung eines schönen Abends zu zweit die eine oder andere Nachricht, die ziemlich eindeutig ist – ein wenig unanständig womöglich? Geht's Dich was an?

Post-Privacy ist toll. Eine Welt wäre doch toll, in der man ganz auf Datenschutz verzichten könnte, weil es gar keine Diskriminierung mehr gäbe, die letztendlich der Grund für ein Bedürfnis nach Privatsphäre ist ... Ist das so? ... „wäre“, „könnte“, „gäbe“ ... Ja, das kann man so sehen, ... muss man aber nicht.

Ich gehe davon aus, dass die Privatsphäre ein hohes Gut ist. Ich gehe davon aus, dass Betriebsgeheimnisse ein hohes Gut sind. Ich gehe davon aus, dass Daten schützenswert sind. Ich lade Dich, liebe Leserin, lieber Leser, dazu ein, gemeinsam mit mir technische Wege zu erforschen, wie vertrauliche Daten vor unerwünschtem Zugriff oder Beschädigung geschützt werden können.

Schwarzmalerei hilft dabei wenig und ist auch gar nicht nötig. Initiativen wie „Digital Courage“ oder „Netzpolitik.org“ sind nicht ohne Grund entstanden. Guter Datenschutz sowohl als Standortfaktor als auch als Wettbewerbsvorteil wird mittlerweile auch bei größeren Playern erkannt – nicht mehr nur von kleinen Nischenanbietern. Gleichzeitig agieren einige Teilnehmer immer enthemmter.

Wirksamer Datenschutz ist und bleibt daher in weiten Teilen eine Holschuld des Verbrauchers – um nicht zu sagen eine „Tun“-Schuld. Genau das soll hier unser Thema sein.

Dir, lieber Leser, liebe Leserin, wünsche ich nun viel Spaß beim Lesen und insbesondere natürlich viel Erfolg bei der Umsetzung!

Fürth, im März 2018

Markus von Rimscha

Inhaltsverzeichnis

1	Einleitung	1
1.1	Datenschutz im Spannungsfeld	2
1.2	Was sind meine Daten wert?	6
	Literatur	7
2	Algorithmen	9
2.1	Symmetrische Verschlüsselung	10
2.1.1	ROT	10
2.1.2	XOR	11
2.1.3	Rijndael/AES	13
2.1.4	Sonstige	21
2.2	Asymmetrische Verschlüsselung	21
2.2.1	RSA	23
2.2.2	McEliece	24
2.2.3	Sonstige	33
2.3	Hash-Funktionen	33
2.4	Zufallszahlen	38
2.5	Sicherheit	39
2.5.1	Quanten-Kryptographie	41
2.5.2	Post-Quanten-Kryptographie	42
2.6	Ergänzende Strategien	43
2.6.1	Hybride Verschlüsselung	43
2.6.2	Perfect Forward Secrecy	46
2.6.3	Bewusste Verlangsamung	47
2.7	Bewertung gängiger Verfahren	48
	Literatur	49

3	Anwendungen	51
3.1	Schutz wovor? Schutz wie?	53
3.1.1	Wer greift uns an?	53
3.1.2	Wer verarbeitet welche Daten?	56
3.1.3	Was ist unsere Strategie?	59
3.2	Ersteinrichtung eines neuen Geräts	62
3.2.1	Updates	63
3.2.2	Systemeinstellungen	63
3.2.3	Software-Quellen	64
3.2.4	Ungenutzte Funktionen	65
3.2.5	Dateiendungen	65
3.2.6	Virens Scanner	66
3.3	Passwortsicherheit und Authentifizierung	67
3.3.1	Passwörter	67
3.3.2	Passwort-Safes	69
3.3.3	Passwort-Verwaltung im Browser	71
3.3.4	Passwörter regelmäßig ändern	72
3.3.5	2-Faktor-Authentifizierung	72
3.3.6	Single-Sign-On	73
3.3.7	Biometrische Zugangskontrolle	75
3.4	Verschlüsselung des gesamten Systems	76
3.4.1	Handy/Tablet	76
3.4.2	Desktop-PC/Notebook	76
3.5	Verschlüsselung lokaler Daten	77
3.5.1	Verschlüsselte ZIP-Archive	77
3.5.2	Verschlüsselte Container	78
3.5.3	Verschlüsselung einzelner Dateien	79
3.6	Internetzugang	79
3.6.1	Router- und Firewall-Konfiguration	80
3.6.2	Öffentliches WLAN	82
3.7	Verschlüsselung und Synchronisation von Cloud-Daten	82
3.7.1	Ende-zu-Ende-Verschlüsselung	83
3.7.2	Containerbasierte Verschlüsselung	85
3.7.3	Dateibasierte Verschlüsselung	86
3.8	Verschlüsselung externer Datenträger	87
3.8.1	USB-Datenträger	87
3.8.2	Netzwerk-Speicher	89
3.9	Vertrauliche Kommunikation	89
3.9.1	E-Mail	89
3.9.2	Messenger	106

3.10	Internet-Nutzung	107
3.10.1	Rechner-Accounts	107
3.10.2	Web-Accounts	108
3.10.3	Browser-Einstellungen	109
3.10.4	Datensparsamkeit	110
3.10.5	Suchmaschinen	111
3.10.6	Fremdinhalte	111
3.10.7	Cookies	114
3.10.8	HTTPS	115
3.10.9	Online-Banking	116
3.10.10	Top-Level-Domains	121
3.10.11	Cloud-Anwendungen	122
3.10.12	TV, Multimedia und Spielkonsolen	124
3.10.13	Internet of Things	125
3.10.14	Anonymisierung, Wiedererkennung, Lokalisierung	126
3.10.15	Vertrauens-Netzwerke	130
3.11	Aktive Schnittstellen	131
3.12	Desktop-Anwendungen und Apps	132
3.13	Schadensbegrenzung	133
3.13.1	Anbieter-Hacks	133
3.13.2	Identitäts-Diebstahl	135
3.13.3	Backups	136
3.13.4	Virtuelle Maschinen	137
3.14	Verkauf eines Geräts	138
3.15	Technische Grenzen	139
3.15.1	Betriebssystem und Dateisystem	139
3.15.2	Hardware	141
3.16	AGBs	143
3.17	Die Vertrauensfrage	143
3.18	Die echte Welt	145
3.18.1	Skimming	145
3.18.2	Bonus-Programme	146
3.19	Tagesaktuelle Informationsquellen und Links	147
	Literatur	150
	Stichwortverzeichnis	155