HERBERT HERTRAMPH

DIGITAL CLEANING

INFORMATIONSFLUT BEWÄLTIGEN, DIGITAL AUFRÄUMEN UND ORDNUNG HALTEN MIT SYSTEM

mitp

Herbert Hertramph

Dies ist ein Auszug
aus dem Buch:

Digital Cleaning

Informationsflut bewältigen, digital aufräumen und
Ordnung halten mit System

1. Auflage

mitp

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

ISBN 978-3-95845-535-1
1. Auflage 2017

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

© 2017 mitp Verlags GmbH & Co. KG

Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, 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.

Lektorat: Miriam Robels
Korrektorat: Petra Heubach-Erdmann
Covergestaltung: Sandrina Dralle / Christian Kalkert
Coverbild: © Lightkite, shutterstock.com
Satz: III-satz, Husby, www.drei-satz.de

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

Inhaltsverzeichnis

Einführung 7

Teil 1: JETZT Aufräumen und strukturieren 15

1 Tabula rasa: Beginnen Sie mit einem Black-Box-Archiv 16
1.1 Der 4-Punkte-Plan, um von vorne zu beginnen 19
1.2 Tools, die beim ersten Entrümpeln hilfreich sein können 20

2 Eine Struktur für Ihre Informationen 24
2.1 Mit Master-Ordnern arbeiten 27
2.2 Das chronologische Archiv – »Muster-gültig« 29
2.3 Work in Progress: Das thematische Archiv 33
2.4 Chaosfreundlich: Koffer-Archive 37

3 Lassen Sie aufräumen: Ihre digitalen Dienstboten 42
3.1 Alles im Blick 42
3.2 Struktur von der Stange: Umbenennungstools 43
3.3 Textbausteine nutzen 45

4 Das Fundbüro: Finden statt Suchen 54
4.1 Einfach, schnell und gut: Die Suche in Ihrer Struktur 54
4.2 Hilfreiche Such-Tools 61
4.3 Clouds durchsuchen 63

Teil 2: IN ZUKUNFT Ordnung halten und Zeit sparen 67

5 Automatisierungen für neue Informationen: File Juggler, Hazel und DropIt 68
5.1 Das Heinzelmännchen-Prinzip 68
5.2 Tools, die für Ordnung sorgen 70

6 Papier reduzieren: Analog zu digital 79
6.1 Scanner-Apps: Gut für den Alltagsscan 81
6.2 Flachbettscanner und Scan-Druck-Kombinationen 82
6.3 Dokumentenscanner: Ideal für die gesamte Eingangspost 83
6.4 Wenn Papier aufbewahrt werden muss 85
6.5 Mehr machen mit Scan-PDF-Dateien 86

7 E-Mail-Flut bewältigen 92
7.1 Trash-Mail-Account einrichten 93

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

7.2 Newsletter reduzieren 93
7.3 Umgang mit relevanten Mails. 95
7.4 Suchfunktionen nutzen 97
7.5 MailStore Home – ein ultraschnelles Langzeit-Archiv für E-Mails 98

8 Web-Information 101
8.1 Archive.org – ein Archiv mit Zeitstrahl-Funktion 102
8.2 Pocket und Instapaper 105
8.3 Alternative Speichermöglichkeiten 109
8.4 Feeds: Lassen Sie liefern! 112

9 Mediendateien: Fotos & Co. 118
9.1 Automatisierte Inhaltserkennung 119
9.2 Fotos annotieren 123

10 Notizen: Vom Einkaufszettel bis zur umfangreichen Textnotiz 125
10.1 Notizen für Puristen 126
10.2 Notizen angereichert 130
10.3 An der Schwelle zum Dokumentenmanagement 134
10.4 Notizen überprüfen 141
10.5 Praxisbeispiele für Notiz-Archive. 143

11 Exkurs: Texte mit Markdown strukturieren 146
11.1 Der 7-Minuten-Mini-Markdown-Kurs 148
11.2 Markdown-Editoren: Ulysses und Writemonkey 153

Teil 3: JEDERZEIT Daten sichern und verschlüsseln 157

12 Backup: Strategien für den Alltag 158
12.1 Von Zeitmaschinen und Ablageorten 158
12.2 Mac: Eine Zeitmaschine für alle 161
12.3 Windows: Backup einfach und komfortabel. 162
12.4 Keller oder Cloud? 165
12.5 Cloud – verschlüsselt und mit Standort Deutschland 167

13 Der Cryptograf: Informationen verschlüsseln 174
13.1 Basteln Sie sich ein sicheres Passwort. 174
13.2 Verwenden Sie einen Passwortsafe 178
13.3 Dateien und Ordner verschlüsseln – einfach, sicher und für alle Systeme geeignet 183

14 Dauerhaft aufgeräumt 191

Weiterführende Links 196

Index 198

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

Teil 3

JEDERZEIT Daten sichern und verschlüsseln

Kapitel 13

Der Cryptograf: Informationen verschlüsseln

Wir haben es heute auf Schritt und Tritt mit Login-Vorgängen zu tun: Vom simplen Mail-Zugang über das Onlinebanking, Bezahlvorgänge via Paypal, Accounts im Büro, verschlüsselte Archive – ständig werden PINs, Mail-Adressen, Nutzernamen und Passwörter angefordert. Zwar gibt es Technologien, die auf Merkmalerkennungen wie Fingerabdruck, Irisscan, Stimmerkennung und so weiter beruhen, aber das getippte Pass*wort* dürfte uns noch etliche Zeit als Hauptidentifikationsmerkmal begleiten.

13.1 Basteln Sie sich ein sicheres Passwort

Ähnlich wie bei den Daten »schleppt« man auch hier meist eine ganze Historie mit sich, die irgendwann in der Schulzeit begann. Damals hatte man vielleicht seinen GMX-Account »schocki.mockii@gmx.de« mit dem Passwort »Buffy18« gesichert, später seinen Uni-Account mit »schmidt-2019!«. Dazwischen kamen unzählige Web-Anmeldungen, Amazon-, Facebook- und Twitter-Accounts und ... und ... und ... Besonders »gemein« sind Hochschulen und andere Arbeitgeber, die von ihren Mitarbeitern fordern, alle sechs Monate das Passwort zu wechseln. Dabei kann man nicht einfach aus »1-Rucki!Zucki« ein »2-Rucki!Zucki« machen – das lehnt das System ab, weil das neue Passwort dem vorhergehenden zu ähnlich ist. Oft wird sogar die Einhaltung einer Vielzahl von Kriterien gefordert: ein Sonderzeichen soll dabei sein, mindestens eine Ziffer, ein Großbuchstabe, ein Kleinbuchstabe, mindestens acht Zeichen und so weiter. So, dann sitzt man da, denkt sich was Schönes aus, schließlich passt es – und dann kommt der Urlaub. Ich habe nicht wenige Leute getroffen, die nach drei Wochen herrlich entspannten Tauchvorgängen in der Karibik vor ihrem Account saßen und verzweifelt versuchten, sich an die genaue Schreibweise zu erinnern. Und nach der dritten Fehleingabe war Schluss ...

Dazu kommen all jene Fälle, in denen Datenbanken großer Anbieter von professionell agierenden »Bösewichten« entwendet werden. Wenn Sie dann noch das gleiche Pass-

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

wort für Amazon und Paypal verwenden ... Machen Sie nicht? Bravo! Aber eventuell klicken Sie aus Bequemlichkeit in Ihrem Browser auf »Passwort speichern«? Zwei Klicks genügen – sofern Sie kein Masterpasswort vergeben haben – und alle Informationen zu Ihren Accounts liegen offen. Das kriegt sogar der Kollege aus der Abteilung XY hin, der bei der letzten Beförderung übergangen wurde ...

So, jetzt aber genug der Ausmalerei. Die Basics von guten Passwörtern sind Ihnen inzwischen vertraut: keine Geburtsdaten, keine Namen wie »Waldi« oder »Martha«, keine Nummernfolgen wie »654321« und so weiter. Aber schauen wir mal etwas genauer hin, um zu sehen, wodurch ein Passwort eigentlich »sicher« wird.

Zunächst die gute Nachricht: So einfach, wie in Krimis Passwörter gehackt werden, ist es zum Glück nicht. Zum einen bewahren viele größere Webanbieter Ihr Passwort nicht im Klartext auf – es wird vielmehr durch eine ellenlange Zeichenkette verschlüsselt. Aus »Heidi!!,,1999« wird dann »xzhq,!rsti39__$$qzielkKMkasdiwer_-asdfj«. Wenn solche Zeichenketten entwendet werden, sind die Ausgangspasswörter nicht ohne Weiteres rekonstruierbar.

Zudem ist bei guten Online-Angeboten meist die Anzahl der Versuche begrenzt, oft gibt es auch eine Zeitsperre. Anders sieht es aus, wenn jemand etwa Zugriff zur Hardware oder zu einer verschlüsselten Datei hat und immer wieder von vorne beginnen kann. Dann könnte er schon eher – große Zeiträume und Rechnerkapazitäten vorausgesetzt – erfolgreich sein, indem er alle möglichen Kombinationen durchspielt. Bei diesen »BruteForce«-Attacken wird mit diversen Lexika gearbeitet – sowohl »richtigen« Wörterbüchern als auch solchen, die Erfahrungen von Hackern gesammelt haben und häufig gewählte Varianten beinhalten, zum Beispiel, dass der Buchstabe »E« oft gegen eine »3« ausgetauscht wird. Wenn man auf diesem Weg nicht fündig wird, so hilft bei einem hohen Verschlüsselungsgrad nur noch das Durchspielen von Trillionen möglicher Buchstaben-, Ziffern- und Sonderzeichen-Kombinationen. Und das benötigt zum Glück auch beim heutigen Stand der Technik Zeit – bei einem langen Passwort derart viele Monate und große Rechnerkapazitäten, dass es für den – professionell – Crackenden in der Regel unökonomisch ist, alle Kombinationen durchzuspielen.

Übrigens: Unsinnig ist, was in Filmen oft als Vorgang eines Passworthacks gezeigt wird, um den Vorgang spannend zu machen: Da wird Stelle um Stelle gelöst, ähnlich wie bei einem Spielautomaten die Rotationsscheiben. Passwörter können nur als »Ganzes« entschlüsselt werden. Das Crack-Programm erfährt nicht, ob von »RudiRatlos« die bisherigen Buchstaben »Rudi« schon Bestandteil des endgültigen Passworts sind – es muss immer wieder von vorne anfangen. (Ob irgendwann einmal durch völlige neue Technologien, etwa »Quantencomputer«, alle bisherigen Verschlüsselungen hinfällig werden, soll momentan nicht unser Thema sein.)

Nun gibt es zwar Programme, die via Zufallsgeneratoren sehr lange Passwortketten erzeugen und in Eingabefelder kopieren können. So vertrauenswürdig diese kryptischen Zeichenketten aussehen – Sie werden sich diese nicht merken können und machen sich damit abhängig von diesen Tools.

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

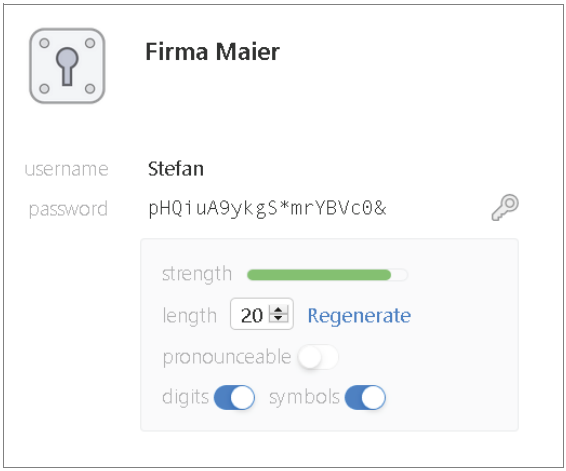

Abb. 13.1: 1Password-Generator: schwer zu merken

Es gibt eine Reihe von Internet-Angeboten, die die Sicherheit Ihres Passwortes einschätzen, indem eine Reihe von Simulationen üblicher Hacker-Verfahren durchgeführt wird. (Bei dieser Berechnung werden nach Angaben der Betreiber in der Regel zwar keine Passwörter übertragen, dennoch sollte man sicherheitshalber nicht das »echte«, sondern ein ähnlich aufgebautes Passwort benutzen.)

Hier einmal die Ergebnisse des Angebots http://www.wiesicheristmeinpasswort.de/.

Abb. 13.2: Leicht zu knacken

»Schmidtchen« benötigt praktisch keine Zeit zum Entschlüsseln. Für »Schmidt!,chen« müssten hingegen 25 Stunden aufgewendet werden, aber auch das wäre noch deutlich zu einfach.

Mit »hDbEk,wDsZd!« kommen wir hingegen in einen Bereich von einigen Jahrhunderten Rechenzeit.

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

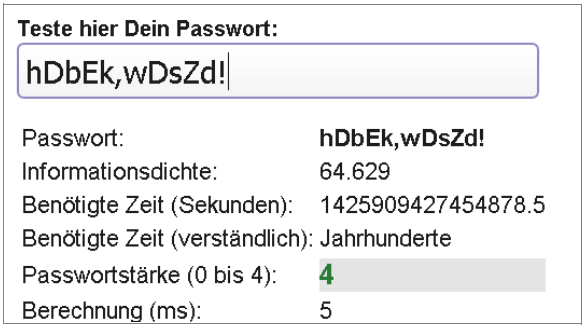

Abb. 13.3: Einige Jahrhunderte für die Entschlüsselung

Wahrscheinlich haben Sie schon von der Empfehlung gehört, von einem Merksatz, zum Beispiel einer Liedzeile, jeweils den ersten Buchstaben der darin vorkommenden Wörter zu verwenden. Nehmen wir als Beispiel den Satz »Hat das Blümchen einen Knick, war der Schmetterling zu dick!«

Daraus könnte man sich im einfachsten Fall aus den Anfangsbuchstaben das Kunstwort zimmern: Hdbek,wdszd! und läge mit zwölf Stellen sogar über der 8-Stellen-Empfehlung des »Bundesamts für Sicherheit in der Informationstechnik« (https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html).

Damit gerade auf mobilen Geräten nicht gar zu umständlich getippt werden muss, wird zunächst etwas gekürzt: Als »Stamm-Passwort« nur die erste Hälfte des Merksatzes »Hat das Blümchen einen Knick,« genommen. Damit erhält man für die erste Passworthälfte »Hdbek,«.

Dieser Stamm wird nun um ein Muster erweitert, das man sich gut merken kann und das sich von Konto zu Konto unterscheidet. Sollte also doch einmal ein Passwort in die falschen Hände geraten, so ist dieses für die anderen Konten nutzlos. Man kann zum Beispiel den ersten und letzten Buchstaben des jeweiligen Web-Angebots zur Unterscheidung nehmen.

Für »A mazo n« also beispielsweise »Hdbek,_An4«,

für »P aypa l« entsprechend »Hdbek,_Pl4« und

für »D ropbo x« »Hdbek,_Dx4«

Damit lässt sich sowohl das Stammpasswort als auch die jeweilige Ergänzung gut merken. Da manche Dienste die Verwendung einer Ziffer fordern, ist diese auch dabei.

Wenn Sie schließlich mit Ihrem neuen Muster zufrieden sind, sollten Sie Ihre bereits bestehenden/älteren Accounts mit dem neuen Passwort versehen – zumindest jene, die Sie häufig nutzen.

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

Viele Dienste – Google, Apple, Dropbox, Evernote und so weiter – bieten Ihnen auch ein Zwei-Wege-Verfahren der Autorisierung an, sodass Sie neben dem Passwort bei Anmeldevorgängen eine Einmal-PIN eingeben müssen, die Sie über den SMS-Weg erhalten. Diesen zusätzlichen Schutz sollten Sie nutzen, auch wenn kein System perfekt ist.

13.2 Verwenden Sie einen Passwortsafe

Mit einem »merkbaren« und komplexen Passwort, das sich zudem je nach Account ändert, ist schon mal ein wichtiger Schritt getan. Allerdings trifft man je nach Angebot auf weitere Hürden: Das Elster-Angebot des Finanzamts benötigt eine Zertifizierungsdatei, bei manchen Angeboten wird mal als Account-Name die E-Mail-Adresse verwendet, mal ein Nutzername und so weiter. Und wenn man einzelne Accounts nur selten nutzt, so vergisst man auch sehr schnell die Einzelheiten, sodass man sich leicht selbst »ausschließt«.

Die Lösung: ein »Tresor«, der all diese Einzelheiten für Sie sicher aufbewahrt.

Das Prinzip von Passwortmanagern ist einfach und funktioniert nach einem ähnlichen Muster: Sie tragen alle Passwörter in eine Datenbank ein, die hoch verschlüsselt ist. Mit einem »Generalschlüssel« öffnen Sie diese Datenbank und können Ihre unterschiedlichen Konto-Daten lesen. Sie müssen sich also nur ein einziges Passwort merken.

Was macht einen guten Passwortmanager aus?

- Das Programm sollte von einem vertrauenswürdigen Anbieter kommen, sprich: Es sollte schon länger auf dem Markt sein und eine große Nutzerbasis haben. Ein Beispiel wäre hier das kanadische Unternehmen AgileBits, das den bekannten Manager 1Password vertreibt (https://agilebits.com/). Bekannt sind auch RoboForm (https://www.roboform.com/de) und LastPass (https://www.lastpass.com/). Bei den Beispielen beziehe ich mich auf KeePass, das kostenlos und Open Source ist – dessen Quellcode also auch von außenstehenden IT-Experten prinzipiell überprüft werden kann (http://keepass.info/).
- Man sollte die Möglichkeit haben, die Datenbank ausschließlich lokal – also auf eigenen Speichermedien – zu verwalten. Sofern der ausgewählte Service über ein Online-Verfahren funktioniert, sollte der Anbieter gewährleisten, dass die Datenbank vor dem Verschicken auf dem eigenen Rechner bereits verschlüsselt ist und die Übertragung selbst natürlich auch über eine abgesicherte Server-Verbindung (erkennbar an `https://` statt `http://`) funktioniert.
- Mancher Anwender möchte eine solche Datenbank nur zu Hause aufbewahren oder zum Beispiel auf einen USB-Stick. Eventuell stellt sich aber nach einiger Zeit heraus, dass man doch gerne auch von unterwegs darauf zugreifen möchte. Für den Fall des Falles – wenn man etwa gerade eine Gedächtnislücke am EC-Automaten hat – sollte also eine verschlüsselte Zugriffsmöglichkeit bestehen (zum Beispiel via App).

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

Bonus-Punkte für einen solchen Manager:

- Außer den »puren« Account-Daten sollten auch Dokumente und Fotos gespeichert werden können.
- Unterschiedliche Datenbanken sollten verwaltet werden können, sodass man in einem »Familien-Tresor« oder »Team-Tresor« Zugangsdaten mit einer Gruppe teilen kann.

Zu den beiden letztgenannten Punkten:

In vielen Fällen sind die Notizfelder, die derartige Passwortmanager ohnehin aufweisen, ausreichend. Aber in bestimmten Situationen ist es sehr nützlich, wenn man zusätzlich ein Dokument aufnehmen kann: Ich habe darin zum Beispiel mein Elster-Zertifikat für den Zugang des Finanzamts verwahrt und meine zusätzlichen Notfall-Codes, falls ich bei einem 2-Faktoren-Zugang einmal keine SMS empfangen kann. Aber auch ein Foto von einem Modem kann sich im Einzelfall als sinnvoll erweisen.

Auch das Teilen einer solchen Datenbank innerhalb der Familie kann eine sehr sinnvolle Sache sein. Erst kürzlich hatte ich im Bekanntenkreis den Fall, dass Familienangehörige in ein Pflegeheim eingewiesen werden mussten, die Kinder aber an unterschiedlichen Orten wohnten. Wenn dann rasch etwas zu regeln ist, Geld für laufende Kosten überwiesen werden muss, sensible Gesundheitsdaten schnell von unterschiedlichen Personen ergänzt oder aktualisiert werden sollen, so kann dies ein Weg sein, um Informationen für alle zu bündeln. Aber auch Passwörter des Heimnetzwerkes, der Garagentür und dergleichen wären Anwendungsmöglichkeiten.

13.2.1 Beispiel Passwort-Safe »KeePass«

KeePass (http://keepass.info/) ist klein, kostenlos und Open Source, existiert schon viele Jahre und wird kontinuierlich weiterentwickelt. Auch wenn das Tool ursprünglich für Windows entwickelt wurde, gibt es sowohl für Mac als auch für Android und iOS Apps, die mit der KeePass-Datenbank umgehen können.

Zunächst vergeben Sie das Hauptpasswort, das Ihnen den Zugang zu allen Schlüsselwörtern ermöglicht (Abbildung 13.4). Dieses Passwort sollten Sie sich besonders gut merken, denn nur durch dieses können Sie Ihre Datenbank öffnen. Falls Sie das Passwort vergessen, gibt es keine Möglichkeit, die Datenbank zu öffnen. Sofern Ihnen das zu »riskant« erscheint, können Sie vom Inhalt der Datenbank auch von Zeit zu Zeit einen Listen-Ausdruck anfertigen und an einem »physisch« sicheren Ort aufbewahren, zum Beispiel einem Bankschließfach.

Im Anlegen einer Ordnerstruktur, Wahl von Icons und Farben sind Sie frei – eine grobe Unterscheidung nach Kategorien ist sicher sinnvoll, oft genügt aber auch die Suchfunktion der Datenbank, die auf Tastendruck die Einträge eingrenzt (Abbildung 13.5).

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

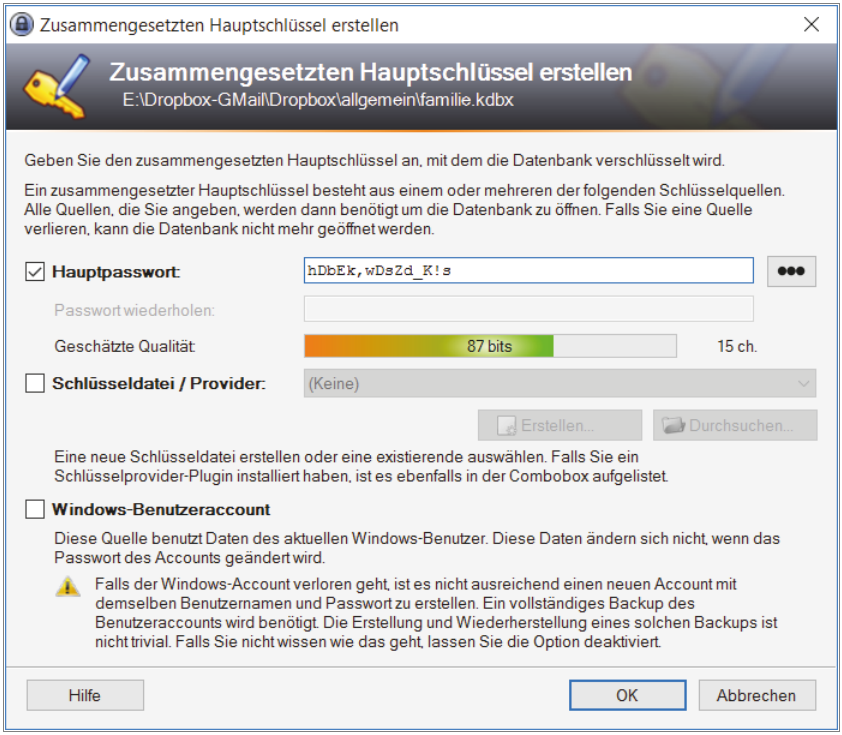

Abb. 13.4: Eingabe Ihres Generalschlüssels für den Safe

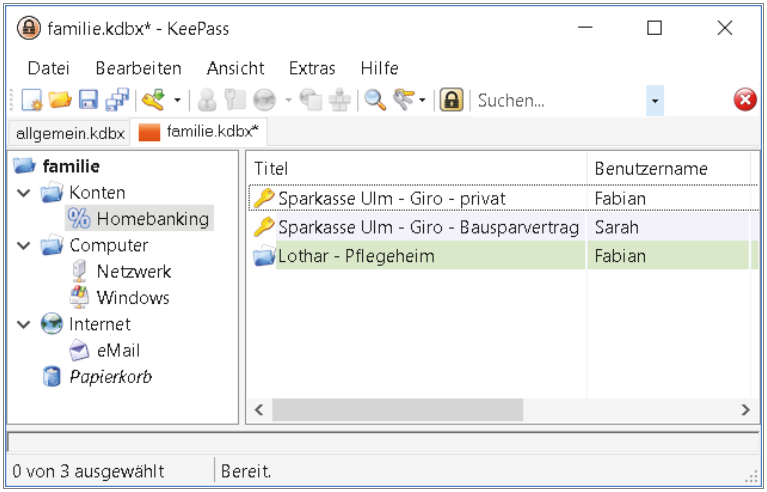

Abb. 13.5: Sie können eigene Kategorien anlegen.

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

Die Basis-Felder eines Eintrags erklären sich von selbst, in den meisten Fällen vergeben Sie einfach einen Titel und tragen Ihre Account-Daten ein. KeePass arbeitet über Erweiterungen auch mit Browsern zusammen und kann später über Shortcuts die Abfragefelder einer Webseite automatisch ausfüllen. Wenn Sie diese Funktionen nützen möchten, so sollten Sie zusätzlich das Feld »URL« ausfüllen.

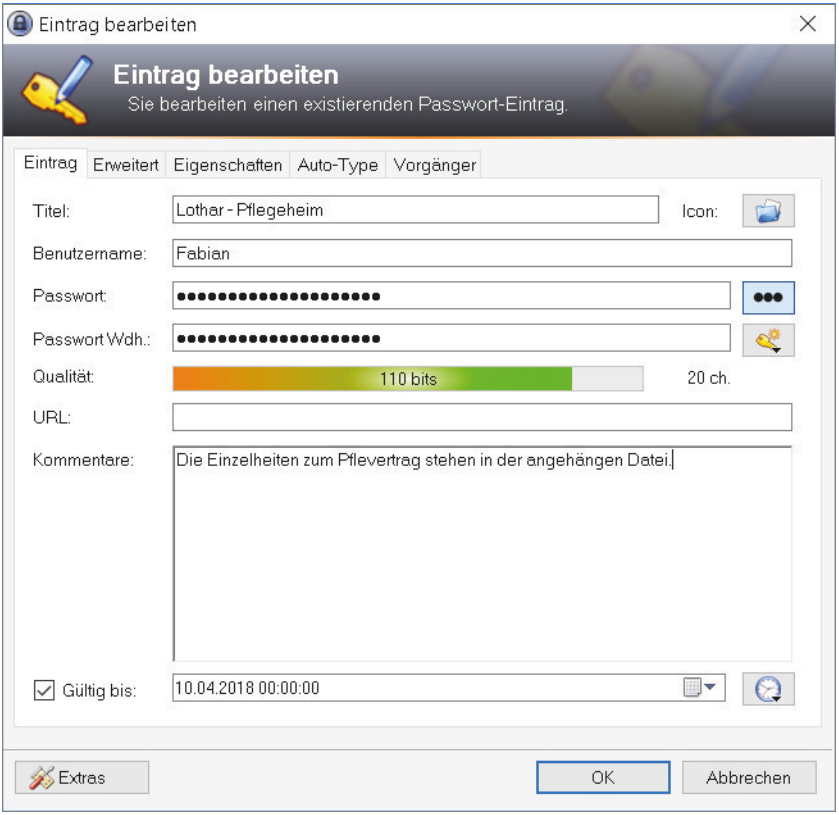

Abb. 13.6: Standardfelder sind rasch ausgefüllt.

KeePass hat weiterhin einen Passwort-Generator integriert, der sehr komplexe Zufallspasswörter erzeugt. Können Sie nutzen, allerdings machen Sie sich dann auch ein wenig von dem Tool abhängig, denn diese Passwörter werden Sie sich nicht merken können. Der Vorteil bei dem eingangs erwähnten Verfahren – ein Stammpasswort mit mnemotechnisch einprägsamen Mustern zu ergänzen – ist, dass Sie in vielen Fällen auch ohne KeePass Ihre Anmeldedaten rekonstruieren können.

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

Wie bereits erwähnt: Dokumente, Fotos und Zertifikate können durch einfaches Drag&Drop hinzugefügt werden. Da die gesamte Datenbank verschlüsselt wird, umfasst die Verschlüsselung auch diese Dokumente.

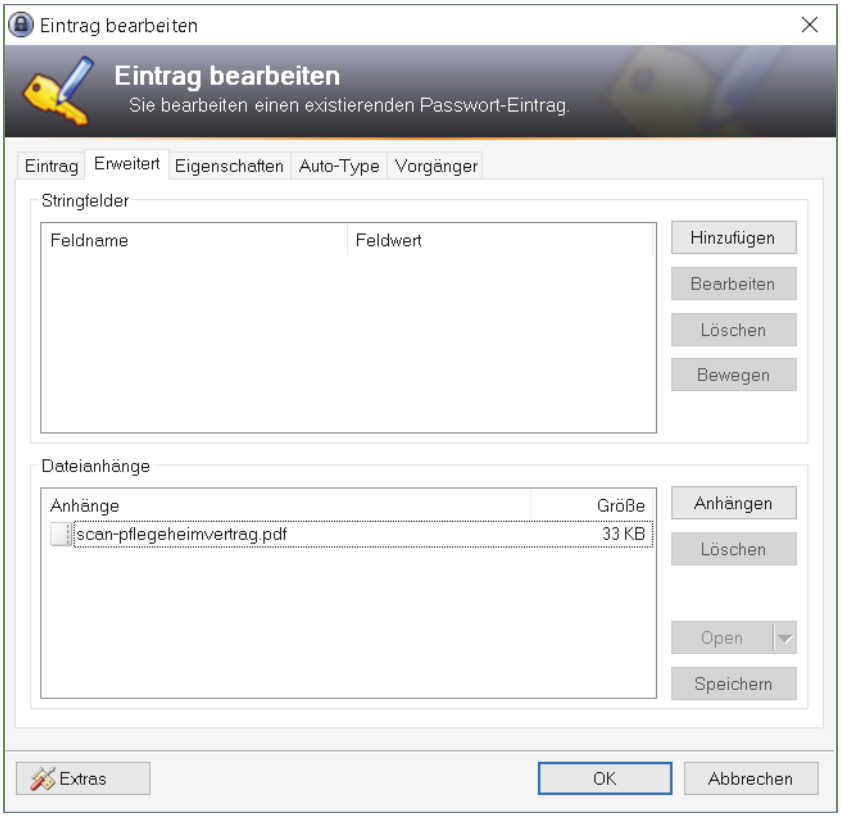

Abb. 13.7: Dokumente in den Tresor aufnehmen

Die Homepage von KeePass führt zahlreiche Browser-Ergänzungen und Varianten für viele Betriebssysteme auf (http://keepass.info/plugins.html). Ich persönlich verwende auf dem Mac KeePassX (https://www.keepassx.org/) und auf dem iPhone Kypass (https://www.kyuran.be/software/kypass/), da diese App auch mit meinem Fingerabdruck umgehen kann. Unter Android klappt dies auch mit Keepass2Android (https://keepass2android.codeplex.com/).

Der Austausch der Datenbank kann beispielsweise über Dropbox erfolgen (die Datenbank bleibt ja verschlüsselt), Sie können die Datenbank aber auch »per Hand« via USB-Kabel übertragen. Zudem kann KeePass auch auf Speichermedien zugreifen, die in Ihrem Netzwerk eingebunden sind.

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

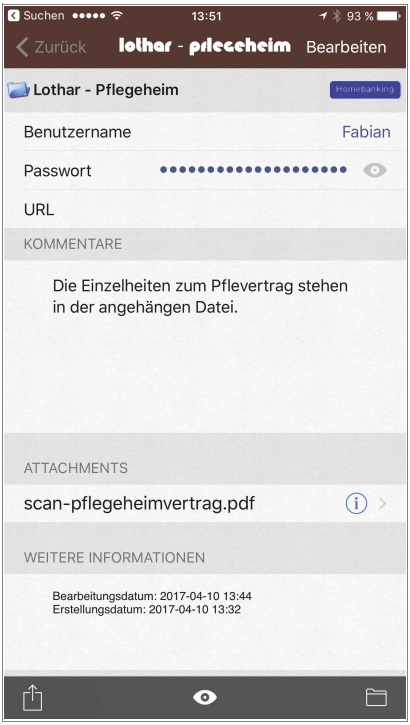

Abb. 13.8: Darstellung der Datenbank in KyPass (iPhone)

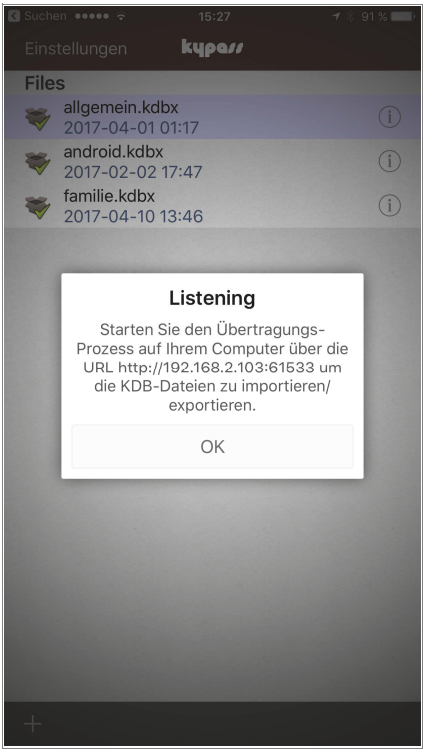

Abb. 13.9: Synchronisierung im eigenen Netzwerk

13.3 Dateien und Ordner verschlüsseln – einfach, sicher und für alle Systeme geeignet

Heute hat man unzählige Möglichkeiten, Informationen zu verschlüsseln. Viele davon haben Betriebssysteme oder Softwareprogramme mehr oder weniger gut integriert: Auf dem Desktop-PC und Mac können Sie ganze Festplatten verschlüsseln, Word oder Acrobat lassen Sie einzelne Office-Dokumente sperren, für USB-Sticks und externe Festplatten gibt es Lösungen wie beispielsweise VeraCrypt (https://de.wikipedia.org/wiki/VeraCrypt) .Dazu kommen jede Menge Freeware-Tools und kommerzielle Angebote für Spezialfälle, etwa das Verschlüsseln in Cloud-Diensten. Für den Laien ist nur schwer abzuschätzen, wie sicher ein Verfahren ist oder ob Tools untereinander kompatibel sind. Und: Wie hoch ist die »Lebenserwartung« derartiger Tools und Verfahren? Windows ändert schon mal ganz gerne von einer Version zur anderen etwas. Oder nehmen wir das bis vor einigen Jahren sehr beliebte Werkzeug TrueCrypt (https://de.

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

wikipedia.org/wiki/TrueCrypt). (Zu einer Zeit, als ich noch mit einer externen USB-Festplatte in der Aktentasche zwischen Homeoffice und Büro pendelte, hatte ich immer sensible Daten in einem TrueCrypt-Container abgelegt.) Die Entwickler stellten 2014 »über Nacht« ihre Arbeit ein und ließen weltweit einige Millionen Anwender irritiert zurück.

Oft ist auch kein problemloser Austausch über unterschiedliche Betriebssysteme hinweg beim Einsatz von Verschlüsselungstools gegeben – und ausgesprochen selten ist das Verfahren derart universell ausgelegt, dass es zudem noch auf den mobilen Plattformen funktioniert. Und dennoch: Es gibt ein sehr einfaches Verfahren, das »überall« funktioniert, auf das ich gleich komme. Im Fokus soll hier aber nicht die Frage der Verschlüsselung ganzer Festplatten oder gar von Netzwerk-Medien stehen (zur Frage, wie man ein verschlüsseltes Backup aller seiner Daten erzeugt, siehe Abschnitt 12.5). Viel häufiger tritt in der Praxis der Fall auf, dass man einen bestimmten Bereich seines Archivs verschlüsseln möchte.

Ein Mini-Tresor für alle Fälle: spezialisierte ZIP-Werkzeuge

Nehmen wir an, Sie haben gerade einen Vertrag abgeschlossen und neben den üblichen Projektunterlagen gibt es auch einen Bereich mit internen Absprachen oder Kalkulationen, der möglichst geschützt aufbewahrt oder weitergegeben werden soll. Dabei muss man gar nicht an große »Hacker-Angriffe« aus fernen Ländern denken, oft sind es Fehler von Benutzern, die zum Beispiel unabsichtlich eine sensible Datei an eine E-Mail hängen oder in einen Cloud-Dienst übertragen.

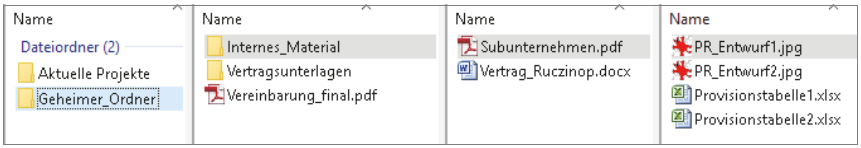

Abb. 13.10: Verzeichnisse und Dokumente schützen

Um solch »Geheime Ordner« zu schützen, gibt es – wie erwähnt – viele Möglichkeiten. Aber wozu ein neues Werkzeug einführen, wenn ein Tool, um das es bereits ging, eine ganz ausgezeichnete Verschlüsselungsmöglichkeit bietet? In Kapitel 13 hatten Sie ja gesehen, dass man Verzeichnisse samt Unterverzeichnissen in ZIP-Archive packen kann. Derartige ZIP-Archive können auf allen Systemen ver- und entschlüsselt werden. Wie das geschieht, dazu gleich mehr, zunächst aber ein wichtiger Hinweis: **Die Art der Verschlüsselung ist bei ZIP-Archiven besonders wichtig!** Denn oft ist nur jene Standard-Verschlüsselung aus früheren Jahren in den Tools eingebaut, die heute nicht mehr als sicher gilt (so zum Beispiel bei der Windows-eigenen ZIP-Verschlüsselung). Zum Glück gibt es eine Reihe von ZIP-Tools, die Standards beherrschen, die auch von Experten als »sehr sicher« klassifiziert werden. Ein solcher Standard – AES-256 – wird von den bereits erwähnten Windows-Tools 7-Zip (http://www.7-zip.de/) beziehungsweise Bandizip (https://www.bandisoft.com/bandizip/de/) beherrscht. Entsprechungen auf der Mac-Seite wären etwa Keka (https://itunes.apple.com/app/keka/id470158793) oder

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

Bandizip X (https://itunes.apple.com/us/app/bandizip-x/id492835684?&ls=1&mt=12), für jeweils rund zwei Euro zu haben.

Verzeichnisse einschließlich Unterverzeichnisse oder ausgewählte Dateien können via Drag&Drop in das Archiv gezogen werden. Die Kriterien für ein sicheres Passwort habe ich ja bereits am Anfang des Kapitels beschrieben.

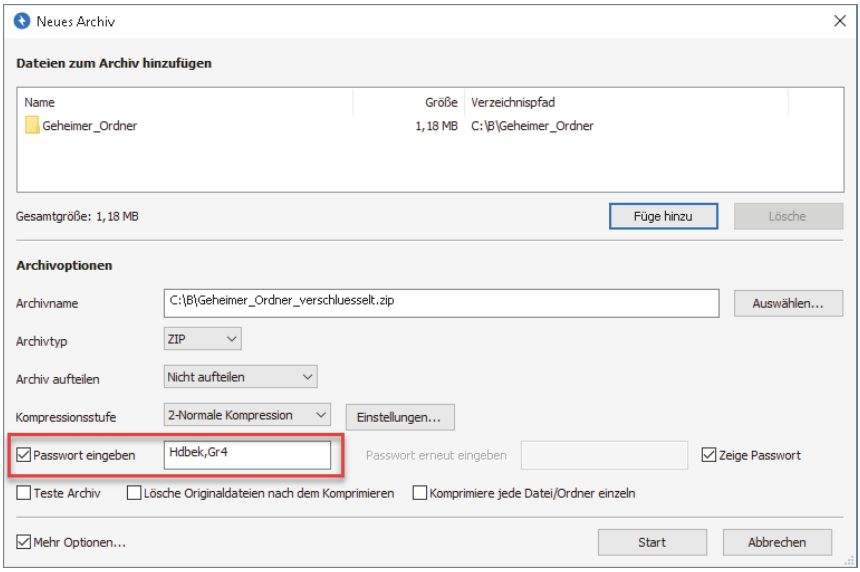

Abb. 13.11: Ein Archiv wird mit Passwort verschlüsselt.

In den Einstellungen darauf achten, dass die erwähnte hohe Verschlüsselung angekreuzt ist.

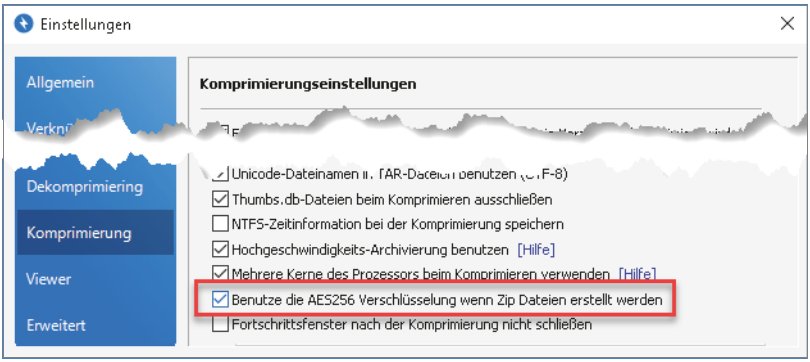

Abb. 13.12: Ein Häkchen genügt.

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

Ebenfalls ist einstellbar, ob die Originaldateien direkt nach dem Packvorgang gelöscht werden sollen. Das so entstandene Archiv können Sie auf Ihren externen Medien speichern, in beliebigen Cloud-Diensten oder auch per E-Mail versenden. Ja, Sie können es auch jederzeit unterwegs einsehen, denn sowohl für Android als auch für iOS gibt es Apps, die mit diesem Format umgehen können.

Abb. 13.13: WinZip für iOS entschlüsselt die Inhalte.

Dabei ist es in der Regel gleichgültig, ob Sie das ZIP-Archiv in bekannten Diensten wie Dropbox, Google Drive oder OneDrive speichern oder via Netzlaufwerk, OwnCloud, WebDav und Ähnlichen die Datei an die App übergeben. Oft beherrschen die Apps neben der Entschlüsselung auch die Verschlüsselung mit dem gleichen hohen Sicherheitsgrad, sodass Sie auch mobil Aktualisierungen vornehmen können. Ein Beispiel für solche Apps ist WinZIP, das es sowohl für iOS gibt (https://itunes.apple.com/de/app/winzip-1-tool-zum-zip-unzip/id500637987?mt=8, circa sechs Euro) als auch für Android (https://play.google.com/store/apps/details?id=com.winzip.android&hl=de, circa zwei Euro). Unter Android beherrschen aber auch eine Reihe von Dateimanagern das Entpacken derartiger Archive.

Übrigens: Sie werden feststellen, dass bei den erwähnten Tools die Dateinamen innerhalb des Archivs einsehbar bleiben (der Inhalt der Datei natürlich nicht). Mir persönlich ist das ganz lieb, denn so kann ich weiterhin nach Dateien suchen lassen, auch wenn diese sich in einem solchen Archiv befinden. Falls Sie die Dateinamen ebenfalls lieber unkenntlich hätten, so gibt es zwei einfache Möglichkeiten: Entweder Sie packen das Archiv in ein weiteres verschlüsseltes Archiv, das dann eben nur diese eine Datei enthält, die damit nicht mehr einsehbar ist. Oder Sie verwenden ein Tool wie etwa WinRAR (https://www.winrar.de/), das die Dateinamen zusätzlich verschlüsselt – dann sollten Sie allerdings testen, ob diese von den von Ihnen verwendeten Plattformen auch erkannt werden.

Auch in diesem Bereich gilt, ähnlich wie bereits bei den Backup-Verfahren ausgeführt: Es mag noch bessere Möglichkeiten geben, um alle möglichen Eventualitäten von Gefährdungen in den Griff zu bekommen – aber das beschriebene Vorgehen ist sehr

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

einfach, erfordert keine Lernkurve und funktioniert auf allen Systemen mit einem recht hohen Sicherheitsgrad. Damit steigt die Chance, dass man es auch wirklich im Alltag verwendet, womit schon sehr viel gewonnen ist.

Cryptomator: Der Zwei-Türen-Tresor für jede Cloud

Wenn man Cloud-Dienste nicht nur als zusätzliche Archive, sondern auch bei der täglichen Arbeit einsetzt, so kann es rasch lästig werden, wenn man ständig ver- und entschlüsseln muss. Das ist vergleichbar mit einem Safe im Büro, den man ständig auf- und zuschließen muss, um wichtige Papierordner zu entnehmen, Daten nachzuschlagen, neue Papiere abzuheften und so weiter. Natürlich würde es niemandem einfallen, hier alle zehn Minuten einen 12-stelligen Zahlencode einzugeben. Was aber, wenn der Safe Sie erkennen könnte und die Tür automatisch offen wäre, wenn Sie sich nähern – sobald aber eine andere Person im Raum ist, ohne Codeeingabe fest verschlossen bleibt? So ähnlich kann man sich Programme wie Cryptomator (https://cryptomator.org/de/) oder Boxcryptor (https://www.boxcryptor.com/de/) vorstellen. Ich werde mich hier auf Cryptomator beziehen, da das Tool unter Windows, Mac und Linux plus Android und iOS einsetzbar ist. Zudem ist es kostenlos, gleichgültig, wie viele unterschiedliche Cloud-Dienste man nutzt. Und Open Source noch dazu – was will man mehr?

Die Funktionsweise von Cryptomator ist sehr simpel: Sie legen in Ihren Clouds »Tresore« an. Alles, was Sie in diesen Tresoren aufnehmen, wird noch auf Ihrem Gerät verschlüsselt, bevor es überhaupt zur Cloud geschickt wird. Dabei wird der gleiche hohe Standard eingehalten, den Sie bereits von den beschriebenen ZIP-Tools kennen: AES-256. Weder hat der Cloud-Betreiber einen Schlüssel zu diesen Daten noch kann er sie auf anderem Weg einsehen. Die Tür bleibt also »nach außen« verschlossen. Aber diese Tresore haben noch eine zweite Tür, die sich auf Ihrer Festplatte befindet. Und diese bleibt »offen«, sodass Sie von Ver- und Entschlüsselungsvorgängen – die superschnell im Hintergrund ablaufen – nichts mitbekommen. Sie können also beispielsweise Dateien aus Ihrem Dropbox-Tresor auf Ihrer Festplatte bearbeiten und in den Google-Drive-Tresor schieben, ohne dass Sie bei diesem Hin und Her Passwörter eingeben müssten. So können Sie trotz der Nutzung der Cloud wie gewohnt arbeiten und sind dennoch auf der sicheren Seite.

Da man die Cloud aber auch oft für Daten nimmt, die man an andere weitergeben möchte und die daher unverschlüsselt bleiben müssen, ist es meist sinnvoll, den Tresor nur für einen Teil der Cloud-Daten einzusetzen und die übrigen Daten nicht zu verschlüsseln – so erhalten Sie auch bessere Trefferquoten, wenn Sie die Suchfunktion Ihres Cloud-Dienstes nutzen, der ja verschlüsselte Inhalte nicht in die Suche einbeziehen kann.

Wie sieht das nun praktisch aus? Zunächst installieren Sie von der Homepage die Programmversion, die zu Ihrem Betriebssystem passt, was in wenigen Sekunden erledigt ist. Cloud-Anbieter wie Dropbox und Ähnliche müssen natürlich bereits auf Ihrem System installiert oder im Netzwerk zugänglich sein, damit dort ein Tresor eingerichtet werden kann.

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

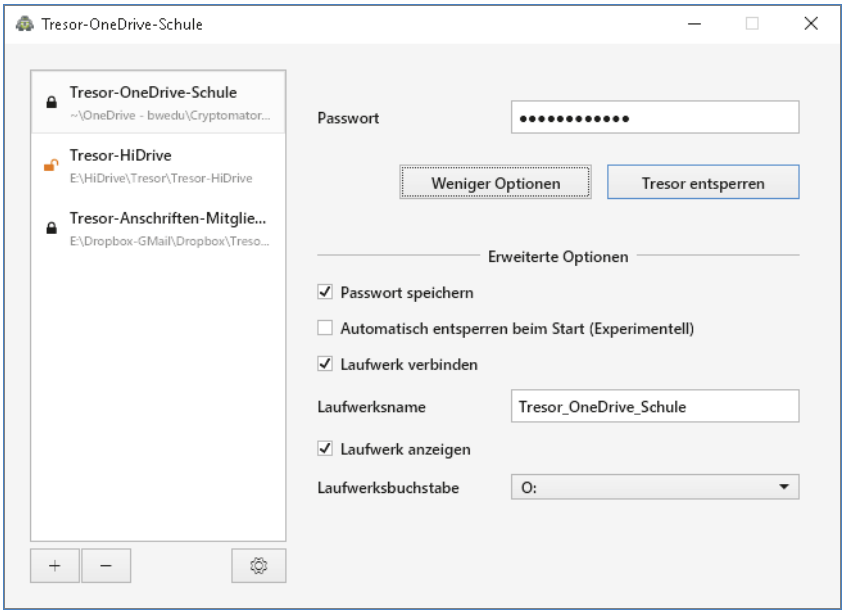

Abb. 13.14: Tresore können in beliebigen Cloud-Diensten angelegt werden.

In Abbildung 13.14 wurde ein Tresor bei Microsoft OneDrive, einer bei Strato-HiDrive und ein Dritter in Dropbox aufgenommen. Dazu müssen Sie lediglich das Plus-Zeichen anklicken und im Dateimanager den Verzeichnis-Ort des gewünschten Dienstes ansteuern.

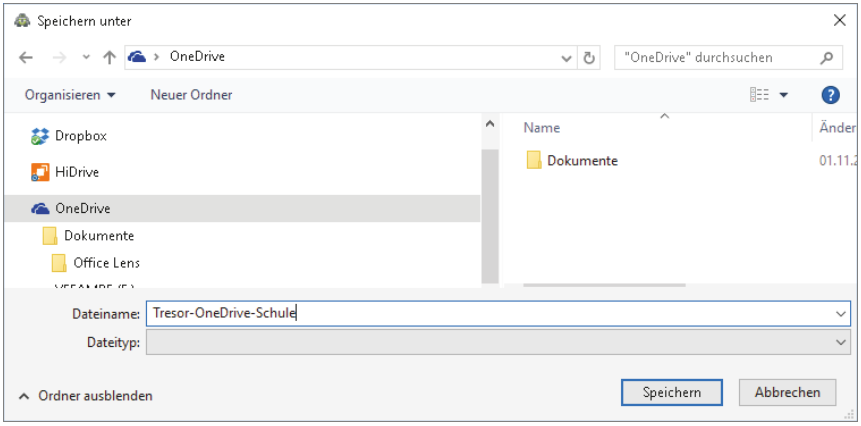

Abb. 13.15: Verzeichnis wählen

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

Sie können beim gleichen Cloud-Dienst mehrere Tresore anlegen. Die Tresore können sich auch in Unterverzeichnissen des Dienstes befinden.

Cryptomator richtet den Tresor automatisch als eigenständiges Laufwerk ein. Sie können die Wahl des Laufwerksbuchstabens dem Tool überlassen oder selbst einen Wunsch-Buchstaben wählen. Da der Name Ihres Tresors eingeblendet wird, sollten Sie problemlos das neue Laufwerk in Ihrem Dateimanager ausfindig machen können.

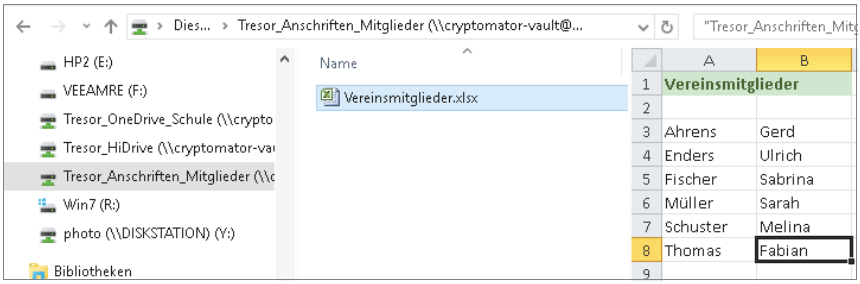

Abb. 13.16: In der Cloud verschlüsselt, auf der eigenen Festplatte einsehbar

Neue zu verschlüsselnde Dokumente ziehen Sie einfach auf dieses Laufwerk. Sie können innerhalb des Tresors auch Verzeichnisse erstellen oder ganze Verzeichnisstrukturen in den Tresor kopieren. Alles bleibt verschlüsselt, auch Dateinamen und Verzeichnisnamen sind für Außenstehende nicht einsehbar. Sie selbst können aber wie gewohnt Dateien einsehen, per Doppelklick öffnen oder bearbeiten.

Wenn Sie eine Datei unverschlüsselt auf Ihrer Festplatte speichern oder per E-Mail verschicken möchten, so müssen Sie nichts tun. In der gleichen Sekunde, in der Sie eine Datei aus dem Tresor ziehen oder an eine E-Mail anhängen, wird sie automatisch von Cryptomator entschlüsselt.

Wenn Sie einen Einzeltresor schließen, Cryptomator beenden oder den PC abschalten, so verschwindet das jeweilige Laufwerk. Sofern Sie Cryptomator nicht so konfiguriert haben, dass das Tool beim Hochfahren des Betriebssystems startet und selbsttätig mit den Passwörtern die Tresore öffnet, so ist von den Tresoren nichts zu sehen.

Sie können von jedem Computer aus, auf dem Sie Cryptomator eingerichtet haben, auf Ihren Tresor per Passwort zugreifen. Falls Sie also Dropbox zu Hause unter Windows verwenden und im Büro den gleichen Dropbox-Account unter Mac, installieren Sie auf beiden Systemen Cryptomator und Sie können von jedem Arbeitsplatz aus den Tresor benutzen. Zu Hause könnten Sie beispielsweise Cryptomator so konfigurieren, dass sofort beim PC-Start alle Tresore sichtbar und geöffnet sind, im Büro bleiben die Tresore zunächst unsichtbar ...

Sehr schön gerade für den Cloud-Bereich: Im Unterschied zu den Container-Modellen, die man bei TrueCrypt/VeraCrypt verwendet, muss man keine Tresorgröße beim Einrichten definieren, die dann kostbaren Cloud-Speicherplatz belegen würde, obwohl der

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.

Tresor/Container noch nicht gefüllt ist. Die Cryptomator-Tresore beanspruchen nur den Speicherplatz, den die darin befindlichen Dateien einnehmen (okay, etwas mehr, da verschlüsselte Dateien grundsätzlich größer als die Ausgangsdateien sind).

Falls Sie auf dem Smartphone oder Tablet einmal eine verschlüsselte Datei einsehen müssen: Cryptomator stellt für Android und iOS Apps zur Verfügung, mit denen Sie Zugriff auf Ihre Tresore erhalten. Es ist also kein Problem, auch mobil ein Dokument aus dem Tresor einer E-Mail anzufügen.

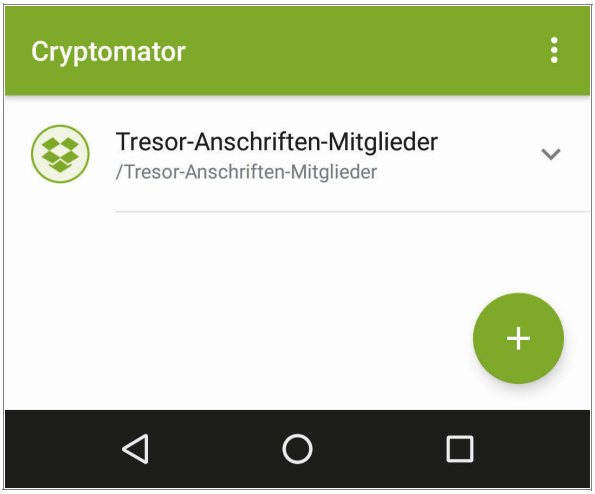

Abb. 13.17: Apps für Android und iOS sind vorhanden.

© des Titels „Digital Cleaning" (ISBN: 978-3-95845-534-4) aus dem mitp-Verlag, Frechen. Nähere Informationen unter www.mitp.de/534.