Inhaltsverzeichnis

1. Internet und Netzwerk 13

1.1 Den Internetzugang zuverlässig absichern 13
Eigene Zugangsdaten verwenden 13
Fernzugriffe und -wartung abschalten 14
Unnötige Wartungsfunktionen abschalten 16
Firmware aktualisieren 17

1.2 Das WLAN gegen Angriffe schützen 18
Eigener Name für das Drahtlosnetzwerk 19
Kennwort und Verschlüsselung optimal wählen 21

1.3 Geräte per Netzwerkkabel anschließen 25
Netzwerkkabel direkt am Internetrouter anschließen 25
Netzwerkkabel – Kabelpaare, Abschirmung und Kategorien 26
Besonderheiten am LAN-1- bzw. WAN-Anschluss 26

1.4 Das lokale Netzwerk erweitern 27
Mehr Anschlüsse und Struktur durch Switches 27
Netzwerklücken per Powerline-Adapter schließen 30

1.5 Wichtige Anwendungen priorisieren 33
Weitere Anwendungen zum Priorisieren ergänzen 35

1.6 VPN-Verbindung zur Firma einrichten 36
VPN-Verbindung in Windows verwenden 37
VPN-Verbindung im Internetrouter einrichten 40

1.7 Per Remotedesktop mit der Firma verbinden 42

2. Windows im Homeoffice optimal nutzen 45

2.1 Den Zugang zum PC absichern 45
Die Anmeldevarianten bei Windows 10 45
Datenschutzlücken auf dem Sperrbildschirm schließen 49

2.2 Ein eigenes Benutzerkonto fürs Homeoffice 51
Ein zusätzliches lokales Konto anlegen 51
Zwischen Benutzerkonten wechseln 53

2.3 Dateiversionsverlauf als Rückgängig-Funktion 54
Den Dateiversionsverlauf aktivieren 54
Was und wie oft sichern? 56
Auf Dateien aus dem Dateiversionsverlauf zugreifen 59

2.4 Dokumente mit der Windows-Suche schnell finden ... 62
Die Suchleiste im Windows-Explorer ... 63
Oft gesuchte Dokumente in virtuellen Ordnern jederzeit verfügbar machen ... 65

2.5 Zweiter Monitor für mehr Bildschirmfläche ... 66
Windows für den Multimonitorbetrieb einstellen ... 67
Die Bildschirme optimal anordnen ... 68
Mit mehreren Monitoren optimal arbeiten ... 69
Tastenkürzel für den Multimonitorbetrieb ... 69

2.6 Mehr Arbeitsplatz durch virtuelle Desktops ... 70
Zusätzliche Desktops anlegen ... 70
Zwischen den virtuellen Bildschirmen hin- und herwechseln ... 71
Fenster auf den virtuellen Desktops anordnen ... 72
Virtuelle Desktops schließen ... 74
Tastenkürzel für virtuelle Desktops in der Übersicht ... 74

2.7 Remotezugriff auf den eigenen PC erlauben ... 75
Die Remoteunterstützung aktivieren ... 75
Einladungen zum Remotezugriff erstellen ... 76
Remoteunterstützung gegen unbefugten Zugriff absichern ... 78

2.8 Kompatibilität für proprietäre Firmenanwendungen ... 79
Lassen Sie Programme wie unter älteren Windows-Versionen laufen ... 80

3. Sicherheit und Datenschutz gewährleisten ... 83

3.1 Sichere Passwörter verwenden ... 83
Wie sicher ist mein Passwort? ... 83
So werden Passwörter sicher ... 84
Wie lang sollte ein gutes Passwort sein? ... 85
Sichere Passwörter generieren ... 86
Passwörter schützen ... 88

3.2 Windows-Firewall für Firmenanwendungen konfigurieren ... 89
Sichere Basiskonfiguration der Firewall ... 90
Schalten Sie Anwendungen den Internetzugang frei ... 91
Erweiterte Firewall-Einstellungen für flexiblen Schutz ... 94

3.3 Malware-Infektionen vermeiden ... 100
Verhaltensregeln: Schädlinge vermeiden ... 101
Fremde Speichermedien prüfen ... 101

Vorsicht bei E-Mail-Anhängen ... 102
Datei-Downloads ... 103
Drive-by-Infektionen verhindern ... 105

3.4 Zuverlässiger Schutz mit Antivirensoftware ... 106
Funktioniert mein Virenschutz? ... 106
Den PC mit Windows Defender schützen ... 107

3.5 Webbrowser sicher und ohne Spuren nutzen ... 117
Im InPrivate-Modus ganz anonym surfen ... 118
Mit wechselnden Benutzerprofilen surfen ... 119
Browserdaten löschen ... 121

4. Dateien sicher austauschen und synchronisieren ... 125

4.1 Dateien per USB-Medium synchronisieren ... 125
Den USB-Stick per »Senden an« füllen ... 125
Dateien vom USB-Medium auf den PC übertragen ... 127

4.2 Dokumente als Offlinedateien jederzeit verfügbar ... 128
Dateien als Offlinedateien lokal bereitstellen ... 128
Offlinedateien ohne Verbindung zum Netz nutzen ... 129
Veränderte Dateien mit dem Netzwerk abgleichen ... 132
Konflikte beim Synchronisieren auflösen ... 135
Offlinedateien durch Verschlüsselung schützen ... 137

4.3 Schneller Datenaustausch per Cloud ... 138
OneDrive – direkt in Windows integriert ... 138
OneDrive konfigurieren ... 139
OneDrive als lokales Laufwerk nutzen ... 140
Dateien zwischen Geräten synchronisieren ... 141
Cloud-Speicher mit Boxcryptor sicher nutzen ... 143

4.4 NAS als zuverlässiger Zwischenspeicher ... 148
Das NAS als persönliche Cloud einrichten ... 148
Qsync auf dem PC nutzen ... 149
Dateien synchronisieren ... 152
Qsync auf Mobilgeräten nutzen ... 153
Dateien auf dem NAS für andere freigeben ... 157

5. Sensible Daten sichern und verschlüsseln 161

5.1 Dateien systematisch sichern und wiederherstellen 161
Vorab: Wohin mit den Sicherungsdaten? 161
Regelmäßige automatische Sicherungen konfigurieren 162
Nach Datenverlusten Dateien aus Sicherungen zurückspielen 167

5.2 Daten auf einem NAS sichern 170
Synology Cloud Station Backup 170
Sicherungsaufträge einrichten 171
Auf gesicherte Dateien zugreifen 173
Frühere Dateiversionen wiederherstellen 174

5.3 Wichtige Dokumente verschlüsseln 175
Dateien und Ordner per EFS verschlüsseln 176
EFS-Zertifikate sichern, um Datenverluste zu vermeiden 177
Gesicherte Zertifikate wiederherstellen 179

5.4 Mobile Geräte komplett verschlüsseln 180
So schützt BitLocker Ihre Daten 180
Ein Laufwerk mit BitLocker verschlüsseln 181
Windows von einem verschlüsselten Laufwerk starten 184
Die Verschlüsselung eines Laufwerks wieder aufheben 185

5.5 USB-Sticks und -Laufwerke verschlüsseln 186
Speichermedien durch Verschlüsselung schützen 186
BitLocker-geschützte Speichermedien nutzen 189
Den BitLocker-Schutz von Speichermedien wieder entfernen 190

6. Gemeinsam arbeiten mit Microsoft Teams 193

6.1 Microsoft Teams: kostenlos anmelden und einrichten 194
App-Version vs. webbasierte Version 197
Schnelle Orientierung in der Teams-Oberfläche 199
Die eigene Verfügbarkeit steuern 200

6.2 Ein Team erstellen und Mitglieder einladen 203
Teams, Kanäle und Personen 203

6.3 Kanäle anlegen und verwalten 209
Neue Kanäle erstellen 209

6.4 Dateien mit anderen austauschen 211

7. Kommunikation mit Kollegen und Kunden 215

7.1 WhatsApp und Co. zur schnellen Kommunikation 215
Den Messenger per Webbrowser am PC nutzen 216
Gruppen erstellen 217
Diskussionsgruppen vorübergehend ruhigstellen 218
Dateien per Messenger teilen 219

7.2 Chats mit Kollegen in Microsoft Teams 220
Chats in separaten Fenstern führen 222
Zustelloptionen bei Chats 223
Den eigenen Bildschirm im Chat freigeben 224
Chats nach Bedarf steuern 225

7.3 Beiträge in Teams-Kanälen veröffentlichen 225
Beiträge beantworten 226

7.4 Hardware für Audio- und Videoanrufe 228
Headset für Audio 228
Kamera für Videokonferenzen 229
Die richtigen Geräte zur Verwendung auswählen 230

7.5 Mit Zoom an Videokonferenzen teilnehmen 231

7.6 Videoanrufe und -besprechungen in Teams 233
Audio- und Videokonferenzen in Kanälen 235

7.7 Dokumente gemeinsam bearbeiten 236
Neue Dokumente erstellen 236
In Echtzeit gemeinsam arbeiten 237
Änderungen und Kommentare verfolgen 238

8. Ergonomie und Selbstorganisation 241

8.1 Im Homeoffice effektiv arbeiten 241
Raum und Zeit zum Arbeiten schaffen 241
Schreibtisch, Stuhl und Bildschirm optimal wählen 242
Durch richtige Pausen mehr schaffen 244

8.2 Aufgabenlisten für Struktur und Erfolgskontrolle 245
Projekte erstellen 245
Aufgabe erstellen 246

Teilaufgaben erstellen 247
Aufgaben erledigen 248

8.3 Die eigenen Aktivitäten erfassen und analysieren 249
Arbeitszeit mit WorkingHours erfassen 249

Stichwortverzeichnis 253

3. Sicherheit und Datenschutz gewährleisten

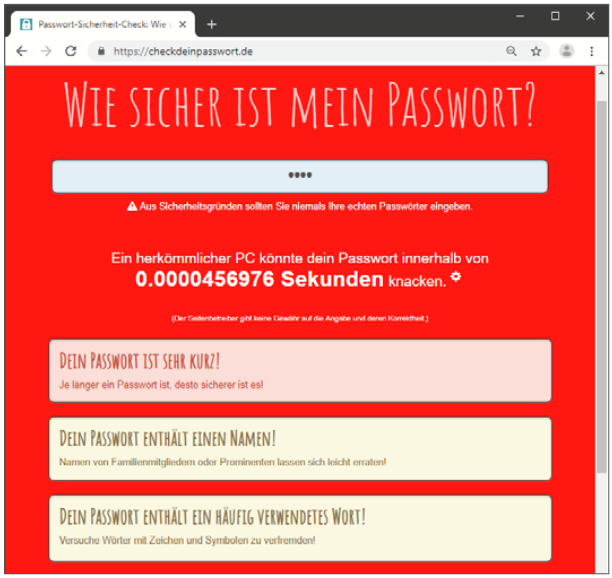
Sicherheit und Datenschutz sollten auch bei der privaten PC-Nutzung immer eine wichtige Rolle spielen. Wenn man allerdings im Homeoffice mit Firmendokumenten und Kundendaten hantiert, bekommen diese Aspekte eine noch höhere Bedeutung. Denn wenn dabei etwas schiefläuft, kann die berufliche Existenz auf dem Spiel stehen. Außerdem bestehen in immer mehr Branchen gesetzliche Anforderungen gerade an den Datenschutz.

3.1 Sichere Passwörter verwenden

Passwörter sind zusammen mit Benutzerkennungen Ihre Eintrittskarte zu allem, was mit vertraulichen und geschützten Daten zu tun hat. Das bedeutet zum einen, dass Sie Passwörter tunlichst nicht vergessen sollten, um sich nicht selbst von Daten und Kommunikationsmöglichkeiten auszuschließen. Zum andern heißt es aber auch, dass jeder, der eines Ihrer Passwörter kennt, errät oder anders ermitteln kann, sich an Ihrer Stelle dieser Daten und Zugänge bedienen kann.

Wie sicher ist mein Passwort?

Auf der Webseite checkdeinpasswort.de können Sie Passwörter testen. Tippen Sie dort in das Eingabefeld Ihr Passwort ein.



Es wird in Echtzeit bewertet, sodass sich die Hintergrundfarbe der Seite bei jedem Zeichen dynamisch anpasst. Rot bedeutet »völlig unsicher« und geht mit jedem (guten) weiteren Zeichen allmählich zu Gelb über. Ziel ist es, eine grüne Hintergrundfarbe zu erreichen. Zusätzlich erhalten Sie darunter jeweils eine Erläuterung, was das derzeit eingetippte Passwort unsicher macht. Zur Bewertung verwendet die Webseite eine Liste der häufigsten deutschen Vor- und Nachnamen, eine Liste der häufigsten deutschen Wörter sowie eine Liste der 10.000 weltweit meistgenutzten Passwörter. Findet sich Ihr Passwort oder ein wesentlicher Teil davon in einer dieser Listen, hat es keine Chance, in den »grünen« Bereich zu gelangen.

So werden Passwörter sicher

Effektiver Passwortschutz beginnt mit der Wahl des Passworts. Ein Passwort, das von anderen leicht erraten werden kann, ist so gut wie keins. Viele naheliegende Begriffe lassen sich leicht merken, eignen sich aber überhaupt nicht als Passwort:

- der eigene Name, ebenso wie der von Frau, Freundin, Kindern oder Haustieren,
- Lieblingsfarbe, Lieblingsband, Lieblingsautor, Lieblings...,
- Marke, Typ oder Kennzeichen des eigenen Autos,
- das eigene Geburtsdatum oder das von Verwandten oder Freunden,
- PLZ oder Name des Wohnorts sowie
- alle sonstigen Begriffe, die jedermann wissen oder herausbekommen könnte, der Sie auch nur flüchtig kennt.

Auch bei weniger naheliegenden Begriffen sollten Sie darauf achten, keine Wörter zu benutzen, wie sie z. B. in Lexika oder Wörterbüchern stehen. Genau solche Wortlisten benutzen Hacker, um ein Passwort auf die harte Tour herauszubekommen. Deshalb sollte jedes Passwort Elemente enthalten, die ganz bestimmt nicht in einem Wörterbuch vorkommen. Eine gute Regel ist, in jedem Passwort mindestens eine Zahl und ein Sonderzeichen (etwa , ; . : _ ? ! + - & $ §) an einer willkürlichen Stelle einzubauen.

Der persönliche Satz

Sie suchen nach einem leicht zu merkenden Passwort, das trotzdem sicher ist? Denken Sie sich doch einfach einen sehr persönlichen Satz aus, den Sie sich bestimmt gut merken können. Zum Beispiel: »Mein erstes Haustier war ein Kater namens Felix.« Wenn Sie jetzt jeweils den ersten Buchstaben (oder auch den zweiten, den dritten, den letzten usw.) jedes Wortes nehmen, ergibt sich daraus ein prima Passwort. In diesem Fall wäre es beispielsweise *MeHweKnF*, ein scheinbar völlig sinnloses Wort, das ganz bestimmt in keinem Lexikon auftaucht. Trotzdem hat diese exotische Kombination für Sie einen Sinn und ist deshalb gut zu merken. Vielleicht finden Sie nun noch die Möglichkeit, an einer halbwegs sinnvollen Stelle eine Ziffer und/oder ein Sonderzeichen einzubauen, etwa so: *M1HweK=F*

Wie lang sollte ein gutes Passwort sein?

Die Antwort auf diese Frage scheint nahezuliegen: je länger, desto besser. Tatsächlich ist es aber nicht ganz so einfach. Natürlich hängt die Sicherheit eines Passworts technisch gesehen von seiner Länge ab. Ein Passwort, das aus nur einem Zeichen besteht, kann jedermann durch einfaches Ausprobieren in relativ kurzer Zeit erraten. Mit jedem zusätzlichen Zeichen potenziert sich der dazu nötige Aufwand, sodass ein zehnstelliges Passwort selbst mit technischen Hilfsmitteln kaum zu knacken ist.

Längenbeschränkungen

Manchmal hängt die Länge des Passworts nicht nur von Ihrer Wahl ab. Bei einigen Anwendungen ist eine feste Länge vorgegeben. Ein bekanntes Beispiel sind die vierstelligen PINs von Bankkarten. Ähnlich ist es auch bei anderen PIN-Anwendungen wie z. B. Onlinebanking, wo die Geheimzahlen oder Passwörter teilweise nur zwischen vier und sechs Stellen lang sein dürfen. Diese Beschränkungen liegen meistens in der verwendeten Software begründet, die nur einen begrenzten Speicherplatz für das Verarbeiten der PINs zur Verfügung hat. Ebenso gibt es Mindestlängen bei der Wahl von Passwörtern. Darüber werden Sie meist vor dem ersten Eingeben eines Kennworts informiert. Manchmal erfahren Sie es aber auch erst, wenn Sie ein zu kurzes Passwort gewählt haben und das Programm sich deshalb beschwert. Dann teilt es Ihnen aber mit, wie lang das Passwort denn nun sein muss. Auch wenn es etwas nervig sein mag, erst im x-ten Anlauf ein geeignetes Passwort zu finden, sind Systeme, die die Passwörter der Benutzer auf Sicherheit überprüfen, sehr sinnvoll. Sie helfen den Benutzern, die häufigsten Fehler beim Auswählen sicherer Passwörter zu vermeiden.

Hacker beschränken sich aber nicht auf technische Hilfsmittel. Eine ebenso einfache wie effektive Methode ist es, das Opfer beim Eintippen des Passworts heimlich zu beobachten. Wenn Ihr Passwort nun so lang und kompliziert ist, dass Sie es nur langsam eintippen können und womöglich noch Tippfehler machen und die Eingabe wiederholen müssen, geben Sie einem heimlichen Zuschauer gute Chancen, zumindest Teile des gesuchten Begriffs zu sehen. Wenn er sich den Rest dazu denken kann, ist Ihr Passwort dadurch schon verraten. Achten Sie beim Auswählen des Passworts deshalb darauf, dass es nicht nur sicher, sondern auch schnell und flüssig einzugeben ist.

Wenn Sie auf Nummer sicher gehen wollen und außerdem ein gutes Gedächtnis besitzen, gibt es eine recht einfache Methode, sehr sichere Passwörter zu bilden: Tippen Sie mit geschlossenen Augen ein paar Mal mit verschiedenen Fingern auf die Tastatur. Schauen Sie sich das Ergebnis an und ergänzen Sie es gegebenenfalls mit einigen Zahlen und Sonderzeichen. Wenn Sie es schaffen, sich das Ergebnis einzuprägen, besitzen Sie ein Passwort, das wohl niemand erraten kann.

Sichere Passwörter generieren

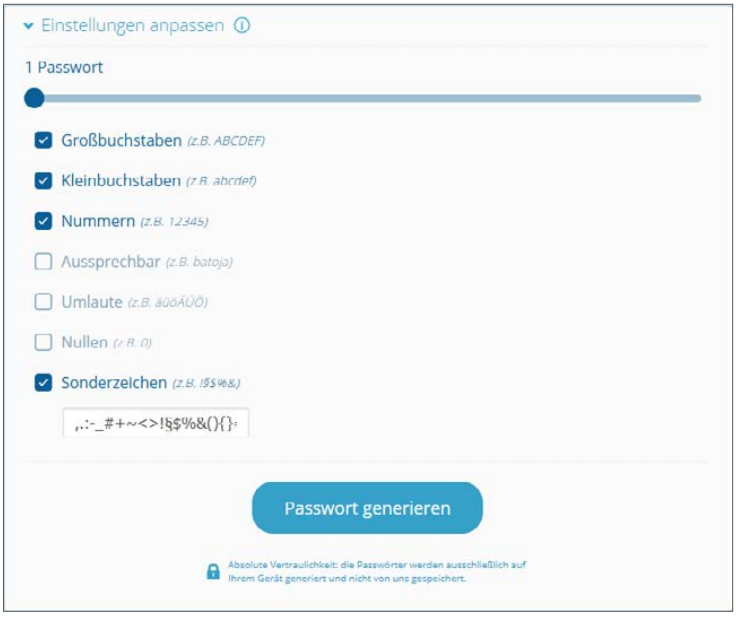
Im Prinzip kann man sich jederzeit selbst ein sicheres Passwort erstellen, indem man willkürlich auf der Tastatur herumhackt und das Ergebnis gegebenenfalls anschließend noch etwas bearbeitet, um den Anforderungen der jeweiligen Anmeldung zu entsprechen.

Denn immer mehr Anbieter machen konkrete Vorgaben, nicht nur zur Länge des Passworts, sondern auch zu obligatorischen Bestandteilen wie Großbuchstaben, Ziffern und Sonderzeichen. Das ist sinnvoll, da Passwörter dadurch wesentlich sicherer werden, macht es aber auch etwas anspruchsvoller, eine entsprechende Zeichenkette zu finden.

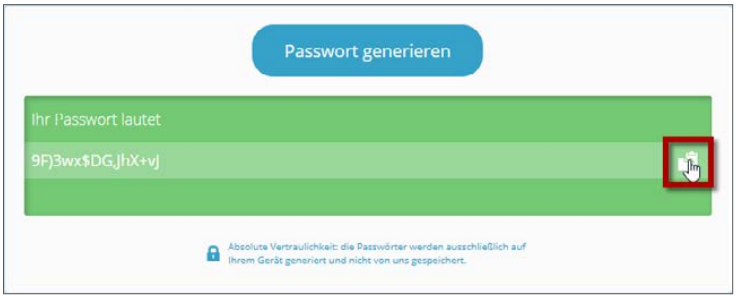
Sie können aber auch einfach einen Online-Passwort-Generator in Anspruch nehmen:

1. Öffnen Sie im Webbrowser beispielsweise die Adresse www.passwort-generator.com.
2. Dort finden Sie direkt oben den Abschnitt *Jetzt sicheres Passwort generieren*.
3. Mit dem Schieberegler wählen Sie die Länge des zu erstellenden Kennworts. Das Formular macht dabei durch die Farbe und die Angabe der zum Knacken benötigten Zeit deutlich, ab wann die Länge als sicher eingeschätzt wird.
4. Macht der Anbieter, bei dem Sie das Passwort verwenden möchten, konkrete Vorgaben zu obligatorischen Bestandteilen, klicken Sie auf *Einstellungen anpassen*.

5. Dadurch klappen Sie zusätzliche Optionen aus. Mit dem blauen Schieberegler können Sie sich beispielsweise gleich mehrere Passwörter erstellen lassen, aus denen Sie dann eines auswählen.
6. Darunter finden Sie Optionen für Groß- und Kleinbuchstaben, Nummern und Sonderzeichen. Haken Sie die Bestandteile an, die der Anbieter fordert.
7. Haben Sie alle Einstellungen wie benötigt vorgenommen, klicken Sie darunter auf *Passwort generieren*.



8. Unterhalb dieser Schaltfläche wird dann das generierte Passwort (oder gegebenenfalls mehrere) angezeigt. Mit einem Klick auf das Symbol rechts daneben fügen Sie die generierte Zeichenkette in die Zwischenablage ein, von wo aus Sie sie direkt in das Anmeldeformular einfügen können.



Aussprechbare Kennwörter

Eine Sonderstellung nimmt die Option *Aussprechbar* ein. Sie lässt sich als Einzige nicht mit anderen Optionen kombinieren und verwendet stets nur Kleinbuchstaben. Damit erzeugt sie silbenbasierte Zufallswörter, die für einen Menschen aussprechbar und somit auch besser zu merken sein sollen. Dafür sind sie aber auch wesentlich leichter zu knacken, was man schnell erkennt, wenn man etwas mit den verschiedenen Optionen experimentiert und den sich dabei ständig verändernden Zeitaufwand für das Knacken im Auge behält. Machen Sie also um die *Aussprechbar*-Option einen großen Bogen.

Passwörter schützen

Auch ein geschickt gewähltes Passwort ist noch lange nicht sicher. Damit es wirklich geheim bleibt, sollten Sie es genauso sensibel wie z. B. die PIN Ihrer Bankkarte oder eine Safe-Kombination behandeln. Dazu gehört, das Passwort nirgends schriftlich zu hinterlassen und es niemand anderem mitzuteilen.

Darüber hinaus gibt es einige besondere Vorsichtsmaßnahmen im Umgang mit Passwörtern:

- Wenn Sie einen neuen Benutzerzugang erhalten, besteht er in der Regel aus einer Benutzerkennung und einem automatisch generierten Passwort. Dieses Passwort wird teilweise nach einfachen Regeln erzeugt. Diese Regeln sind auch Hackern bekannt, die häufig Systeme nach solchen neuen Benutzern durchsuchen. Melden Sie sich deshalb umgehend nach Erhalt der Zugangsdaten an und ändern Sie das Passwort.
- Leichtsinnige Betreiber verzichten teilweise immer noch auf das Verwenden eines Anfangspassworts. Hier ist der Zugang so lange ungeschützt, bis der Benutzer sich das erste Mal anmeldet. Dann wird er automatisch aufgefordert, ein Passwort anzugeben. Auch deshalb ist beim ersten Anmelden für einen neuen Zugang Eile geboten.
- Schreiben Sie ein Passwort nicht auf einen Klebezettel an den Monitor. Auch das Versteck unter der Schreibunterlage ist inzwischen aus diversen James-Bond-Filmen bekannt. Solange Sie nicht als Einsiedler auf einer einsamen Insel wohnen, müssen Sie davon ausgehen, dass andere Personen Zugang zu Ihrem Schreibtisch und Ihrem Rechner haben und sich solche Verstecke zunutze machen. Wenn Sie Ihre Passwörter auf dem Rechner speichern wollen, benutzen Sie dazu ein Programm, das sie verschlüsselt ablegt.
- Geben Sie Ihr Passwort niemand anderem, egal, wie sehr Sie ihm oder ihr vertrauen. Auch wenn diese Person Ihr Passwort nicht missbraucht, kann sie es doch durch eine Unachtsamkeit anderen verraten. Das Passwort zu »verleihen«, heißt immer auch, die Kontrolle darüber aus der Hand zu geben. Auch Mitarbeiter von Onlinediensten, -banken oder -shops fragen Kunden **niemals** nach deren Passwörtern. Allerdings ist dieser Trick bei Hackern sehr beliebt.
- Sollte es doch einmal unbedingt notwendig sein, ein Passwort jemand anderem mitzuteilen, dann gehen Sie so vor: Ändern Sie zunächst das aktuelle Passwort in ein anderes. Dieses neue Geheimwort sollte absolut neutral sein und dem anderen keinen Hinweis darauf geben, wie Sie üblicherweise Ihr Passwort gestalten. Teilen Sie das neue Passwort mit und klären Sie dabei, wie lange der andere den Zugang benutzen wird. Sofort nach Ablauf dieser Zeit melden Sie sich an und wechseln das Passwort erneut. Entweder Sie gehen zu dem alten Passwort zurück oder Sie nutzen die Gelegenheit für einen Wechsel.
- Die wichtigste Regel heißt: Ändern Sie Ihr Passwort regelmäßig, auch wenn es lästig ist. Sie können nie wissen, ob nicht doch jemand Ihr geheimes Erkennungswort bereits ausgespäht oder geknackt hat. Wenn man es bemerkt, ist es meist schon zu spät

und der Schaden ist angerichtet. Wenn Sie aber regelmäßig Ihr Passwort wechseln, geben Sie einem Eindringling möglichst wenig Zeit, mit dem erschlichenen Zugang Unheil anzurichten. Das neue Passwort muss er schließlich erst wieder herausfinden. Wenn ein Hacker Sie ins Visier genommen hat, wird ihn ein regelmäßiger Wechsel des Passworts außerdem abschrecken.

Gefährlich: Passwörter in Anmeldedialogen speichern

Anwendungen mit Onlinefunktionen bieten häufig die Möglichkeit, Zugangsdaten wie Benutzername und Kennwort zu speichern. Das entbindet die Benutzer von der lästigen Pflicht, stets dieselben Eingaben wiederholen zu müssen. Das ist sicherlich sehr bequem, aber alles andere als sicher. Stellen Sie sich vor, Ihr Rechner wird bei einem Einbruch entwendet. Wenn der Einbrecher ohne jegliche Passworteingabe Zugang zu Ihrem Rechner bekommt und dort ungehindert Dokumente und Anwendungen öffnen kann, braucht er nicht mal Hacker zu sein, um auf Ihre Kosten durch das Web zu surfen.

Autovervollständigen im Webbrowser?

Praktisch alle aktuellen Webbrowser verfügen über zahlreiche Komfortfunktionen, die den Benutzern das Surfen möglichst leicht machen sollen. Dazu gehört auch das automatische Vervollständigen von regelmäßig besuchten Anmeldeseiten. Auch hier bedeutet der Komfort einen erheblichen Sicherheitsmangel. Wenn Sie sich beispielsweise ohne Eingabe eines Passworts per Webbrowser Zugang zum Firmen-Intranet verschaffen können, weil der Browser dies automatisch für Sie erledigt, kann das auch jeder andere, der Zugang zu Ihrem Rechner erlangt. Für kritische Kennwörter sollte man deshalb keinesfalls die Autovervollständigung verwenden.

Besser und sicherer ist es, einen Passwort-Manager zu nutzen. Der integriert sich in den Webbrowser und kann ebenfalls Anmeldeformulare ausfüllen. Allerdings erst, wenn Sie zumindest einmal das Masterpasswort des Managers eingetippt haben.

3.2 Windows-Firewall für Firmenanwendungen konfigurieren

Angesichts der Gefahren im Internet ist eine Firewall eine unerlässliche Maßnahme. Sie filtert unerwünschte und potenziell gefährliche Pakete und Anfragen aus dem Datenstrom heraus und verhindert so, dass sie auf den PC gelangen. So werden die Zugänge des PCs vor unerwünschten Gästen geschützt, und auch bösartige Angriffe wie Portscans und Denial-of-Service-Attacken werden abgewehrt. Windows bringt hierfür einen Basisschutz in Form seiner klassischen Windows Defender Firewall mit.

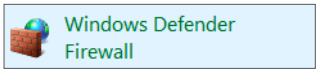
Sichere Basiskonfiguration der Firewall

Die Windows-Firewall kann für jegliche Arten von Internetverbindung verwendet werden. Dabei spielt es keine Rolle, ob es sich um eine Einwählverbindung, einen DSL-Zugang über ein lokales Netzwerk oder auch um ein Drahtlosnetzwerk handelt. Die Firewall-Einstellungen können auf die jeweilige Rechner- und Zugangskonfiguration und das persönliche Sicherheitsbedürfnis abgestimmt werden.

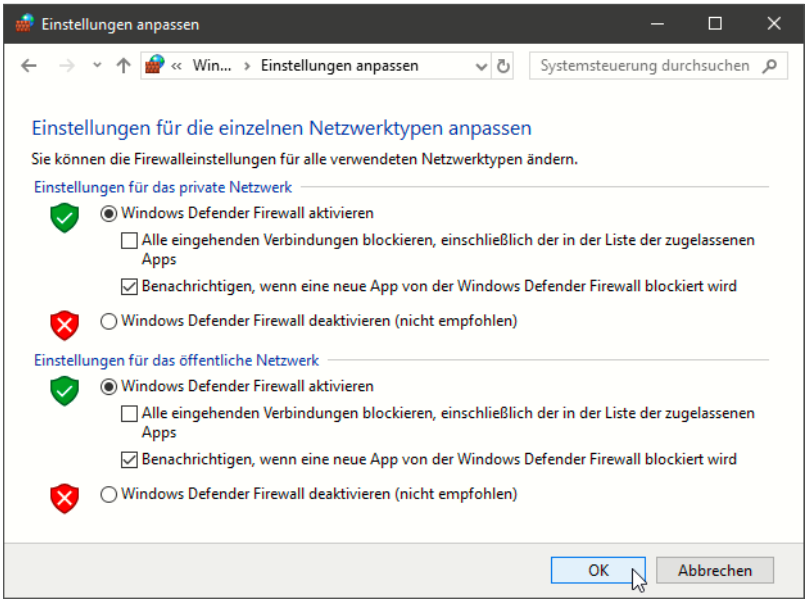
Hierzu unterscheidet die Firewall grundsätzlich zwei Arten von Netzwerken:

- Das sind zum einen **private Netzwerke** zu Hause oder auch an einem Arbeitsplatz, wo der PC mit anderen – prinzipiell vertrauenswürdigen – PCs verbunden ist. Standardmäßig sind hier der Datenaustausch und das Teilen von Ressourcen möglich, und die Firewall-Einstellungen sind weniger restriktiv bzw. lassen problematische Aktivitäten gegebenenfalls nach einer Rückfrage zu.
- **Gast- oder öffentliche Netzwerke** wie z. B. offene WLAN-Hotspots oder Firmennetze, die von vielen Anwendern genutzt werden, behandelt Windows wesentlich restriktiver. Datenaustausch und Ressourcenfreigabe sind hier standardmäßig nicht möglich. Eine vom öffentlichen Netzwerk bereitgestellte Internetverbindung kann selbstverständlich genutzt werden, unterliegt aber einer strengen Kontrolle bezüglich der Art der übertragenen Daten.

1. Um die *Windows Defender Firewall* einzustellen, öffnen Sie zunächst das gleichnamige Modul der klassischen Systemsteuerung.



2. Im anschließenden Menü können Sie nun den aktuellen Status von Netzwerk und Firewall sowie die Grundkonfiguration der Firewall einsehen. Hier zeigt sich die Unterscheidung in private und öffentliche Netzwerke deutlich. Für jeden Bereich ist eine eigene Übersicht vorhanden, und Sie können dieselben – getrennten – Einstellungen für beide Arten von Netzwerken vornehmen.
3. Um die Konfiguration der Firewall zu verändern, klicken Sie links auf *Windows Defender Firewall ein- oder ausschalten*. So öffnen Sie die eigentlichen Firewall-Einstellungen. Auch hier ist alles zweigeteilt, und alle Einstellungen können separat für geschlossene und öffentliche Netze vorgenommen werden:
   - Standardmäßig ist die Schutzfunktion mit *Windows Defender Firewall aktivieren* eingeschaltet und läuft mit Basisregeln, die die üblichen Internetanwendungen zulassen. Nicht angeforderte Datenpakete von anderen Rechnern werden dabei verworfen, wenn diese nicht ausdrücklich als Ausnahmen definiert sind. Somit sind Sie vor Portscans, Trojanern etc. schon recht gut geschützt.
   - Insbesondere für mobile PCs, die hin und wieder an öffentlichen Netzwerken wie z. B. WLANs betrieben werden, ist die Option *Alle eingehenden Verbindungen blockieren, einschließlich der in der Liste der zugelassenen Apps* gedacht. Sie ignoriert auch definierte Ausnahmeregeln und bietet so noch mehr Schutz.



- Die Option *Benachrichtigen, wenn eine neue App von der Windows Defender Firewall blockiert wird* setzt Sie davon in Kenntnis, wenn die Firewall aktiv ins Geschehen eingreift. Das kann sinnvoll sein, da ansonsten Anwendungen mit Internetzugriff nicht funktionieren und Sie nicht erfahren, warum das so ist. Sollten die Meldungen der Firewall nervig sein, können Sie sie aber so unterdrücken.
- Die Firewall mit *Windows Defender Firewall deaktivieren* auszuschalten, empfiehlt sich nur, wenn Sie stattdessen andere mindestens ebenbürtige Schutzmaßnahmen ergreifen.

4. Wenn Sie die geänderten Einstellungen mit *OK* übernehmen, wird die Firewall-Funktion entsprechend Ihrer Auswahl eingestellt. Dies ist ohne Neustart möglich, sodass Sie den Modus auch während des Betriebs jederzeit schnell wechseln können.

Schalten Sie Anwendungen den Internetzugang frei

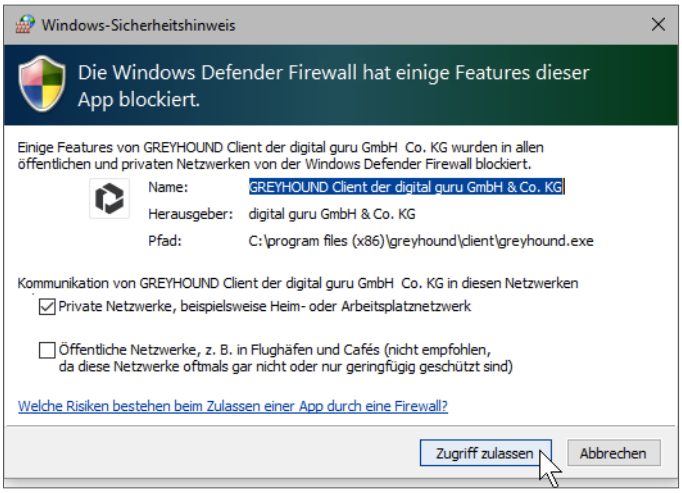
Die Firewall überwacht nicht nur den von außen ankommenden Datenverkehr, sondern achtet auch auf Programme, die vom PC aus Daten ins Internet übertragen wollen. Schließlich könnte es sich dabei ja um Trojaner oder andere schwarze Schafe handeln.

Nimmt eine Anwendung Kontakt mit dem Internet auf, vergleicht die Firewall diese mit ihrer internen Liste und wird aktiv, wenn das Programm dort nicht verzeichnet oder gar gesperrt ist. Das kann freilich auch passieren, wenn Sie selbst eine Anwendung zum ersten Mal starten. Dann müssen Sie Windows beibringen, dieses Programm zu akzeptieren.

Nachricht beim Blockieren von Programmen

Damit das interaktive Freischalten von Anwendungen für den Internetzugriff gelingen kann, muss in den Einstellungen der Windows Defender Firewall die Option *Benachrichtigen, wenn eine neue App von der Windows Defender Firewall blockiert wird* eingeschaltet sein (siehe vorangegangenen Abschnitt).

1. Wenn ein Programm auf das Internet zugreifen möchte, das die Firewall bislang nicht in der internen Liste verzeichnet hat, blockiert sie dessen Zugriff zunächst. Sie erhalten dazu ein Hinweisfenster.



2. Haben Sie dieses Programm selbst aufgerufen und wollen es online nutzen, können Sie zunächst wählen, ob der Zugriff nur in geschlossenen privaten Netzwerken oder auch an öffentlichen Hotspots erlaubt sein soll.
3. Klicken Sie dann unten auf *Zugriff zulassen*.
4. Wurde das Programm versehentlich gestartet oder handelt es sich um ein Programm, das gar keine Internetfunktionen haben sollte, oder haben Sie vielleicht gar kein Programm gestartet, klicken Sie unten rechts auf die Schaltfläche *Abbrechen*. Damit wird dieses Programm auf die rote Liste gesetzt.

Die Zugangserlaubnis für eine Anwendung zurückziehen

Wenn Sie einem Internetprogramm den Zugriff aufs Internet gestattet haben, fragt Windows nicht mehr nach, sondern startet das Programm immer sofort. Das liegt daran, dass die Firewall alle Programme, denen Sie den Zugriff einmal erlaubt haben, in einer Liste speichert, um wiederholte Nachfragen zu vermeiden. Sie können ein Programm aber wieder aus dieser Liste streichen.