Maßnahmen zur Erhöhung der IT-Sicherheit
Version 1.4

datenschutz nord GmbH
Mai 2021

datenschutz nord

Inhaltsverzeichnis

Der Schutz personenbezogener Daten ist eine wesentliche Aufgabe der Verantwortlichen. Neben der rechtlichen Bewertung von Datenverarbeitungsvorgängen muss dieser die Datensicherheit gewährleisten.

Durch den Verantwortlichen sind verschiedene Maßnahmen zu treffen, die der Datensicherheit und dem Datenschutz dienen.

Viele Maßnahmen sind mit einem überschaubaren Aufwand und ohne tiefgreifende Kenntnis von der Informationstechnologie umsetzbar. Hierbei handelt es sich um:

- sichere Passwörter auswählen
- Windows-Festplatte verschlüsseln
- USB Sticks verschlüsseln
- sichere E-Mails versenden
- Daten regelmäßig sichern
- Sperrbildschirm einrichten
- Virenscanner aktivieren
- Firewall einsetzten
- stetig Sicherheitsupdates durchführen
- mit Standardbenutzerkonten arbeiten
- Dokumentenentsorgung beachten
- korrekt am Arbeitsplatz verhalten

Nachfolgend werden die vorgenannten Themen erklärt. Diese sollten zeitnah in der Einrichtung umgesetzt werden.

Bei Fragen oder Problemen nehmen Sie unbedingt Kontakt zu uns auf: kirche@datenschutz-nord.de

Ihr Kirchen-Team

datenschutz nord Gruppe

1. Vorgehen für die Erstellung von sicheren Passwörtern

Um zu verhindern, dass unbefugte Personen beispielsweise Zugang zu einem Rechner erhalten, müssen Passwörter gut gewählt werden. Ist das nicht der Fall, können sie mit einfachen Möglichkeiten schnell „erraten“ oder „geknackt“ werden. Ein sehr beliebter Ansatz dafür ist das strategische Bilden aller möglichen Kombination von Zeichen und schlichtem Ausprobieren, ob das Passwort stimmt. Damit lässt sich theoretisch sogar jedes Passwort „erraten“, wenn man nur genug Zeit mitbringt.

In jedem Fall sollten Passwörter niemals auf Notizzetteln am Arbeitsplatz notiert oder an andere Personen weitergegeben werden. Passwörter sollten mindestens 10 Zeichen lang sein und nicht nur aus Buchstaben oder Zahlen oder Sonderzeichen bestehen. Es müssen keine besonderen Kombinationen daraus genutzt werden, allerdings erhöht die Verwendung verschiedener Zeichensätze die Menge der möglichen Zeichen und damit die Dauer, alle unterschiedlichen Kombinationen dieser Zeichen auszuprobieren. Es sollten ebenfalls persönliche Daten, wie eine Adresse, dem Geburtsdatum oder dem Jahrestag, vermieden werden.

Überlegen Sie sich einen Satz, den Sie mit dem Gerät oder der Aufgabe am Arbeitsrechner assoziieren und sich leicht merken können.;	Beispielsatz: „Ein Kindergarten hat im Juli und August geschlossen“
Bauen sie ein paar Zahlen und/oder Sonderzeichen ein;	Mit Zahlen und Sonderzeichen entsteht nun folgender Satz: „Ein Kindergarten hat die Monate 07-08 geschlossen!“
Verkürzen Sie den Satz durch Verwendung der Anfangsbuchstaben; Achten Sie auf eine Mindestlänge von 10 Zeichen und schon haben Sie sich ein solides Passwort erstellt.	„EKhdM07-08g!“
	Damit erhalten Sie eine Methodik, sich vernünftige Passwörter zu überlegen.

2. Verschlüsselung von Laufwerken und Speichermedien

Die Verschlüsselung einer Festplatte oder eines USB Sticks sorgt dafür, dass beispielsweise im Falle eines Geräteverlustes die Daten weiterhin geschützt sind und ein Zugriff erschwert wird.

Windows 10 Pro bietet dafür den bereits integrierten BitLocker an, mit dem sowohl Betriebssystemlaufwerke (Festplatten mit einem installierten Betriebssystem) als auch externe Speichermedien, wie USB Sticks, verschlüsselt werden können.

Im Falle von **Windows 10 Home** ist eine Verschlüsselung des Systemlaufwerks nicht möglich, da BitLocker in der Home-Variante nicht integriert ist. In diesem Fall kann auf ein externes Programm, wie beispielsweise VeraCrypt, zurückgegriffen werden (siehe Anhang A „Verschlüsselung des gesamten Betriebssystems mit VeraCrypt“).

2.1. Verschlüsselung des gesamten Betriebssystems mit BitLocker

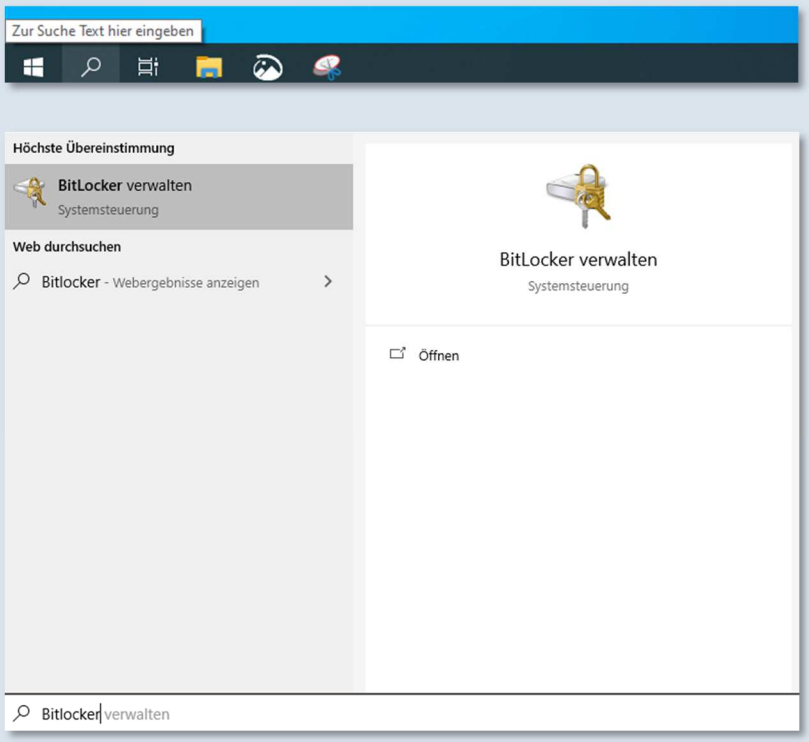
Diese Methode verschlüsselt das gesamte Windowssystem mit samt ihren Dateien, die Sie auf ihrem Arbeitsrechner gespeichert haben. Kurz gesagt, Ihr gesamtes System. Tatsächlich verschlüsselt ist das System jedoch nur im abgeschalteten Zustand. Daher sollte der Arbeitsrechner, wenn er nicht verwendet oder transportiert wird, immer zuvor ordnungsgerecht heruntergefahren werden.

Voraussetzung: Ein separater USB Stick oder ein Drucker, Windows 10 Pro.

2.1.1. Laufwerk verschlüsseln

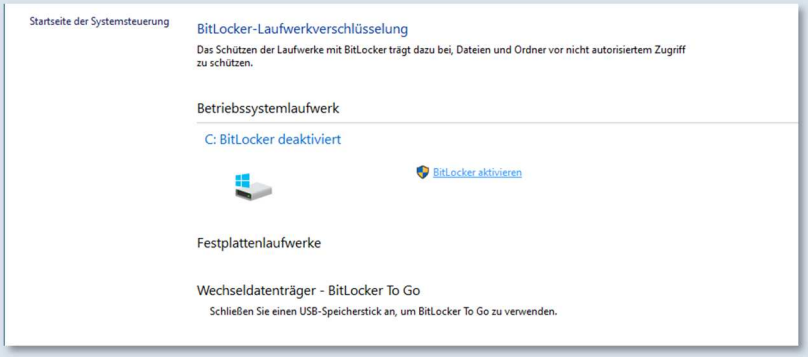
Klicken Sie auf der Taskleiste auf die Lupe, um die Suchfunktion zu starten.

Geben Sie den Begriff „BitLocker“ ein und klicken Sie auf den Eintrag „BitLocker Verwalten“.

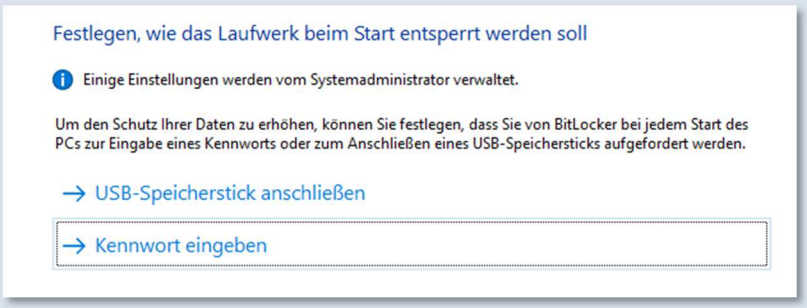


Dieser öffnet die Systemsteuerung mit der BitLocker-Laufwerkverschlüsselung, in der Ihre Betriebssystemlaufwerke aufgelistet werden, die mit BitLocker verschlüsselt werden können.

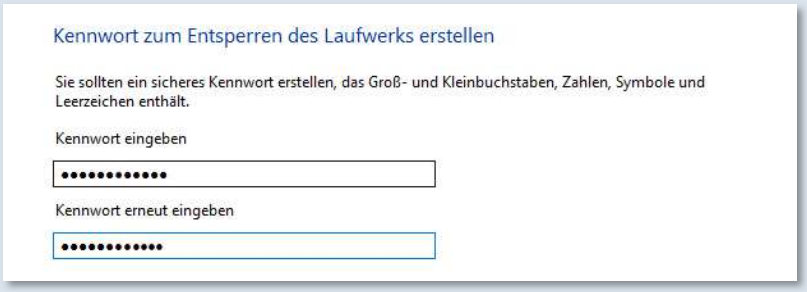
Klicken Sie neben dem gewünschten Laufwerk auf „BitLocker aktivieren“ und richten Sie nun die Verschlüsselung ein.



Bestimmten Sie ein Kennwort zum Entsperren des Laufwerks;

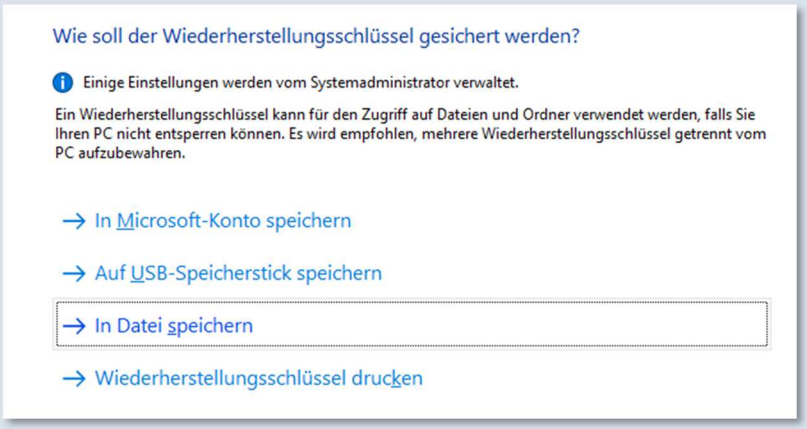


Wählen Sie ein sicheres Kennwort nach den Kriterien, wie sie Ihnen in Kapitel 1 „Vorgehen für die Erstellung von sicheren Passwörtern“ vorgestellt wurden.

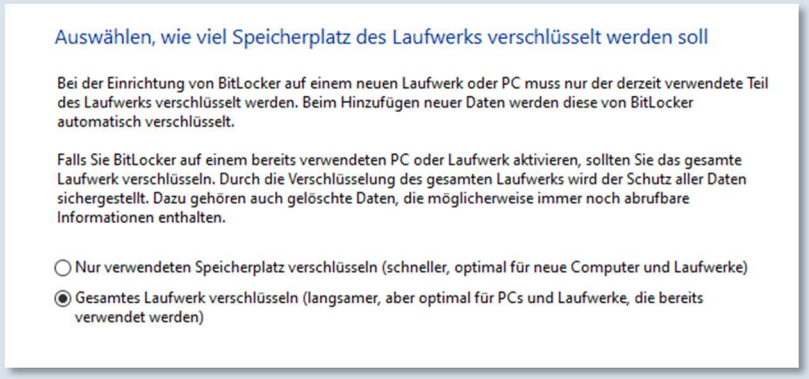


Sichern Sie den Wiederherstellungsschlüssel in einer Datei auf einem USB Stick und verwahren Sie ihn an einem sicheren Ort.

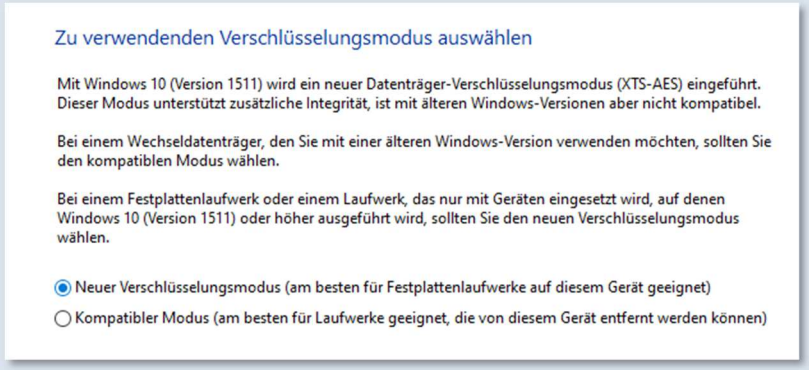
Alternativ können Sie den Wiederherstellungsschlüssel auch ausdrucken und an einem sicheren Ort verwahren.



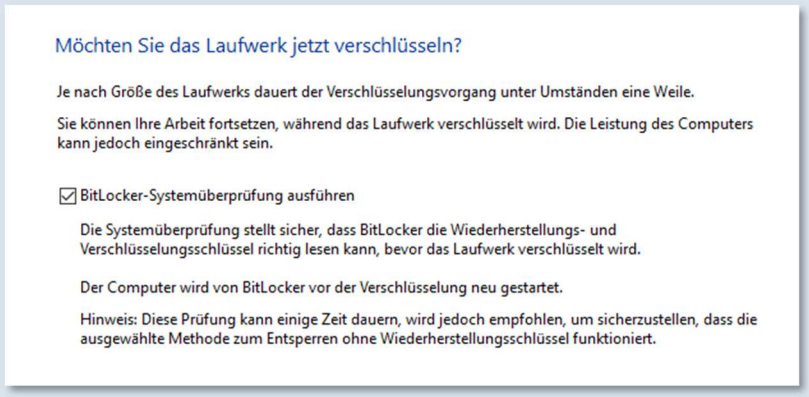
Verschlüsseln Sie das gesamte Laufwerk;



Verwenden Sie für das Festplattenlaufwerk den neuen Verschlüsselungsmodus;



Aktivieren Sie die Ausführung einer BitLocker-Systemüberprüfung und starten Sie die Verschlüsselung, die einige Zeit in Anspruch nehmen kann.



2.1.2. Laufwerk entschlüsseln

Nach dem Einschalten des Arbeitsrechners werden Sie automatisch aufgefordert, das Kennwort zum Entsperren des Laufwerks einzugeben. Erst dann kann das System gestartet werden.

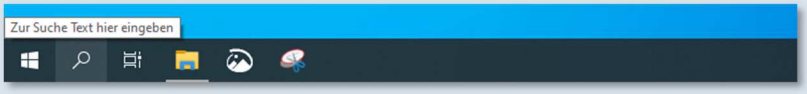
2.2. Verschlüsselung eines USB Sticks unter Windows 10 Pro

Diese Methode verschlüsselt einen mobilen Datenträger. Damit wird sichergestellt, dass der Inhalt eines USB Sticks nur von jenen eingesehen werden kann, die das entsprechende Passwort zum Entsperren kennen.

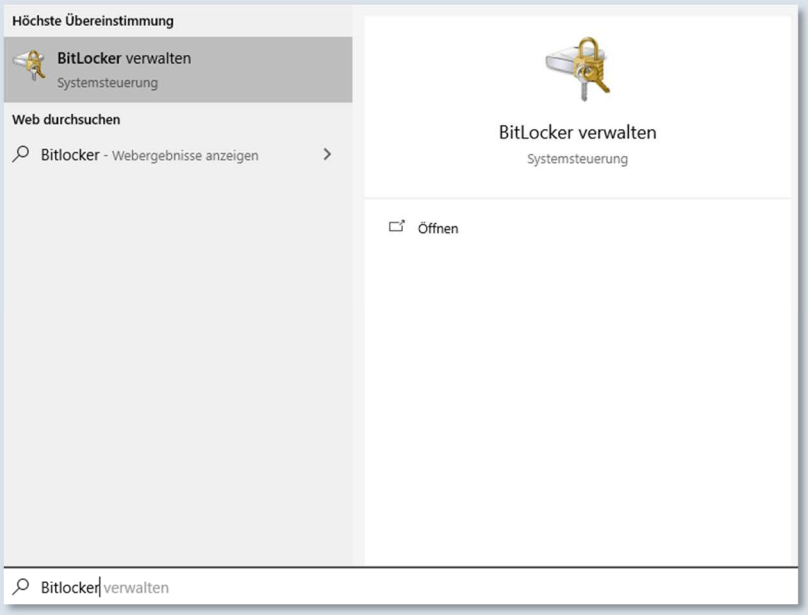
Voraussetzung: Ein separater USB Stick oder ein Drucker.

2.2.1. Laufwerk verschlüsseln

Klicken Sie auf der Taskleiste auf die Lupe, um die Suchfunktion zu starten.

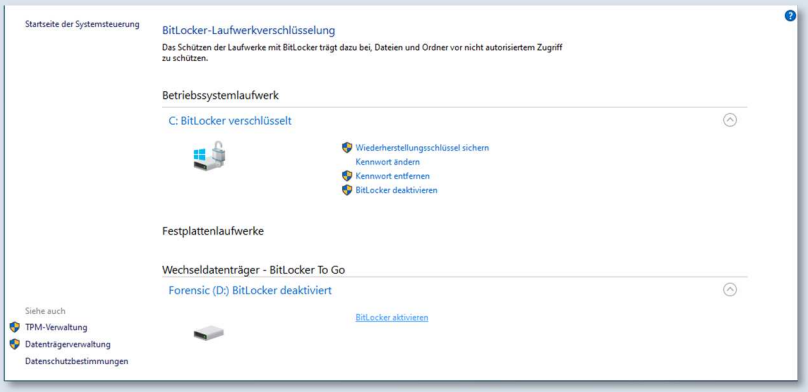


Geben Sie den Begriff „BitLocker“ ein und klicken Sie auf den Eintrag „BitLocker Verwalten“.

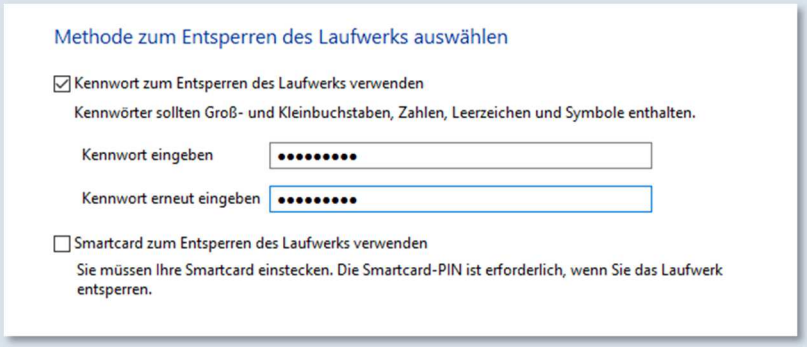


Dieser öffnet die Systemsteuerung mit der BitLocker-Laufwerkverschlüsselung, in der Ihre Betriebssystemlaufwerke und Wechseldatenträger aufgelistet werden, die mit BitLocker verschlüsselt werden können.

Klicken Sie neben dem gewünschten Laufwerk auf „BitLocker aktivieren“ und richten Sie nun die Verschlüsselung ein.

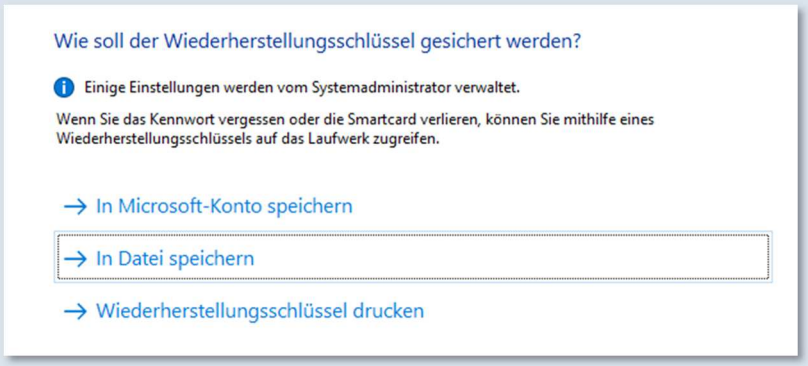


Wählen Sie ein sicheres Kennwort nach den Kriterien, wie sie Ihnen in Kapitel 1 „Vorgehen für die Erstellung von sicheren Passwörtern“ vorgestellt wurden.

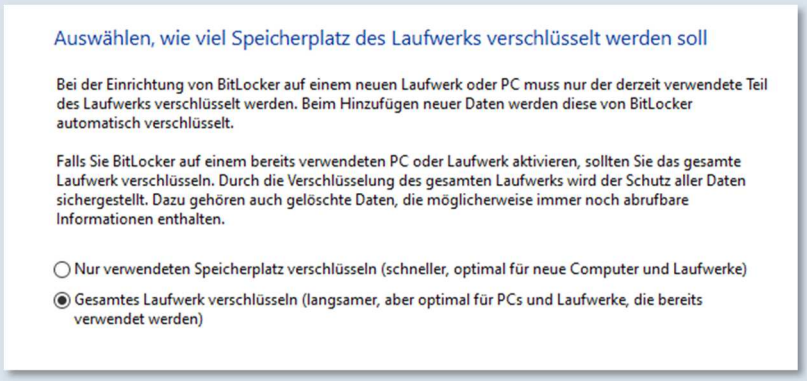


Sichern Sie den Wiederherstellungsschlüssel in einer Datei auf einem USB Stick und verwahren Sie ihn an einem sicheren Ort.

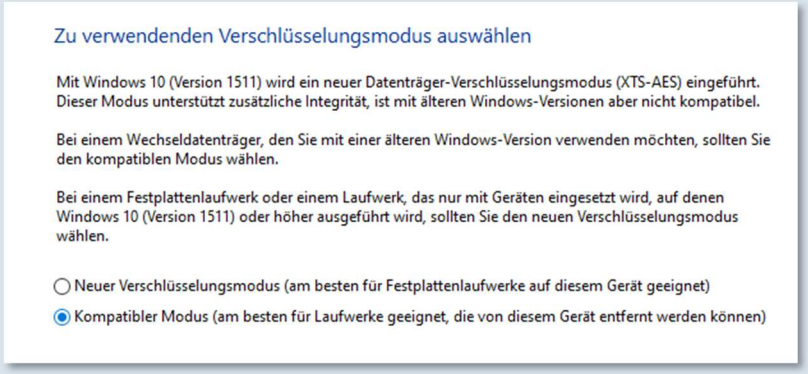
Alternativ können Sie den Wiederherstellungsschlüssel auch ausdrucken und an einem sicheren Ort verwahren.



Verschlüsseln Sie das gesamte Laufwerk;



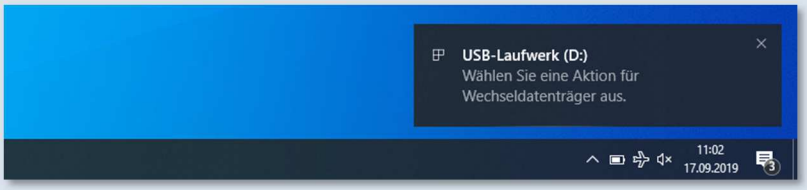
Verwenden Sie für das Laufwerk den kompatiblen Modus und starten Sie die Verschlüsselung, die einige Zeit in Anspruch nehmen kann.



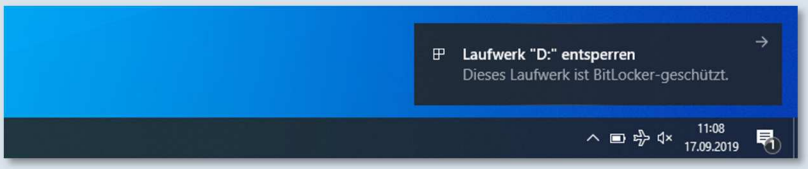
2.2.2. Laufwerk entschlüsseln

Schließen Sie den USB Stick an Ihrem Arbeitsrechner an;

Klicken Sie auf das Benachrichtigungsfeld zum Auswählen einer Aktion für den Wechseldatenträger;



Klicken Sie wiederum auf das Benachrichtigungsfeld zum Entsperren des Wechseldatenträgers;



Geben Sie Ihr Kennwort zum Entschlüsseln des BitLocker geschützten Laufwerks ein;

nun ist Ihr USB Stick wieder entschlüsselt.

2.3. Verschlüsselung des gesamten Betriebssystems mit VeraCrypt

Siehe hierzu unten **Seite 30**.

3. Sicherer Versand von Dateien per E-Mail

Um personenbezogene Daten oder andere sensible Informationen beim Versand per E-Mail gegen Abfangen oder Abhören von Nachrichten oder am Arbeitsplatz vor dem unbefugten Öffnen und Einsehen zu schützen, sollten Dokumente zuvor geschützt werden.

Sind Dokumente entsprechend geschützt, können sie sicher per E-Mail an andere Personen versendet werden. Der anschließende Austausch des Kennwortes sollte über einen zweiten Weg erfolgen, als entweder persönlich oder per Telefon und nicht per E-Mail.

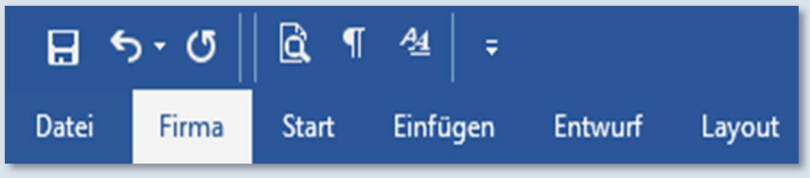
Verwenden Sie zum Versand und Empfang von dienstlichen E-Mails keine privaten, sondern nur dienstlich gebilligte E-Mailkonten.

3.1. Kennwortschutz von Dokumenten

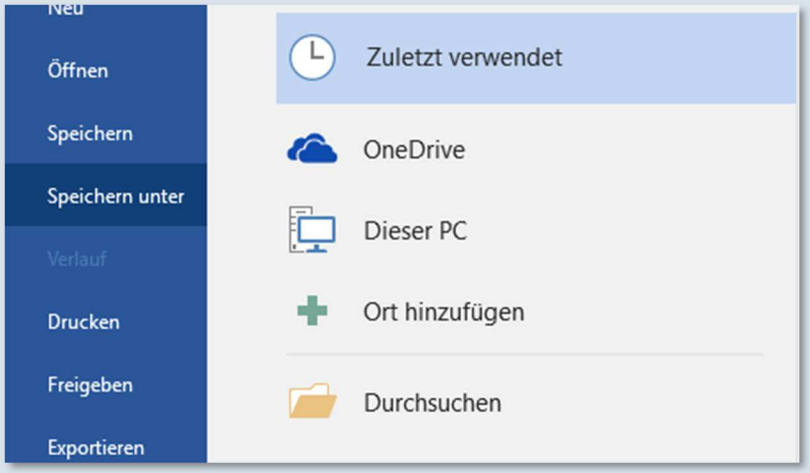
Bei dieser Methode wird das Öffnen eines Microsoft-Office-Dokumentes (Word, Excel und PowerPoint) durch ein Kennwort geschützt. Nur wer dieses kennt, kann das Dokument öffnen, einsehen und bearbeiten.

3.1.1. Datei mit Kennwort schützen

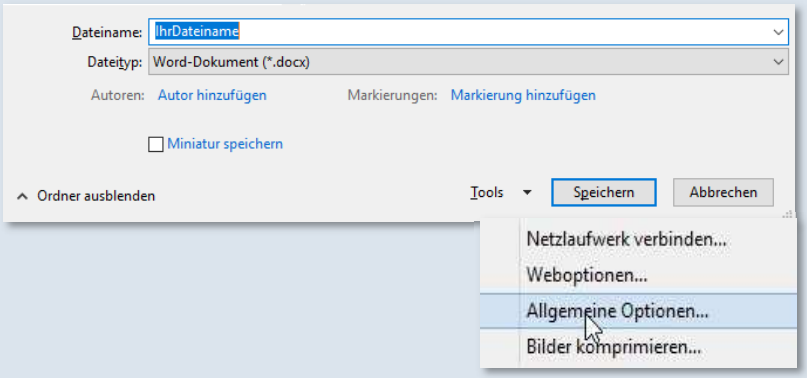
Klicken Sie oben in der Menüleiste auf den Reiter „Datei“;



Wählen Sie anschließend unter „Speichern unter“ und „Durchsuchen“ den Ort aus, an dem Sie die Datei speichern möchten;

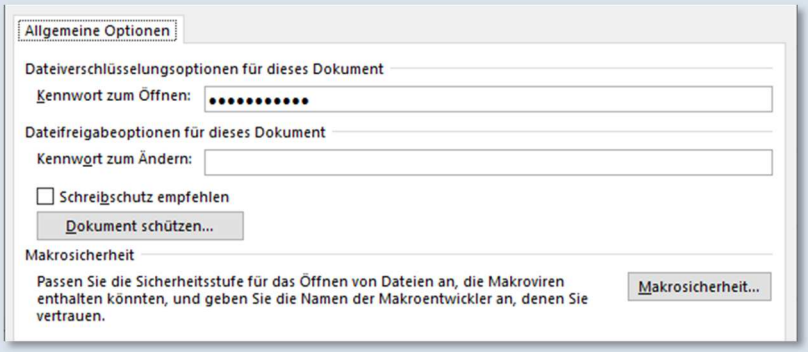


Vergeben Sie einen Dateinamen und wählen Sie über die Schaltfläche „Tools“ die „Allgemeinen Optionen“ aus;



Wählen Sie ein sicheres Kennwort nach den Kriterien, wie sie Ihnen in Kapitel 1 „Vorgehen für die Erstellung von sicheren Passwörtern“ vorgestellt wurden;

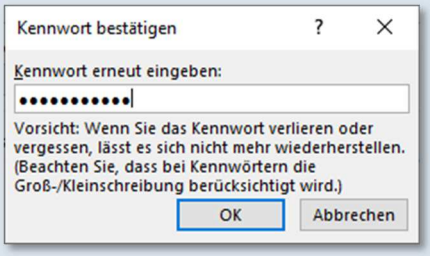
klicken Sie anschließend auf OK;



Bestätigen Sie das Kennwort zur Verschlüsselung der Datei mit erneuter Eingabe;

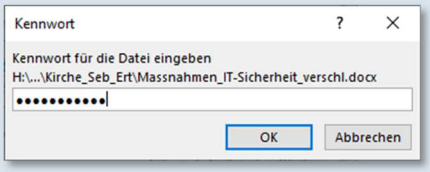
jetzt kann die Datei sicher per E-Mail versendet werden.

Übermitteln Sie das Kennwort über einen zweiten Weg (Bsp.: persönlich oder telefonisch)



3.1.2. Datei mit Kennwort öffnen

Öffnen Sie wie gewohnt eine Office-Datei und geben Sie das Kennwort der Verschlüsselung ein.



3.2. Erstellen verschlüsselter ZIP-Archive

Bei dieser Methode wird ein Archiv erstellt, Dateien hinzugefügt und anschließend verschlüsselt. Ein ZIP-Archiv ist mit einem Ordner vergleichbar, in dem Dateien und Unterordner mit Dateien gesammelt und anschließend kompakt verschlüsselt werden können.

Für die Ver- und Entschlüsselung von ZIP-Archiven eignet sich die Software 7-Zip. Obwohl Windows eigene Boardmittel besitzt, ist zu achten, dass diese für die Entschlüsselung von Archiven mit AES-256 nicht funktionieren.

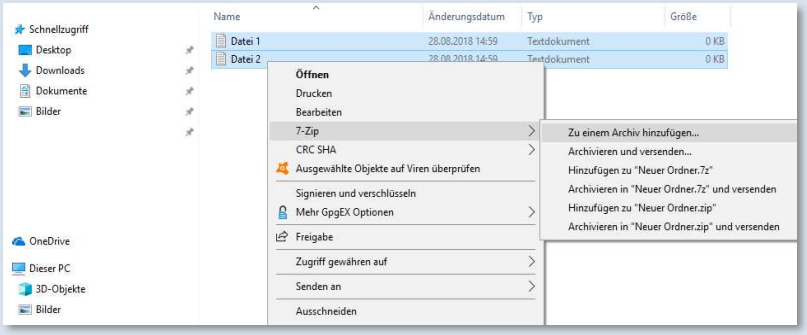
Voraussetzung: Installation der Software 7-Zip

3.2.1. ZIP-Archiv anlegen und verschlüsseln

Um ein Archiv zu erzeugen, markieren Sie zuerst die Dateien und Ordner die Sie packen möchten;

Klicken Sie die Markierung mit der rechten Maustaste an;

Wählen Sie „7-Zip“ und „Zu einem Archiv hinzufügen“ aus.



Wählen Sie einen Dateinamen, verwenden Sie als Archivformat „zip“ und belassen Sie die Einstellungen mit ihren Default-Werten;

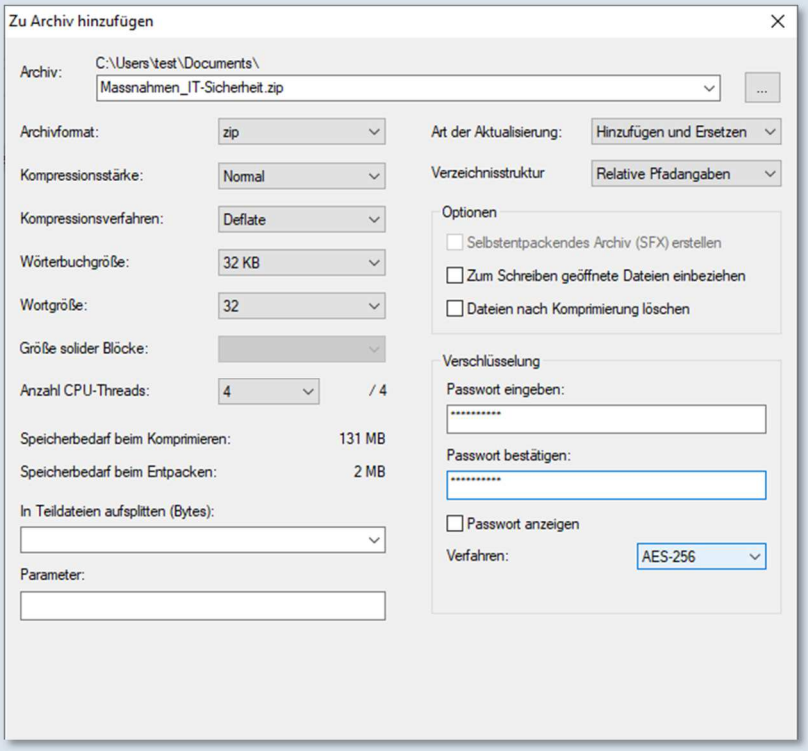
Wählen Sie ein sicheres Kennwort nach den Kriterien, wie sie Ihnen in Kapitel 1 „Vorgehen für die Erstellung von sicheren Passwörtern“ vorgestellt wurden;

Wählen Sie bei dem Verfahren die Verwendung von „AES-256“ aus.

Bestätigen Sie mit Ok;

jetzt kann das Archiv mit den Dateien sicher per E-Mail versendet werden.

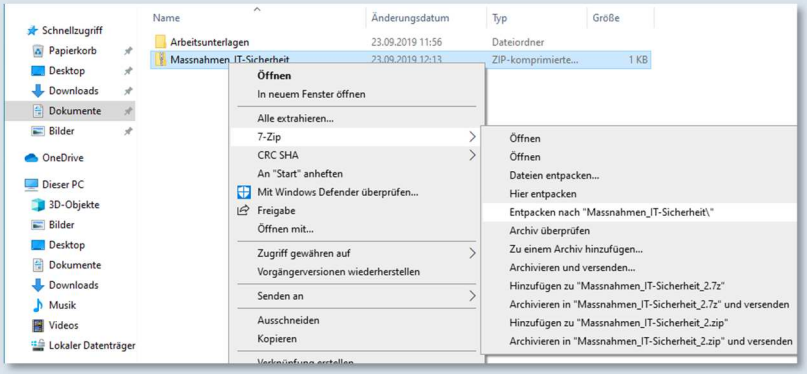
Übermitteln Sie das Kennwort über einen zweiten Weg (Bsp.: persönlich oder telefonisch)



3.2.2. ZIP-Archiv entschlüsseln und öffnen

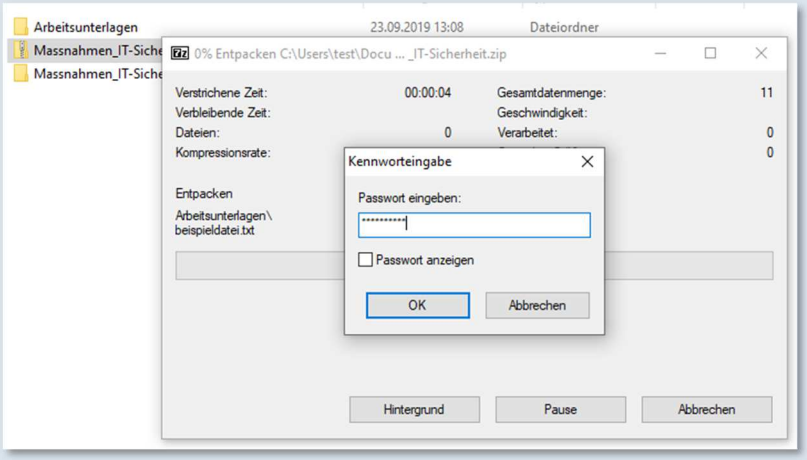
Wählen Sie das verschlüsselte ZIP-Archiv aus und klicken Sie es mit der rechten Maustaste an;

Wählen Sie „7-Zip“ und „Entpacken nach „...“ aus.



Geben Sie das Kennwort der Verschlüsselung ein;

Die Inhalte des Archives werden in einen gleichnamigen Ordner entschlüsselt abgelegt.



4. Verwendung von Datensicherungen

Daten können auf unterschiedliche Weisen verloren gehen, durch versehentliches Löschen, Versagen des Arbeitsrechners, Einfangen eines Virus. Eine regelmäßige Sicherung der wichtigsten Dateien auf einem separaten, verschlüsselten USB Stick kann diesem Verlust vorbeugen.

Wie ein USB-Stick verschlüsselt wird, kann Kapitel 2.2 „Verschlüsselung eines USB Sticks“ entnommen werden.

Voraussetzung: ein USB-Stick mit ausreichend Speicherplatz

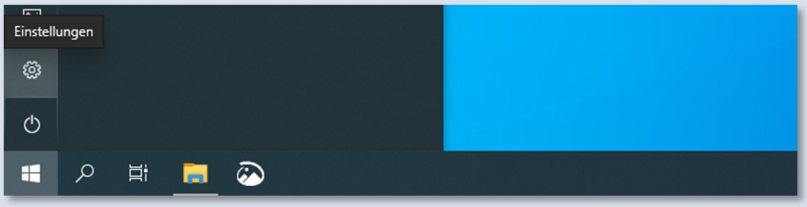
Überlegen Sie sich, welche Dateien Sie auf einem separaten Speichermedium gegen Verlust sichern möchten.	BSP: Informationen, die Sie zu Ihrer Aufgabenerfüllung benötigen und nicht bzw. nur mit großem Aufwand aus anderer Quelle wiederhergestellt werden können.
Überlegen Sie sich, wie regelmäßig Sie diese Dateien sichern möchten;	Dies sollten Sie davon abhängig machen, wie viel Datenverlust für Sie tolerierbar ist und wie der Aufwand einer Neuerstellung der Daten im Verhältnis mit einer Datensicherung steht. BSP: 1x die Woche, jeden Freitag 1x am Tag, nach dem Mittag,
Schließen Sie einen verschlüsselten USB Stick an Ihrem Arbeitsrechner an und entschlüsseln Sie ihn.	Angaben finden Sie in der Anleitung von Kapitel 2.2
Legen Sie beim ersten Sichern einen Ordner „Datensicherung“ an und öffnen Sie diesen. Legen Sie weiter einen Ordner für die Aktuelle Datensicherung an. BSP: Benennung nach dem Datum der Datensicherung	
Legen Sie die zu sichernden Daten in dem zuvor angelegten Ordner ab.	Sorgen Sie dafür, dass Sie Datensicherungen nicht ewig aufbewahren, da sie viel Speicherplatz verbrauchen können. Es bietet sich beispielsweise an, Backups aus den vergangenen 4 Wochen aufzubewahren.

5. Einrichtung eines Sperrbildschirms

Ein Sperrbildschirm sorgt dafür, dass der Arbeitsrechner auch bei kurzen Abwesenheiten gegen den Zugang unbefugter Personen geschützt ist. Dieser sollte sich automatisch nach einigen Minuten der Inaktivität einschalten und erst nach erneuter Eingabe des Benutzerkennwortes wieder ausschalten.

Der Sperrbildschirm muss von jedem Benutzer am Arbeitsrechner separat eingestellt werden.

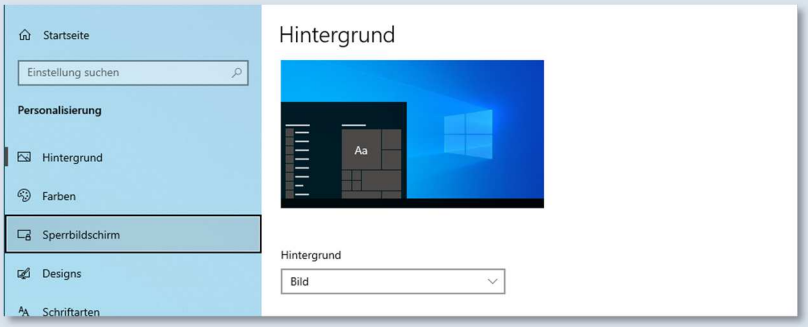
Öffnen Sie über die Taskleiste das Windowsmenü und klicken Sie auf das Zahnrad, um die „Windows-Einstellungen“ zu öffnen.



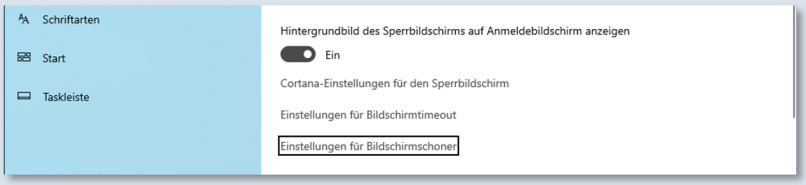
Dort erhalten Sie eine Übersicht der verschiedenen Einstellungsbereiche. Wählen Sie den Bereich „Personalisierung“ mit dem Bildschirmsymbol aus.

In der linken Menüübersicht gehen Sie weiter auf den Eintrag „Sperrbildschirm“.

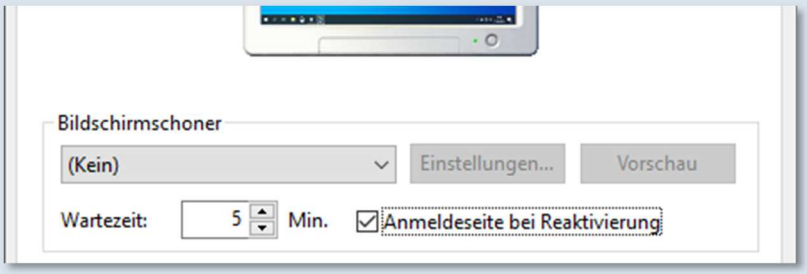
Dort werden eine Vorschau Ihres Sperrbildschirms sowie weitere Konfigurationsmöglichkeiten angezeigt.



Wählen Sie die „Einstellungen für Bildschirmschoner“ aus;



Setzen Sie das Häkchen bei „Anmeldeseite bei Reaktivierung“ und stellen Sie eine Dauer für die automatische Aktivierung der Bildschirmsperre bei Inaktivität ein (Empfohlen sind maximal: 5-10 Minuten).

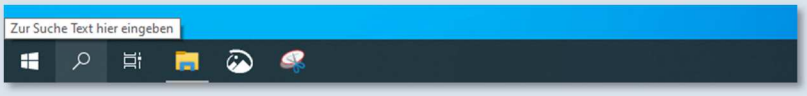


6. Aktivierung eines Virenscanners

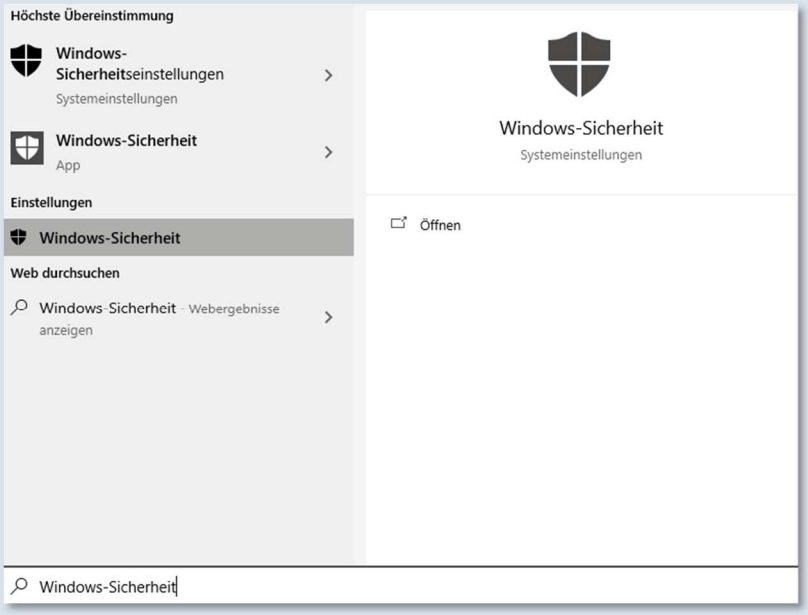
Beim Surfen im Internet, dem Herunterladen von Dateien oder dem Öffnen von E-Mails unbekannter Absender muss immer aufgepasst werden, dass keine Schadprogramme auf den Arbeitsrechner gelangen. Ein Virenscanner hilft solche Schadprogramme zu erkennen, den Fund zu melden und sie rechtzeitig in einen abgeschirmten Bereich, die Quarantäne, zu verschieben.

Windows 10 bietet dafür entsprechende Möglichkeiten bereits an.

Klicken Sie auf der Taskleiste auf die Lupe, um die Suchfunktion zu starten.

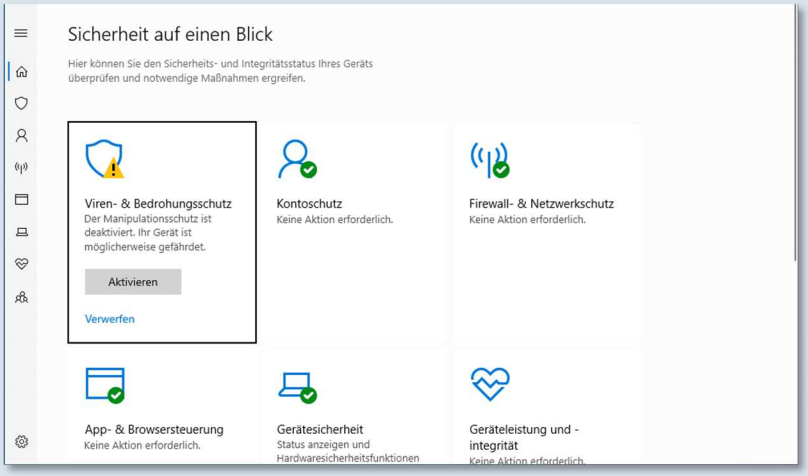


Geben Sie den Begriff „Windows-Sicherheit“ ein und klicken Sie auf den Eintrag „Windows-Sicherheit“.

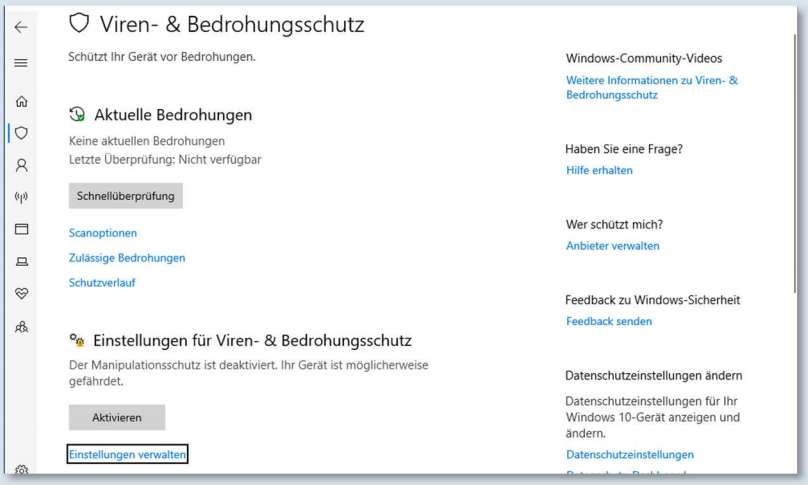


Dieser öffnet die Systemeinstellung für zusätzliche Sicherheitsmaßnahmen, wo in einer Übersicht die verschiedenen Schutzbereiche aufgelistet werden.

Klicken Sie auf den Bereich „Vieren- & Bedrohungsschutz“ mit dem Schild-Symbol.



Folgen Sie der Seite bis zu den „Einstellungen für Viren- & Bedrohungsschutz“ und klicken Sie „Einstellungen verwalten“ an;

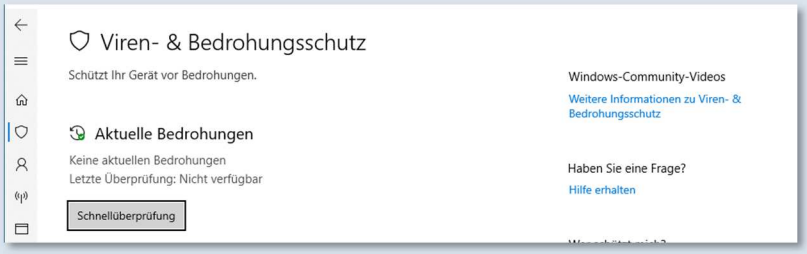


Schalten Sie die folgenden Maßnahmen ein:

Schalten Sie die folgenden Maßnahmen aus:

Verwerfen Sie den Hinweis zum Einrichten von OneDrive;

Drücken Sie in der linken Menüübersicht auf das Schildsymbol und kehren Sie damit in die Einstellungen für „Viren- & Bedrohungsschutz“ zurück;



Starten Sie eine „Schnellüberprüfung“ und warten Sie, bis diese abgeschlossen ist;

Ihr Gerät ist nun mit Maßnahmen gegen Viren und andere Bedrohungen geschützt und warnt Sie vor möglichen Gefährdungen. Zusätzlich haben Sie eine erste Überprüfung manuell durchgeführt.
Hinweise zu möglichen Gefährdungen sollten Sie immer beachten, lesen und zur Kenntnis nehmen. Gegebenenfalls ist sogar die Durchführung weiterer Aktionen gefordert.

7. Verwendung einer Firewall

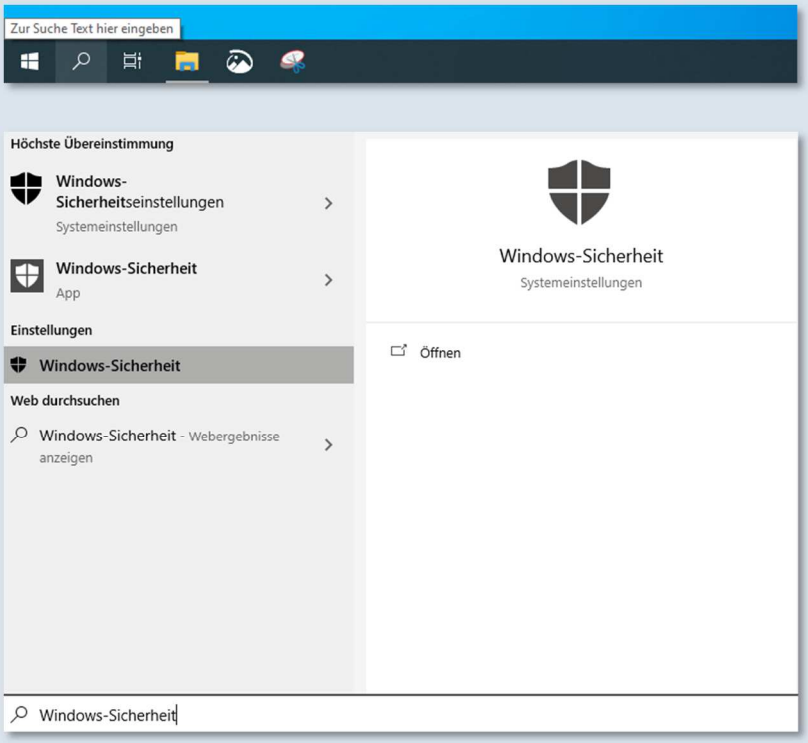
Eine Firewall kontrolliert alle eingehenden und ausgehenden Kommunikationsverbindungen. Sie legt fest, welche Anwendungen und Dienste mit dem Internet wie genau kommunizieren dürfen. Typischer Weise werden eingehende Verbindung, also vom Internet aus zum Arbeitsrechner, generell geblockt und müssen manuell freigegeben werden. Ausgehende Verbindungen, also vom Rechner ins Internet, werden hingegen typischerweise zugelassen.

Auf den verwendeten Arbeitsrechnern sollte eine Firewall daher immer aktiviert sein, um eingehende Verbindungen über das Netz zu verhindern. Bei Windows 10 ist diese im Auslieferungszustand bereits aktiviert. Schalten Sie diese Funktion nicht aus.

Sie können den Status der Firewall wie folgt überprüfen:

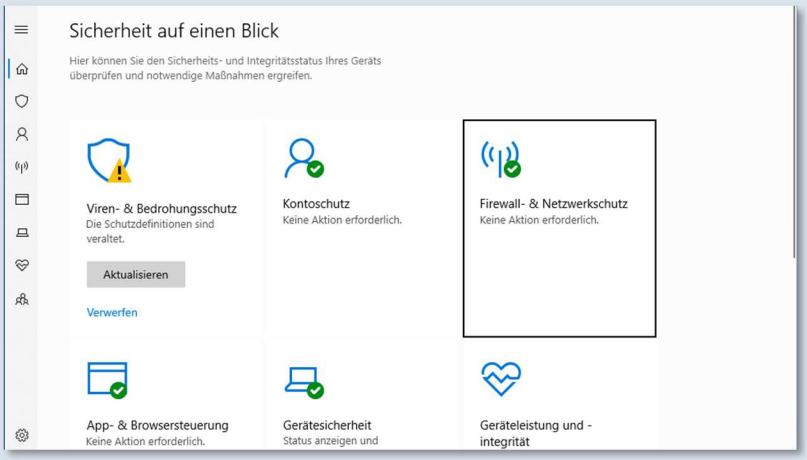
Klicken Sie auf der Taskleiste auf die Lupe, um die Suchfunktion zu starten.

Geben Sie den Begriff „Windows-Sicherheit“ ein und klicken Sie auf den Eintrag „Windows-Sicherheit“.

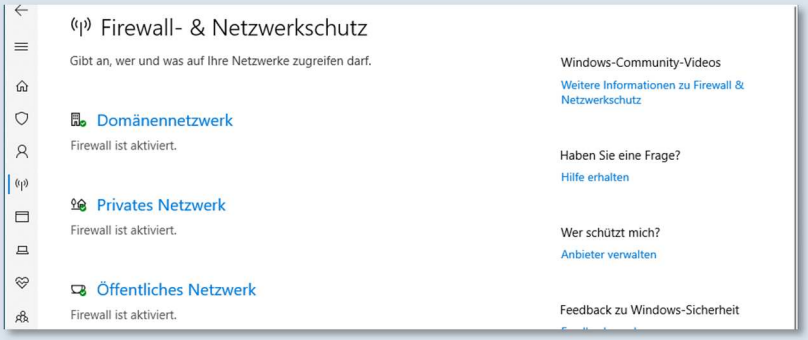


Dieser öffnet die Systemeinstellung für zusätzliche Sicherheitsmaßnahmen, wo in einer Übersicht die verschiedenen Schutzbereiche aufgelistet werden.

Klicken Sie auf den Bereich „Firewall- & Netzwerkschutz“ mit dem Antennen-Symbol.



Stellen Sie sicher, dass die Firewall in jedem der drei Fälle aktiviert ist.

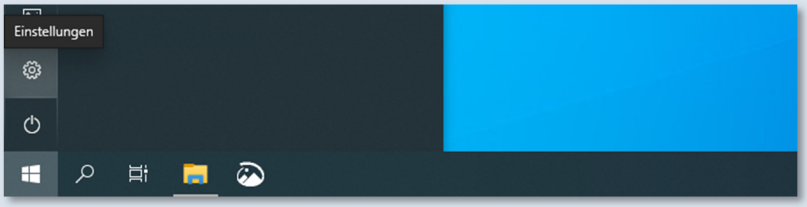


8. Aktualisierung des Betriebssystems

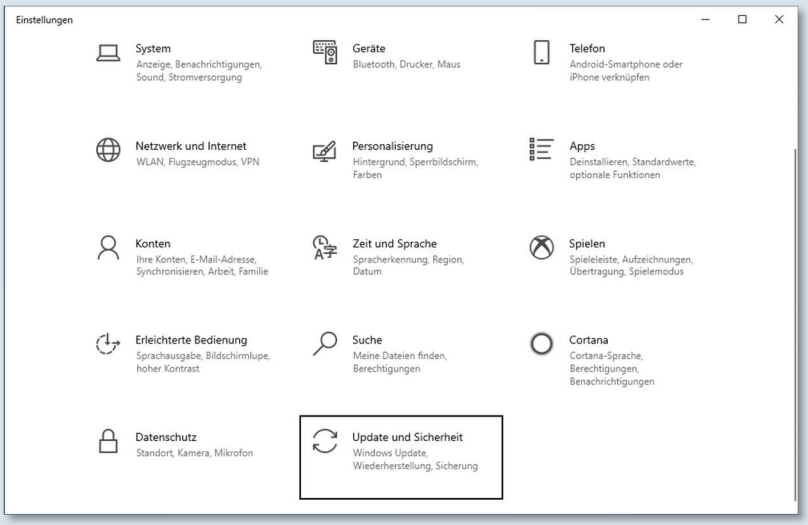
Bei Windows 10 werden Sicherheitsupdates im Auslieferungszustand automatisch installiert, sofern eine Verbindung zum Internet besteht. Dies gilt auch für Microsoft Office. Achten Sie darauf, dass diese Funktion nicht deaktiviert wird.

Nach der Installation weiterer Software müssen Sie ggfs. selbst sicherstellen, dass diese aktuell gehalten wird, insbesondere bei zusätzlich installierten Internet-Browsern. Installieren Sie des Weiteren Software nur aus vertrauenswürdigen Quellen. Deinstallieren Sie Software, die Sie nicht benötigen.

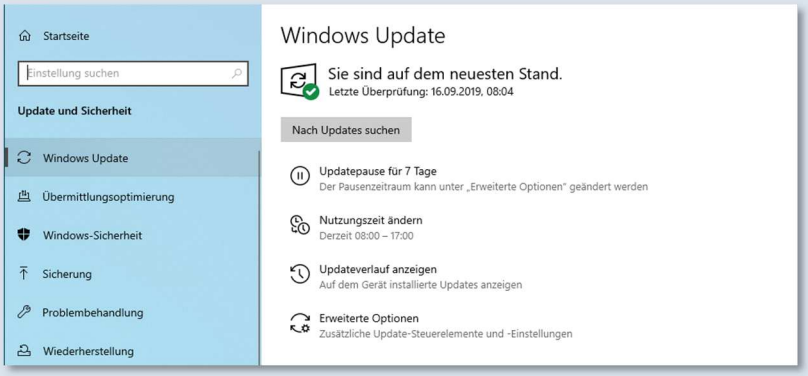
Öffnen Sie über die Taskleiste das Windowsmenü und klicken Sie auf das Zahnrad, um die „Windows-Einstellungen“ zu öffnen.



Dort erhalten Sie eine Übersicht der verschiedenen Einstellungsbereiche. Wählen Sie den Bereich „Update und Sicherheit“ mit dem Aktualisierungssymbol aus.



Auf der rechten Seite können Sie nach neuen Systemupdates für Windows suchen und diese anschließend installieren lassen.



9. Sicheres Arbeiten mit mehreren Benutzern

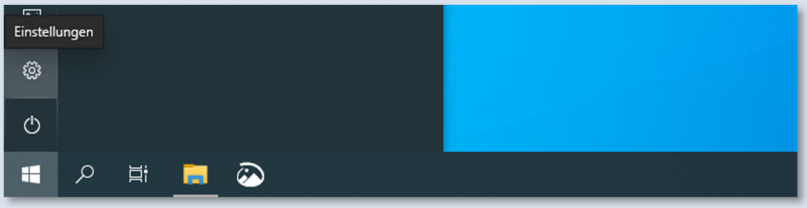
Sofern mehrere Nutzer an einem Arbeitsrechner arbeiten, sollte für jeden ein eigenes Benutzerkonto eingerichtet werden. Damit wird verhindert, dass Nutzer Änderungen an Daten im Namen anderer Personen vornehmen, auf Dokumente zugreifen, die für sie nicht freigegeben sind, oder individuell Software installieren können.

Ebenso wichtig ist, dass Nutzer für die normale Arbeitserledigung keine Administrator Konten verwenden oder ihnen Adminrechte zugewiesen werden. Administrative Änderungen an einem Arbeitsgerät, wie bspw. dem Installieren von Software, sollte demjenigen obliegen der das Gerät verwaltet und nur zu den Zeitpunkten vorgenommen werden, wenn sie erforderlich sind.

Standardmäßig besitzt ein Arbeitsrechner mit Windows 10 nach der ersten Inbetriebnahme einen Admin-Benutzer. Da dieser im Alltagsbetrieb nicht verwendet werden sollte, sollten immer Standardbenutzer angelegt werden. Daher sollte der Verwalter des Gerätes erst für sich selber ein eigenes Standardkonto anlegen und anschließend für notwendige Mitarbeiter. Es sollte darauf geachtet werden, das entsprechende Mitarbeiter beim Anlegen anwesend sind, um ihr sicheres Kennwort sowie nötig Sicherheitsfragen selbstständig auswählen zu können. Ist dies nicht möglich, sollten die Mitarbeiter darauf hingewiesen werden, diese nach der ersten Anmeldung sofort zu ändern.

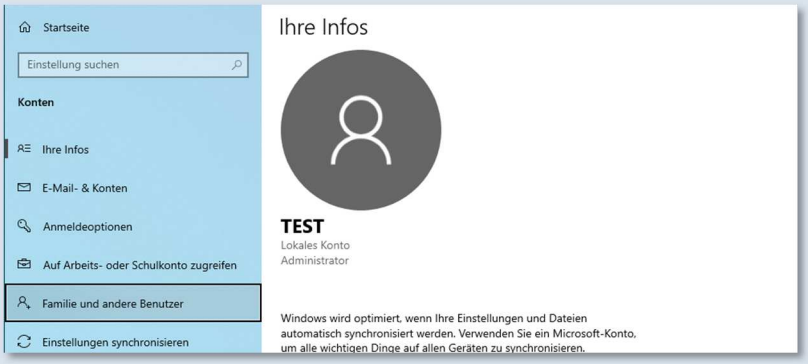
9.1. Anlegen eines neuen Benutzers

Öffnen Sie über die Taskleiste das Windowsmenü und klicken Sie auf das Zahnrad, um die „Windows-Einstellungen“ zu öffnen.



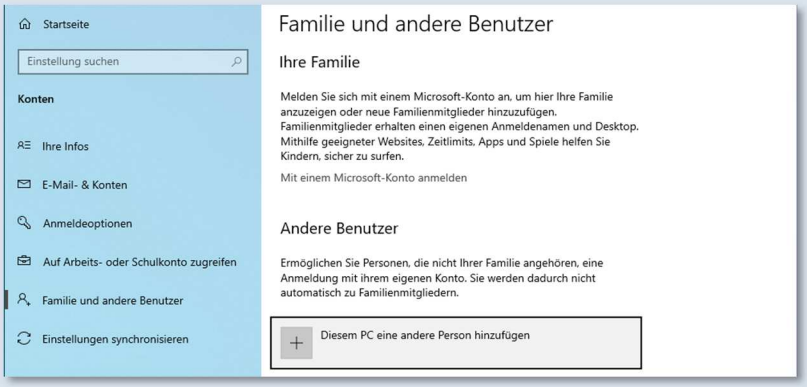
Dort erhalten Sie eine Übersicht der verschiedenen Einstellungsbereiche. Wählen Sie den Bereich „Konten“ mit dem Personensymbol aus.

In der linken Menüübersicht gehen Sie weiter auf den Eintrag „Familie & weitere Benutzer“.



Dort werden Familienmitglieder und andere Personen angezeigt, die ein eigenes Benutzerkonto auf Ihrem Arbeitsgerät haben.

Fügen Sie nun eine weitere Person hinzu.

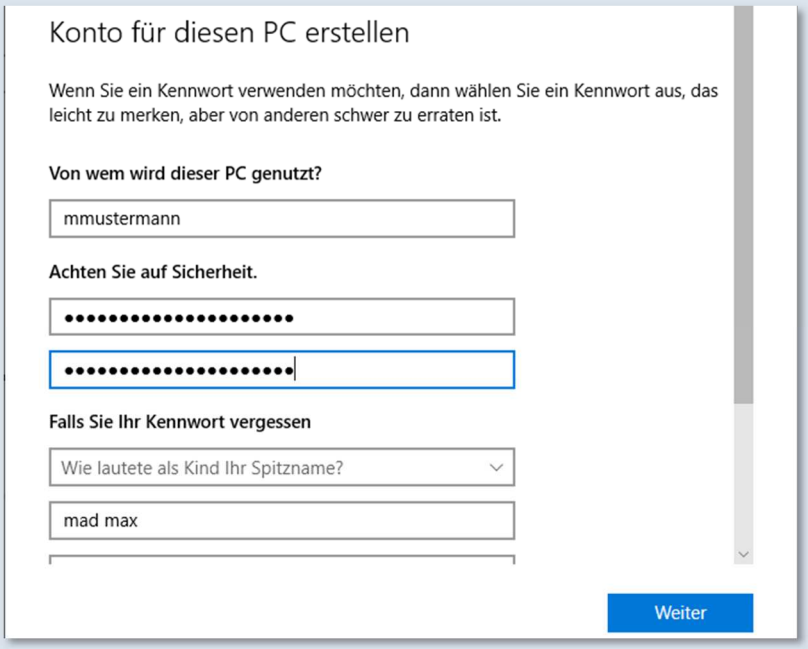


Wählen Sie aus, dass Sie die Anmeldeinformationen für die Person nicht kennen; Wählen Sie aus, dass Sie einen Benutzer ohne Microsoft Konto hinzufügen wollen;

Geben Sie einen Namen für den neuen Benutzer an.

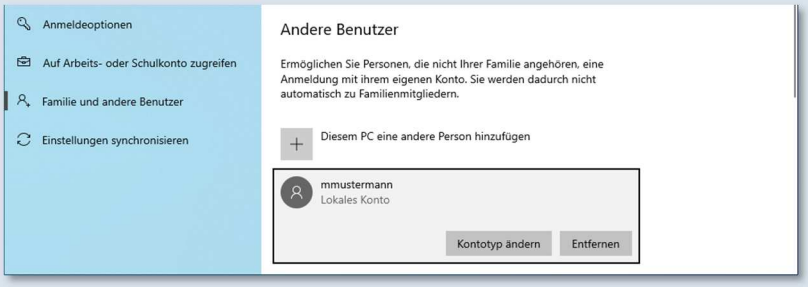
Bestimmen Sie ein sicheres Kennwort (beachten Sie die Kriterien aus Kapitel 1 „Vorgehen für die Erstellung von sicheren Passwörtern“).

Erstellen Sie Ihre Sicherheitsfragen. Das Erstellen der Sicherheitsfragen lässt sich in Windows 10 nicht verhindern. Wählen Sie die Fragen und Antworten so aus, dass nur Sie diese beantworten können.

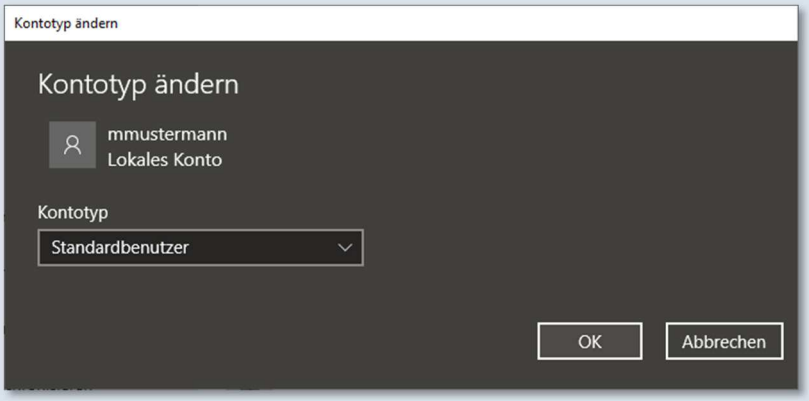


9.2. Beschränkung auf Standardkonten

Klicken Sie auf das neue Benutzerkonto und wählen Sie „Kontotyp ändern“ aus.

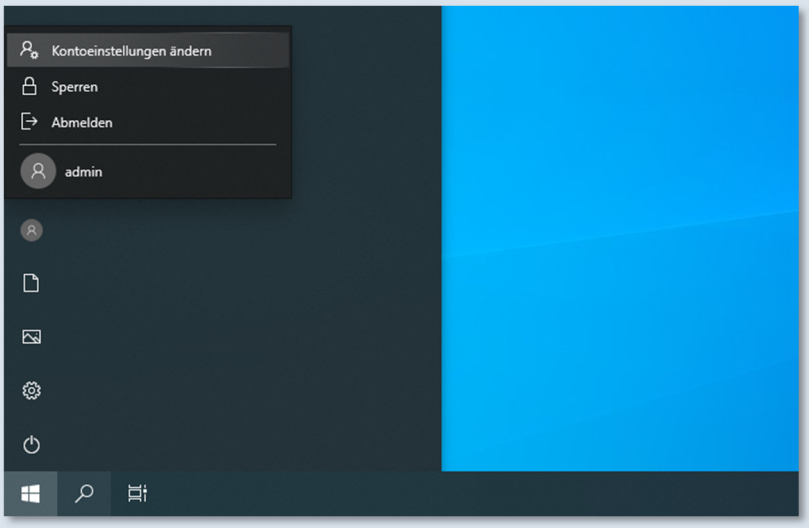


Überprüfen Sie, dass als Kontotyp der „Standardbenutzer“ ausgewählt ist.



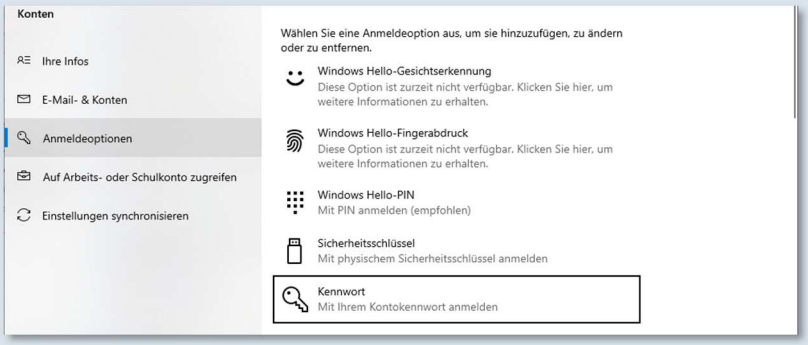
9.3. Nachträgliches Ändern des Benutzerkennwortes

Öffnen Sie über die Taskleiste das Windowsmenü, klicken Sie auf das kreisförmige Personensymbol und wählen Sie „Kontoeinstellungen ändern“ aus.

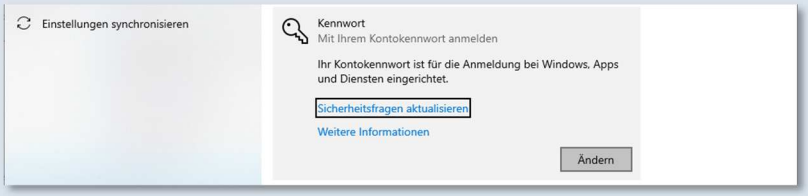


In der linken Menüübersicht gehen Sie weiter auf den Eintrag „Anmeldeoptionen“.

Wählen Sie auf der rechten Seite den Eintrag „Kennwort“ aus.



Hier können Sie die Sicherheitsfragen aktualisieren oder das Kennwort „Ändern“. Achten Sie dabei wieder auf die Kriterien aus Kapitel 1 „Vorgehen für die Erstellung von sicheren Passwörtern“.



10. Ordnungsgerechte Entsorgung von Dokumenten

Wenn Dokumente oder Akten mit schützenswerten Informationen nicht mehr benötigt werden, müssen sie entsorgt werden. Die DIN-Norm 66399 klassifiziert für verschiedenen Materialien (Papier, CD, Festplatte) unterschiedliche Sicherheitsstufen, die definieren, wie entsprechende Materialien zu entsorgen sind. Desto schützenswerter die Dokumente/Akten sind, umso höher ist die Sicherheitsstufe, nach der die Dokumente/Akten zu entsorgen sind.

Für vertrauliche Dokumente oder Akten in Papierform, also beispielsweise jene mit Personenbezug, wird für die Vernichtung mindestens die Sicherheitsstufe P-4 empfohlen. Entsprechende Aktenvernichter können anhand dieser Stufen gekauft werden.

Bei anderen zu vernichtenden Datenträgern oder Geräten wie beispielsweise USB-Sticks, Speicherkarten oder Mobiltelefonen ist sicherzustellen, dass diese nach einem angemessenen Schutzniveau vernichtet werden, ggfs. im Rahmen einer Auftragsverarbeitung.

11. Sicherheitsorientiertes Verhalten am Arbeitsplatz

Um an einem Arbeitsplatz dafür zu sorgen, dass unbefugte Personen weder Einsicht noch Zugriff auf sensible Informationen bzw. Informationen im Allgemeinen erhalten, empfiehlt sich ein ordnungsgemäßes Verhalten am Arbeitsplatz.

Beim Verlassen des Arbeitsplatzes sollten jegliche Unterlagen und Daten mit sensiblen Informationen so aufgebahrt werden, dass unbefugte Personen, wie bspw. Besucher oder Mitarbeiter, ohne größeren Aufwand weder Einsicht noch Zugriff darauf erhalten können. Dokumente, Unterlagen und herumliegende USB-Sticks sollten bspw. in einem verschlossenen Schrank aufbewahrt und am Arbeitsrechner der Sperrbildschirm aktiviert werden. Idealerweise sollten Räumlichkeiten beim Verlassen verschlossen werden. Die Entsorgung von Dokumenten mit sensiblen oder personenbezogenen Informationen sollte nur mit Hilfe von geeigneten Aktenvernichtern vollzogen werden.

Die Vorgehensweise zur Verschlüsselung eines USB Sticks kann dem Kapitel 2.2 „Verschlüsselung eines USB Sticks“ und die zur ordnungsgerechten Entsorgung von Dokumenten dem Kapitel 10 „Ordnungsgerechte Entsorgung von Dokumenten“ entnommen werden.

Verwenden Sie keine Online-Dienste („Cloud Angebote“) zur Verarbeitung von personenbezogenen Daten, die nicht ausdrücklich zur Verwendung freigegeben sind. Dies gilt beispielsweise auch für die Verwendung vom in Windows 10 integrierten Microsoft „OneDrive“ oder Alternativen wie „DropBox“ oder „iCloud“.

Weder Einsicht noch Zugriff auf Informationen und Geräte durch unbefugte Dritte.	Dokumente an einem verschlossen Ort aufbewahren. Am Arbeitsrechner den Sperrbildschirm aktivieren. Den Raum oder das Büro abschließen. USB Sticks an einem verschlossenen Ort aufbewahren. Entsorgung sensibler Papierunterlagen mit P-4 Aktenvernichter. Keine Online Dienste verwenden.

A. Verschlüsselung des gesamten Betriebssystems mit VeraCrypt

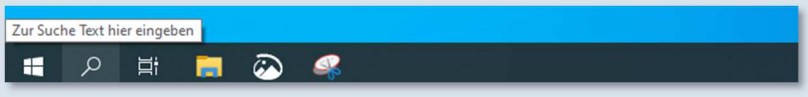
Unter Verwendung der Software VeraCrypt[1] verschlüsselt diese Methode das gesamte Systemlaufwerk mit samt Windows und Ihren Dateien, die Sie auf Ihrem Arbeitsrechner gespeichert haben. Kurz gesagt, Ihr gesamtes System. Tatsächlich verschlüsselt ist das System jedoch nur im abgeschalteten Zustand. Daher sollte der Arbeitsrechner, wenn er nicht verwendet oder transportiert wird, zuvor ordnungsgerecht heruntergefahren werden. Die tatsächliche erstmalige Verschlüsselung kann nach der Konfiguration einige Stunden in Anspruch nehmen.

An dieser Stelle sei darauf hingewiesen, dass die Einrichtung einer Systemverschlüsselung mit VeraCrypt anspruchsvoller und komplizierter umzusetzen ist, als eine mit BitLocker.

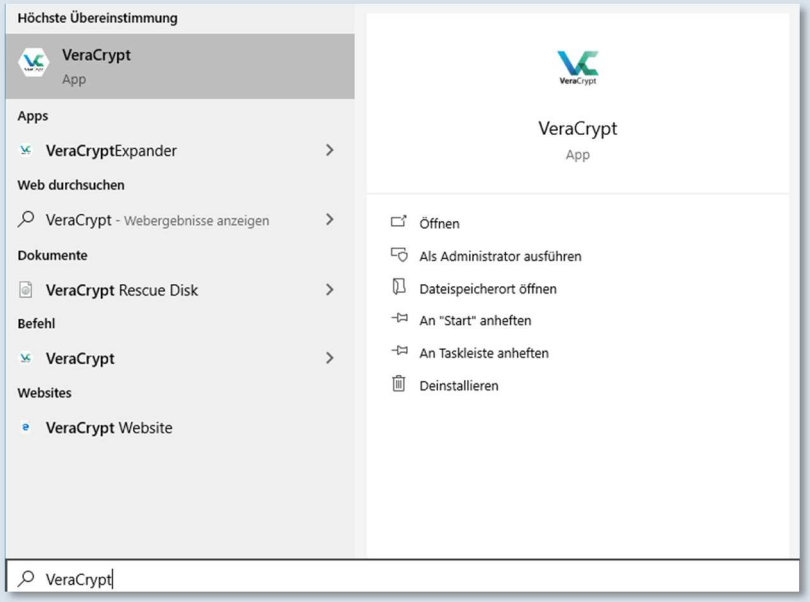
Voraussetzung: Installation der Software VeraCrypt

A.1. Laufwerk verschlüsseln

Klicken Sie auf der Taskleiste auf die Lupe, um die Suchfunktion zu starten.



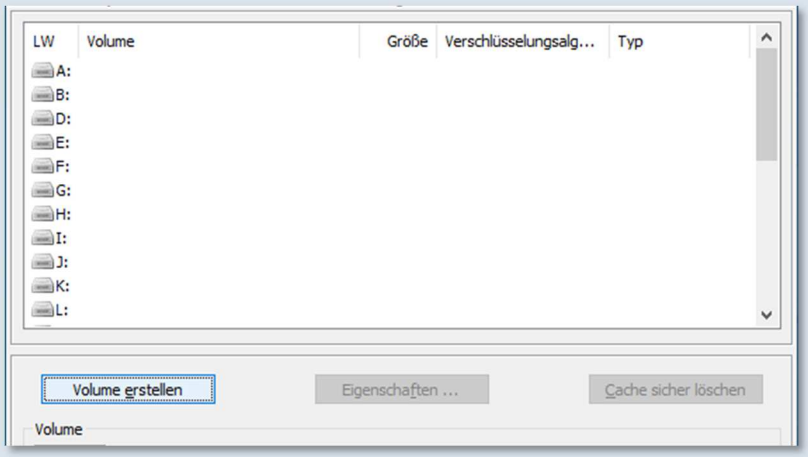
Geben Sie den Begriff „VeraCrypt“ ein und öffnen Sie die App „VeraCrypt“.



[1] In Kontext dieser Dokumentation erfolgte die Verwendung der Software VeraCrypt in der Version 1.24-Hotfix1

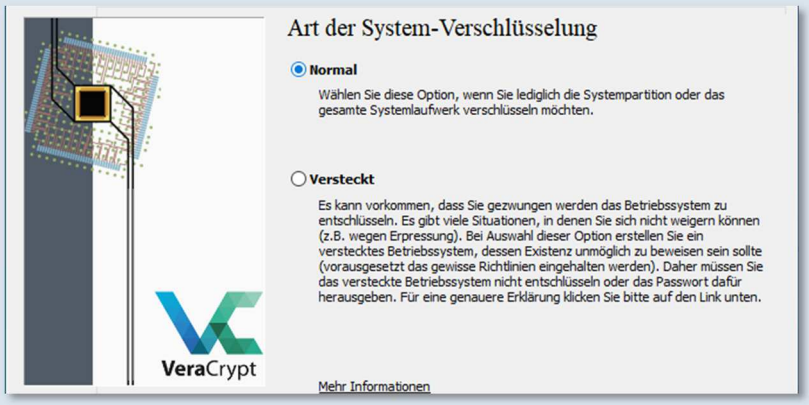
Dieser öffnet das Programm VeraCrypt, in dem eine Übersicht der verfügbaren Laufwerken aufgelistet wird.

Klicken Sie auf „Volume erstellen“, um die Verschlüsselung des Systemlaufwerkes vorzubereiten.



Wählen Sie zur Verschlüsselung des gesamten Systems eine „System-Partition bzw. ein System-Laufwerk“ aus.

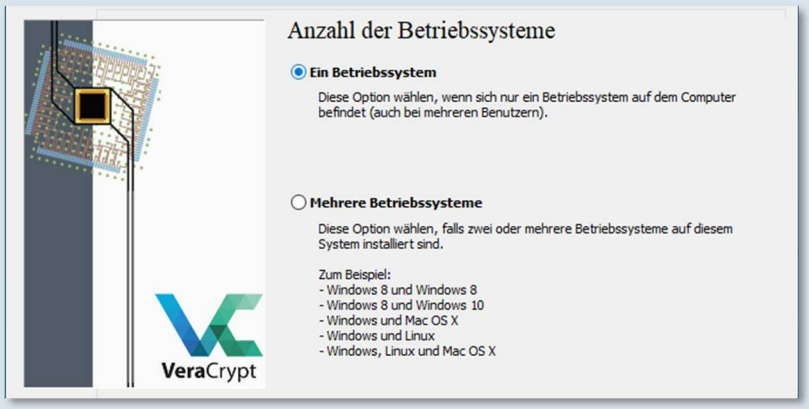
Wählen Sie die „normale“ Art der System-Verschlüsselung aus.



Verschlüsseln Sie das „Gesamte Laufwerk“.

Verschlüsseln Sie ebenfalls den Host-geschützten Bereich.

Sofern Sie auf dem Gerät nicht mehrere Systeme benutzen, wählen Sie für die Anzahl „Ein Betriebssystem“ aus.

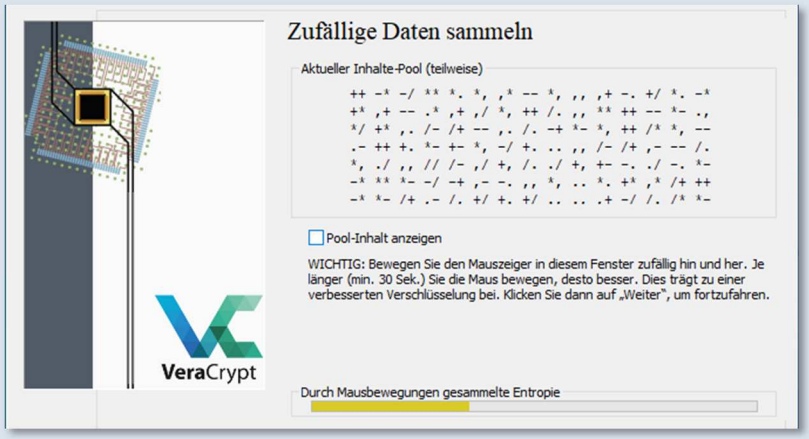


Verwenden Sie als Verschlüsselungsalgorithmus „AES“ und als Hash-Algorithmus „SHA-256“ aus.

Wählen Sie ein sicheres Kennwort nach den Kriterien, wie sie Ihnen in Kapitel 1 „Vorgehen für die Erstellung von sicheren Passwörtern“ vorgestellt wurden;

Für das zufällige Sammeln von Daten bewegen Sie bitte ihre Maus für eine kurze Weile in unbestimmter Manier hin und her, bis sich der Balken mindestens bis in den grünen Bereich fortbewegt hat;

Bestätigen Sie anschließend im nachfolgenden Fenster den generierten Schlüssel.

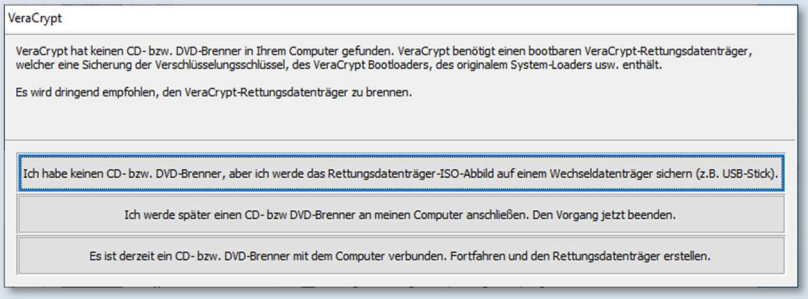


Lesen Sie sich den Hinweis durch und wählen Sie ein Speicherort für einen Rettungsdatenträger;

Idealerweise sollte sich der Speicherort für den Rettungsdatenträger in einem Bereich befinden, der von regelmäßigen Datensicherungen betroffen ist. Siehe dazu Kapitel 4 „Verwendung von Datensicherungen“

Wählen Sie die oberste Möglichkeit „... Rettungsdatenträger-ISO-Abbild auf einem Wechseldatenträger sicher...“ aus;

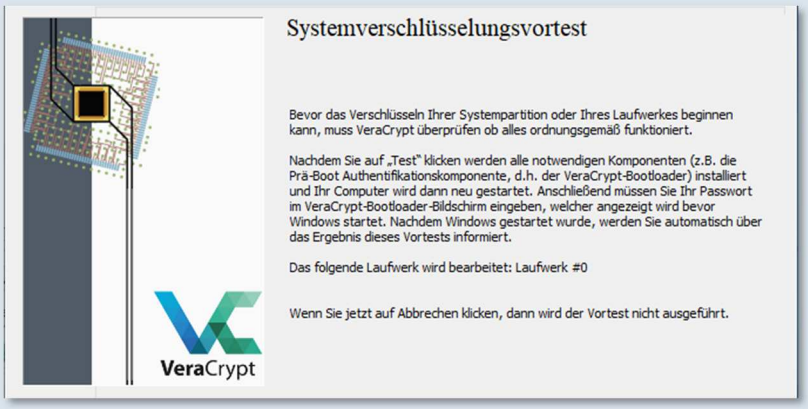
Folgen Sie den Anweisungen, sofern sich der Speicherort nicht in einem Bereich für Datensicherungen befindet.



Auf ein sicheres Löschen kann mit der Auswahl „Ohne (am schnellsten)“ verzichtet werden.

Führen Sie nach den beschriebenen Anweisungen einen Verschlüsselungsvortest durch. Damit wird festgestellt, ob die Verschlüsselung fehlerfrei durchgeführt werden kann.

Hierbei ist ein Systemneustart mit anschließender Eingabe des ausgewählten Kennwortes erforderlich.



Ist nach einem Neustart der Vortest erfolgreich abgeschlossen, können Sie die Verschlüsselung starten, die einige Zeit in Anspruch nehmen wird.

In einer Übersicht wird ihnen der Prozess während des Verschlüsselungsvorgang angezeigt.

A.2. Laufwerk entschlüsseln

Nach dem Einschalten des Arbeitsrechners werden Sie automatisch aufgefordert, das Kennwort zum Entsperren des Laufwerks einzugeben. Erst dann kann das System gestartet werden.