Inhaltsverzeichnis

Vorwort

Sehr geehrte Kolleginnen und Kollegen,

Handy, Smartphone, Tablet und Computer: Sie sind aus der Welt der Jugendlichen nicht mehr wegzudenken. Sie gehören zum Lebensalltag dazu.

- Auf dem Weg zur Schule werden noch einmal kurz die Mails gecheckt.
- Hat mir die Freundin eine WhatsApp geschickt?
- Gibt es etwas Neues in meiner Facebook-Gruppe?
- Hat die Straßenbahn Verspätung oder ist sie heute einmal pünktlich?
- Findet der Unterricht heute nach Plan statt oder fallen Stunden aus?
- Soll es heute Nachmittag regnen? Ich wollte doch mit meinem Freund eine Radtour machen.

Diese und viele andere Fragen werden heute von Jugendlichen in Windeseile mit dem Smartphone erledigt, und zwar ohne weitere Rückfragen und meist auch ohne weitere Vorsichtsmaßnahmen. Viele Jugendliche gehen mit diesen Medien sorglos um, meist zu sorglos. Sind sie sich der Gefahren bewusst, die mit der Nutzung der sozialen Medien, der Messenger-Dienste, des Internets allgemein verbunden sind oder sein können?
Diese Frage und andere sollen in diesem Arbeitsheft beantwortet werden. Der vorliegende Band wird jedoch keine Anleitung zum hundertprozentigen Schutz im Internet geben; dazu gibt es umfangreichere Werke. Er soll auch nicht dazu führen, dass man sich nur noch ängstlich in den digitalen Medien bewegt. Er will aber aufzeigen, welche Gefahren mit der Nutzung verbunden sind und wie man sich weitgehend davor schützen kann, indem man die Möglichkeiten der Absicherung ausreichend nutzt.

Mit diesem Heft sollen Jugendliche sensibilisiert werden, auf ihre Daten besser zu achten, indem sie die digitalen Geräte möglichst gut vor fremden Zugriffen schützen.
Vorfälle in den letzten Wochen, Monaten und Jahren zeigen immer wieder, wie anfällig die Netze für Angriffe von außen sind. Sie müssen nicht jedes Smartphone, nicht jeden Computer treffen, aber man sollte die vorhandenen Mittel einsetzen, um größeren Schaden zu verhindern. Gerade die Angriffe auf die öffentlichen Netze zeigen, wie empfindlich die gesamte Computerstruktur ist. Professionelle Hacker greifen die Netze von Firmen und Verwaltungen an, um Informationen zu gewinnen; sie greifen in private Netze ein, um an persönliche Daten zu gelangen, die dann für kommerzielle Zwecke genutzt werden.

Für Anregungen und Hinweise bin ich dankbar.

Heinz Strauf

heinz@strauf.de

Grundsätzliche Überlegungen zum Schutz meiner Hardware

WAS KANN ICH FÜR MEHR SICHERHEIT TUN?

Noch heute gibt es genügend Menschen, die sich zu wenig Gedanken über den Schutz ihrer Hardware machen. Und das obwohl die fest installierte Hardware als Desktop-Computer im Alltag und in privaten Haushalten immer mehr zugunsten von flexibleren Geräten verschwindet, die über offene Netzwerke dauerhaft mit dem Internet verbunden sind. Das Smartphone als Allroundprodukt birgt neben vielen Vorteilen immer die Gefahr, die sensibelsten Informationen zu einem selbst oder den Kontakten zugänglich zu machen. Da also Smartphones, Smartwatches oder Tablets fast immer online sind, sind auch die Anforderungen an die notwendigen Sicherungsmaßnahmen sehr hoch.

Smartphones, Tablets etc. sind aber auch beliebte Objekte für Diebstähle, gerade weil es stetig neue Modelle gibt, die darüber hinaus schon seit Langem sehr hochpreisig sind. Von daher muss man sich als Nutzer Gedanken darüber machen, wie man die Daten, die sich auf dem Smartphone befinden und die über Datendienste mit dem Gerät gekoppelt sind, sichern kann.

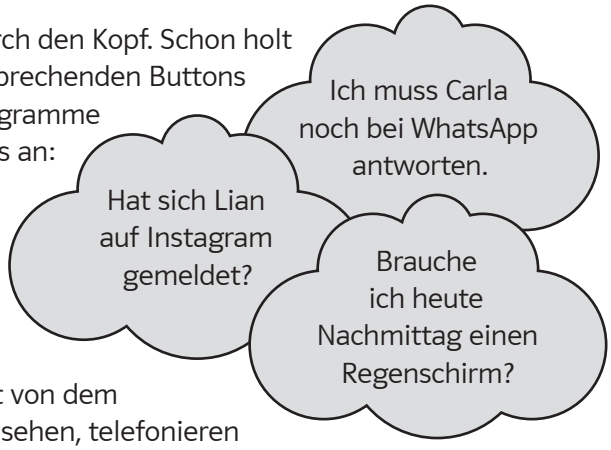
Hier ergeben sich vielfältige Aufgaben für jeden Nutzer, über die sich viele jedoch gar nicht im Klaren sind oder die sie nicht mit der notwendigen Sorgfalt erledigen.

Darüber hinaus darf auch nicht der richtige Schutz der Daten auf dem heimischen PC in Vergessenheit geraten, denn auch dort lauern stetig Gefahren, dass Daten gehackt werden oder sogar der Zugang zu einem Gerät aufgrund eines Virus verweigert wird.

Grundsätzlich gilt hier, man sollte vor allem E-Mails, Links etc. niemals blind vertrauen. Außerdem muss ein guter Virenschutz etc. nicht immer teuer sein, sodass es jedem möglich ist, seine Geräte und Daten zu schützen. Denn bei einem vollständigen Hack geht es ja häufig nicht mehr nur um die eigenen Daten, sondern auch um Daten, Dateien, Bilder, Nachrichten etc. von Kontakten.

Bildschirmsperre – so schütze ich mein Smartphone

Diese Gedanken gehen Mia auf dem Weg zur Schule durch den Kopf. Schon holt sie ihr Smartphone raus und schaut nach. Über die entsprechenden Buttons auf der Oberfläche kann sie sofort die gewünschten Programme aufrufen. Tom, der neben Mia läuft, guckt sie fassungslos an: „Mia, bist du irre? Hast du gar keine Bildschirmsperre?“



Mia geht tatsächlich sehr leichtfertig mit ihrem Smartphone um. Wenn man sofort nach dem Einschalten auf die einzelnen Programme zugreifen kann, ist das Smartphone bei einem Verlust oder einem Diebstahl überhaupt nicht geschützt. Das Smartphone kann sofort von dem Finder oder Dieb genutzt werden, er kann alle Daten einsehen, telefonieren und surfen.

Das ist natürlich gar nicht in Mias Sinne, so informiert sie sich über die verschiedenen Möglichkeiten, ihr Smartphone besser zu sichern.

Eine ganz einfache erste Möglichkeit ist die Bildschirmsperre durch Wischen bzw. Streichen. Dies dient jedoch vor allem dazu, dass, während das Smartphone in der Tasche ist, nicht wahllos irgendwelche Tasten betätigt werden. Zum Datenschutz ist diese Methode natürlich nicht geeignet.

Eine effektivere Methode der Sperre ist ein **Code** aus vier oder sechs Ziffern (Abb. 1).

Eine andere Variante ist das **Muster** (Abb. 2). Man verbindet auf der Tastatur einige Zahlen; nur mit dieser Zahlenkombination ist nun der Bildschirm des Smartphones wieder zu öffnen.

Einige Smartphones können als Bildschirmsperre auch einen **Fingerabdruck** einrichten (Abb. 3). Dies stellt eine nur schwer zu überwindende Sperre dar, denn nur über die bei der Installation gespeicherten Abdrücke lässt sich später der Bildschirm öffnen.

Ganz allgemein gilt: Die automatische Sperre sollte schon nach recht kurzer Zeit einsetzen. Auch wenn sich das Smartphone so sehr häufig automatisch sperrt, was nervig sein kann, ist es jedoch immer sicherer.

Abb. 1

Abb. 2

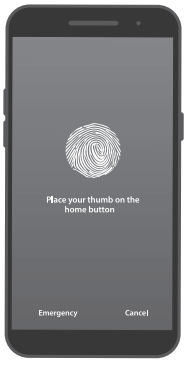


Abb. 3

AUFGABEN

1 **Welche Methoden nutzt ihr? Erstellt eine Strichliste.**

2 **Findet Vor- und Nachteile der Methoden. Diskutiert darüber.**

Passwörter – so schütze ich meine Accounts

WAS KANN ICH FÜR MEHR SICHERHEIT TUN?

Bei diesen vielen Passwörtern, die man im Laufe der Zeit beim Erstellen von Profilen, Accounts und zum Schutz von Smartphone, PC etc. generiert hat, kann man schnell mal den Überblick verlieren. Da liegt der Gedanke doch nah, Passwörter zu verwenden, die man sich besonders gut merken kann, z. B.:

- das Geburtsdatum
- den Vornamen zusammen mit der Lieblingszahl
- 123456
- Test

So leicht darf man es sich natürlich nicht machen. Das Passwort sollte aus einer Kombination von verschiedenen Typen bestehen: Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen. Einige Programme geben vor, aus wie vielen Zeichen in welcher Kombination das Passwort bestehen muss; manchmal erhält man dann bei der Eingabe einen Hinweis darauf, wie stark das eingegebene Passwort ist, sodass man es noch ändern und verstärken kann.

Eine gute Möglichkeit für ein starkes Passwort ist dieses Vorgehen:

Man merkt sich einen einfachen Satz: *Peter geht jeden Tag 1 Stunde um 5 Uhr joggen.* Mit den Anfangsbuchstaben (und Ziffern) bildet man das Passwort, in diesem Fall also: PgjT1Su5Uj. Ein solches Passwort ist für andere schwer herauszubekommen und es fällt auch schwer, sich dieses Passwort zu merken, wenn man nicht den dazugehörigen Satz kennt. Also selbst wenn jemand mal dein Passwort sieht, wird er es sich sicherlich nur schwer merken können – anders als 123456.

Ein weiterer Fehler, den viele in Bezug auf ihre Passwörter begehen, ist, das Passwort für alle Accounts etc. zu nutzen. So gut das Passwort dann auch sein mag, wenn es einmal jemand herausbekommt, hat derjenige Zugriff auf all deine Konten.

Die Passwortflut lässt sich also leider nicht vermeiden, allerdings gibt es allerlei Hilfsprogramme – sogenannte Passwortmanager –, die einem dabei helfen können, den Überblick zu behalten. Dort gibt man alle Passwörter, die man im Gebrauch hat, ein. Für die Öffnung dieses Programms muss man sich dann nur noch ein Passwort merken.

Das sind einige der kostenlosen Passwortverwaltungsprogramme:

DASHLANE	*KEEPASS*	*TRUE KEY*	*ENPASS*	*1PASSWORD*

AUFGABEN

1 **Sprecht über eure jetzigen Passwörter – natürlich ohne sie tatsächlich zu nennen. Was fällt euch auf? Zählen sie zu den einfach zu erratenden Passwörtern?**

2 **Überlegt euch je drei Passwörter nach dem Beispiel oben. Nutzt Sätze, die ihr euch gut merken könnt.**

Passwortcheck – wie sicher sind meine Passwörter?

Du kennst sicherlich schon einige Voraussetzungen für die Erstellung eines Passwortes und weißt auch, welche Kriterien ein gutes Passwort erfüllen muss. Oft wird dir in Apps und Programmen z. B. durch einen Balken von Rot nach Grün gezeigt, wie stark das von dir eingegebene Passwort ist. Das ist aber nicht immer der Fall.

Es gibt deshalb die Möglichkeit, Passwörter durch einen sogenannten Passwortcheck überprüfen zu lassen. Ein solches Programm findest du z. B. unter der Webadresse *https://www.passwortcheck.ch*.

Es öffnet sich dieses Fenster:

Hier wird das zu prüfende Password eingegeben.

Hier erfährt man während der Eingabe, wie stark das Passwort ist.

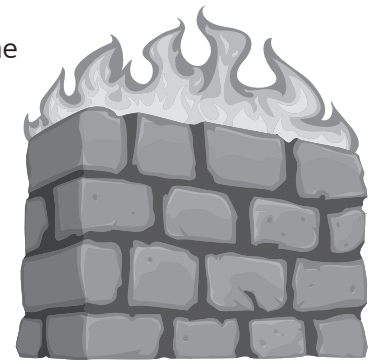
Bei dem Programm *https://checkdeinpasswort.de* ändert sich während der Eingabe des Passworts die Bildschirmfarbe von Rot nach Grün.

AUFGABE

Überprüft auf einer Seite eurer Wahl eure aktuellen Passwörter und kreiert neue.

Eine Firewall einrichten

WAS KANN ICH FÜR MEHR SICHERHEIT TUN?



Neben anderen Vorsichtsmaßnahmen ist die Einrichtung einer Firewall eine der ganz wichtigen Einrichtungen. Die Firewall überwacht den gesamten Datenverkehr auf dem Rechner. Die Firewall soll verhindern, dass es ungewollte Zugriffe von außen gibt. Die Firewall kann auch dafür sorgen, dass bestimmte installierte Anwendungen nur mit der Zustimmung des Nutzers aufgebaut werden können. Durch diese Maßnahmen wird sichergestellt, dass die Anwendungen ständig aktiv kontrolliert werden.

- Wie richtet man eine Firewall ein?
- Kann man Einstellungen nachträglich ändern?

Unter *Windows 10* ist vom System her bereits eine Firewall installiert. Man erreicht die Einstellungen so:

- Unter Einstellungen → *Update und Sicherheit* → *Windows Sicherheit* findet man den Punkt *Firewall & Netzwerkschutz*.
- Jetzt sieht man den Status für die Netzwerke und ob die Firewall aktiviert ist (Abb. 1).
- Wenn man auf *Zugriff von App durch Firewall zulassen* klickt, kann man damit Programme freigegeben (Abb. 2).
- Um weitere Einstellungen an der Firewall vorzunehmen, klickt man auf *Erweiterte Einstellungen*, was aber im Normalfall nicht notwendig ist.

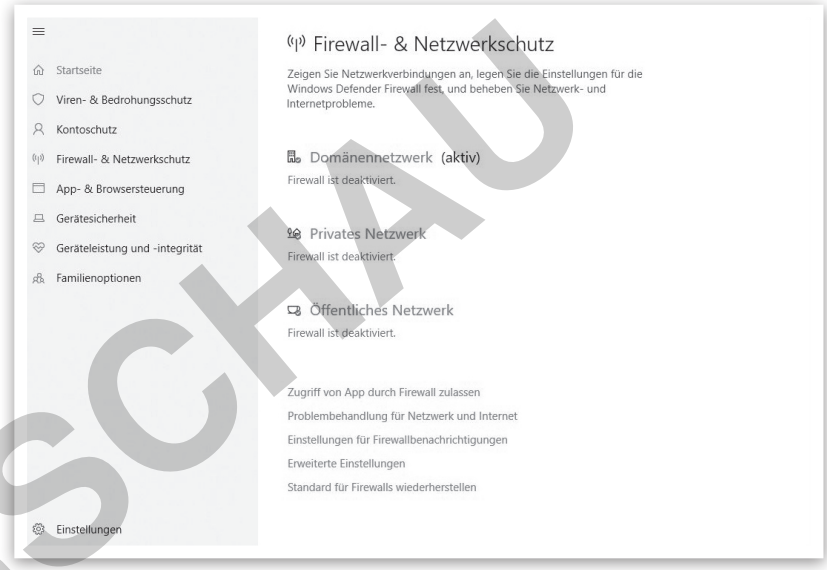


Abb. 1

Wenn man sich bei bestimmten Programmen absichern möchte, kann man diese Programme daran hindern, eine Verbindung zum Internet aufzubauen, damit keine Schadsoftware auf den Rechner gelangt.

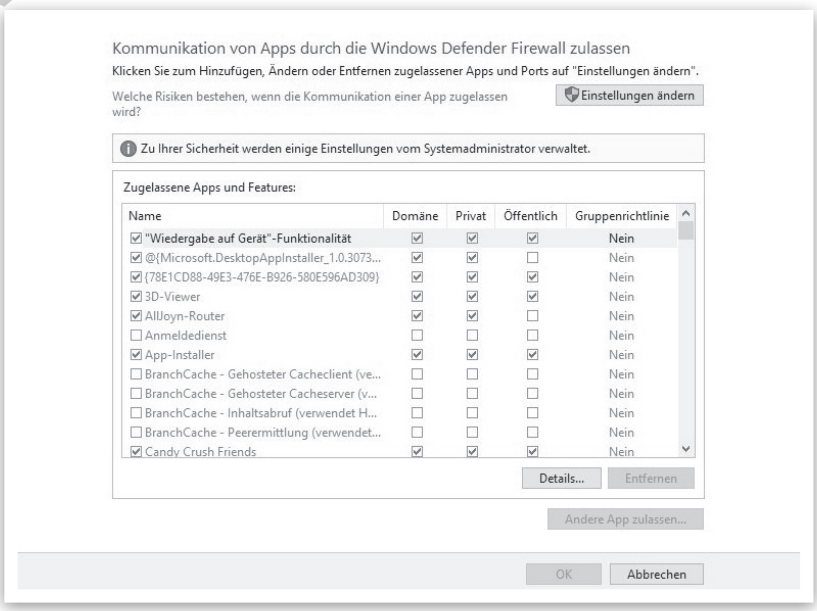


Abb. 2

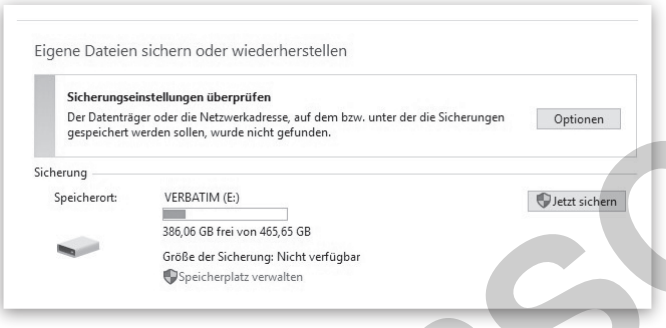
Von wichtigen Daten ein Backup erstellen

„Das ist doch eine Selbstverständlichkeit“, wird eigentlich jeder Nutzer sagen, wenn man ihn nach der Sicherung von wichtigen Dokumenten, Bildern und Videos fragt. Aber was bedeutet das eigentlich: „Sichern wichtiger Daten“? Und welche Möglichkeiten gibt es dafür?

Für viele reicht es schon, wenn sie ihre Daten auf einem weiteren externen Medium oder in einer Cloud gespeichert haben, aber um wirklich gegen den Verlust von allen Daten geschützt zu sein und eine problemlose Wiederherstellung zu ermöglichen, sollte man regelmäßig ein Backup durchführen, was unter *Windows* auch kein Problem bedeutet. Man muss dabei nur berücksichtigen, dass das Backup nicht auf dem Rechner selbst erstellt wird, sondern auf einem anderen Medium. Dazu eignet sich besonders eine kleinere mobile Festplatte oder ein leistungsfähiger Stick. Ein Stick reicht völlig aus, wenn man z. B. nur seine Word-Dokumente und seinen E-Mail-Verkehr sichern möchte. Geht es aber darum, seine umfangreiche Bild- und Videosammlung zu sichern, kommt man um eine externe Festplatte oder auch einen großen (oft kostenpflichtigen) Cloud-Speicherplatz nicht herum.

So erstellt man ein Backup:

Unter dem Punkt *Einstellungen* → *Update und Sicherheit* findet man den Unterpunkt *Sicherung*.



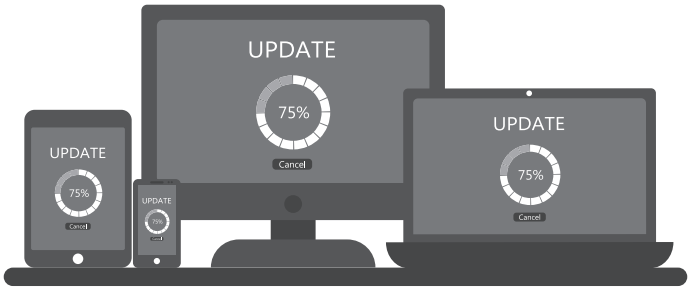
Über den Button *Optionen* kann man bestimmen, auf welchem Datenträger die Sicherungsdateien abgelegt werden sollen.

In dem Feld *Sicherung* sieht man, welches Medium für die Sicherung vorgesehen ist, in diesem Fall das Laufwerk *VERBATIM E:*. Gleichzeitig wird dort angezeigt, wie viel Platz auf dem Speichermedium noch vorhanden ist. Über den Button *Jetzt sichern* startet man den Backup-Prozess.

Über den Verlauf des Backups wird man in einem eigenen Fenster informiert. Sollte man die Sicherung aus irgendeinem Grund unterbrechen wollen, so geschieht dies über den Button *Sicherung beenden*.

Über die Kategorie *Wiederherstellung* kann man später die gespeicherten Daten wiederherstellen, wenn bestimmte Dateien zerstört oder verloren gegangen sein sollten.

Updates regelmäßig durchführen?!



Die Betriebssysteme der Computer und Smartphones müssen immer mehr Anforderungen genügen. Immer wieder gibt es neue Tendenzen, auf die die Hersteller reagieren bzw. reagieren müssen, um mit der Konkurrenz Schritt zu halten. So kündigen die großen Hersteller ihre Updates vorher an, weil mit den Updates meist kleinere oder auch größere Veränderungen verbunden sind.

So ein Update für das Betriebssystem *Windows* kann mitunter Stunden in Anspruch nehmen. Vielen kostet das zu viel Zeit und sie installieren deshalb keine Updates, auch weil viele Neuerungen/Verbesserungen für den durchschnittlichen Nutzer auf den ersten Blick nicht nach einem Zugewinn aussehen.

Ein Update generell nicht durchzuführen, ist in den meisten Fällen allerdings ein Fehler.

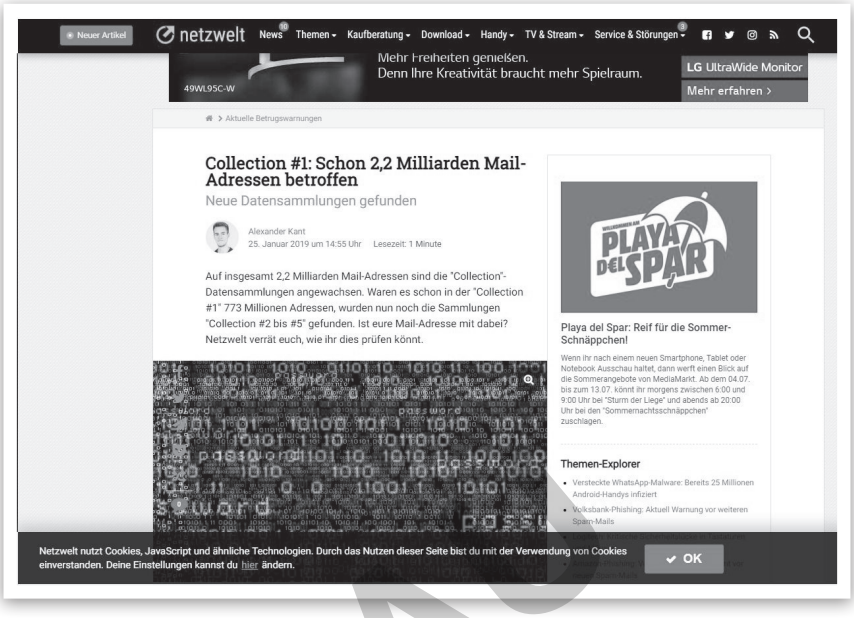
Die Hersteller überprüfen ihre Software regelmäßig und erkennen so, wo sie Schwachstellen hat. Hackern wird es dadurch erschwert, über mögliche Schwachstellen auf Computer zuzugreifen. Ein Update versorgt den Computer mit den entsprechenden Verbesserungen, beseitigt Schwachstellen und sorgt so für einen besseren Schutz des PCs. Aber auch der größere Leistungsumfang, der mit einem Update verbunden sein kann, ist für den Nutzer ein Gewinn.

Deshalb sollte man seinen Computer und sein Smartphone in Bezug auf das Betriebssystem immer auf den neuesten Stand bringen, um Schwachstellen, die einen angreifbar machen, zu beseitigen. Die Updates sind in der Regel kostenlos, können aber einige Zeit und Rechenleistung in Anspruch nehmen. Auf einem Smartphone kann daher im Display die Meldung erscheinen, dass das Update nur mit geladener Batterie und im WLAN durchgeführt werden soll. Um das Betriebssystem immer auf dem neuesten Stand zu haben, sollte bei den Einstellungen darauf geachtet werden, dass die Funktion *Automatisches Update* aktiviert ist, damit man kein Update verpasst.

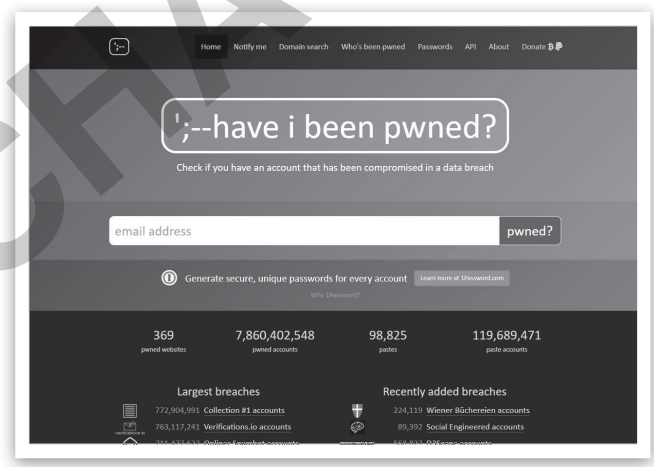
Achtung: Kritisch ist das automatische Update bei Apps auf dem Smartphone. Man kann nicht wissen, ob eine App oder ein Teil von ihr inzwischen kostenpflichtig geworden ist. Deshalb sollten auf dem Smartphone die Updates manuell durchgeführt werden, sodass du dir vorher anschauen kannst, was das Update umfasst/beinhaltet.

„Have I been pwned?“ – wie überprüfe ich die Sicherheit meines E-Mail-Accounts?

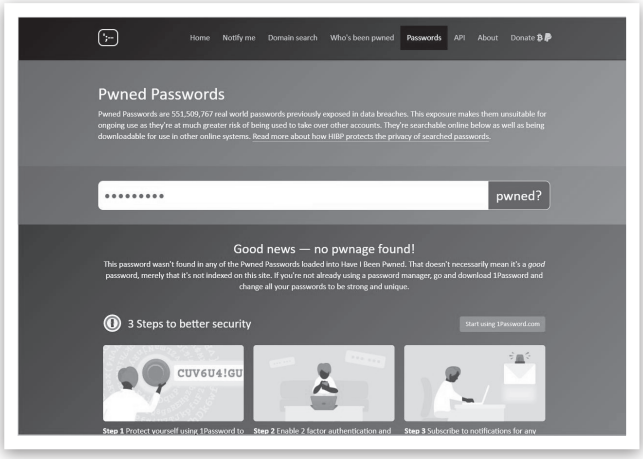
Immer häufiger erfährt man in den Medien, dass größere Datensätze bei den bekannten Anbietern im Netz gehackt/gestohlen wurden. Ob man selbst davon betroffen ist, kann man über die kostenlose Website *haveibeenpwned.com*, die der unabhängige australische Sicherheitsforscher Troy Hunt ins Leben gerufen hat, herausfinden.



In seiner Sammlung sind zurzeit über 300 Millionen Passwörter aus verschiedenen Datenlecks (z. B. von Adobe, Yahoo, Snapchat …) erfasst. Wenn man die eigene E-Mail-Adresse in das Suchfenster eingibt, erhält man sofort eine Rückmeldung, ob man gehackt worden ist oder nicht.



Die App bietet inzwischen auch die Möglichkeit, nach gehackten Passwörtern zu suchen. Wenn man das Passwort eingegeben hat, erhält man sofort eine Rückmeldung, ob das Passwort noch sicher ist. Falls das eingegebene Passwort schon einmal gehackt wurde, erfährt man auch das, allerdings erhält man keine Auskunft darüber, in welchem Account dies geschah.



Wer lieber mit einem Programm in deutscher Sprache arbeiten möchte, kann auf das Programm *Identity Leak Checker* vom Hasso-Plattner-Institut zurückgreifen. Wie in der vorgestellten App gibt man auch hier seine E-Mail-Adresse in das Suchfenster ein; allerdings erhält man die Mitteilung, ob das Konto schon einmal gehackt wurde, nicht sofort, sondern in einer gesondert zugestellten E-Mail.

Cyberangriffe mit *WannaCry*

Im Jahr 2017 machten Meldungen Schlagzeilen, dass in über 150 Ländern mindestens 200.000 *Windows*-Rechner von einer Schadsoftware mit dem Namen *WannaCry* („Willst du weinen?") befallen wurden. Wie kann so etwas passieren, wenn man seinen Rechner eigentlich gut geschützt hat? Die Hacker hatten es verhältnismäßig leicht: Sie kannten eine Sicherheitslücke im Betriebssystem von *Windows*, die kurz nach Bekanntwerden von Microsoft durch ein Update beseitigt wurde. Wenn also alle *Windows*-Nutzer die Möglichkeit des Sicherheitsupdates wahrgenommen hätten, wären sie von dem Angriff verschont geblieben. Dieses Beispiel zeigt, wie wichtig es ist, die angebotenen Updates zu installieren.

Herr Müller will abends, bevor er ins Bett geht, noch seinen Laptop schließen; da sieht er auf dem Bildschirm ein merkwürdiges Bild: Zwei Hände schütteln sich wie bei einer freundlichen Begrüßung oder Verabschiedung mit dem Zusatz „Wanna Decryptor 2.0". Sofort trennt Herr Müller seinen Rechner vom Internet und zieht auch den Stecker aus der Steckdose. Am nächsten Morgen staunte er nicht schlecht, als er den Rechner hochfuhr: Statt einer freundlichen Begrüßung konnte er eine Lösegeldforderung lesen.

Was tun? Sind nun alle Daten verschwunden? Wie kommt Herr Müller an die vielen Fotos, die er auf dem Rechner gespeichert hat? Bekommt er die Dateien komplett wieder, wenn er die geforderte Summe in Bitcoin bezahlt?

Für die privaten Nutzer, die durch die Schadsoftware *WannaCry* geschädigt wurden, empfehlen Sachverständige, nicht auf die Lösegeldforderungen einzugehen. In keinem bisher bekannt gewordenen Fall haben die Hacker tatsächlich die Daten des Rechners entschlüsselt. Dieser Vorgang hätte nämlich für die Hacker insofern ein Problem werden können, weil man so die Spur zurückverfolgen könnte.

Microsoft reagierte schnell, insbesondere für die Betriebssysteme, die eigentlich nicht mehr aktualisiert werden (z. B. *Windows XP*). Es wurde ein Notfall-Patch zur Verfügung gestellt, damit die bestehende Sicherheitslücke in Zukunft geschlossen ist.