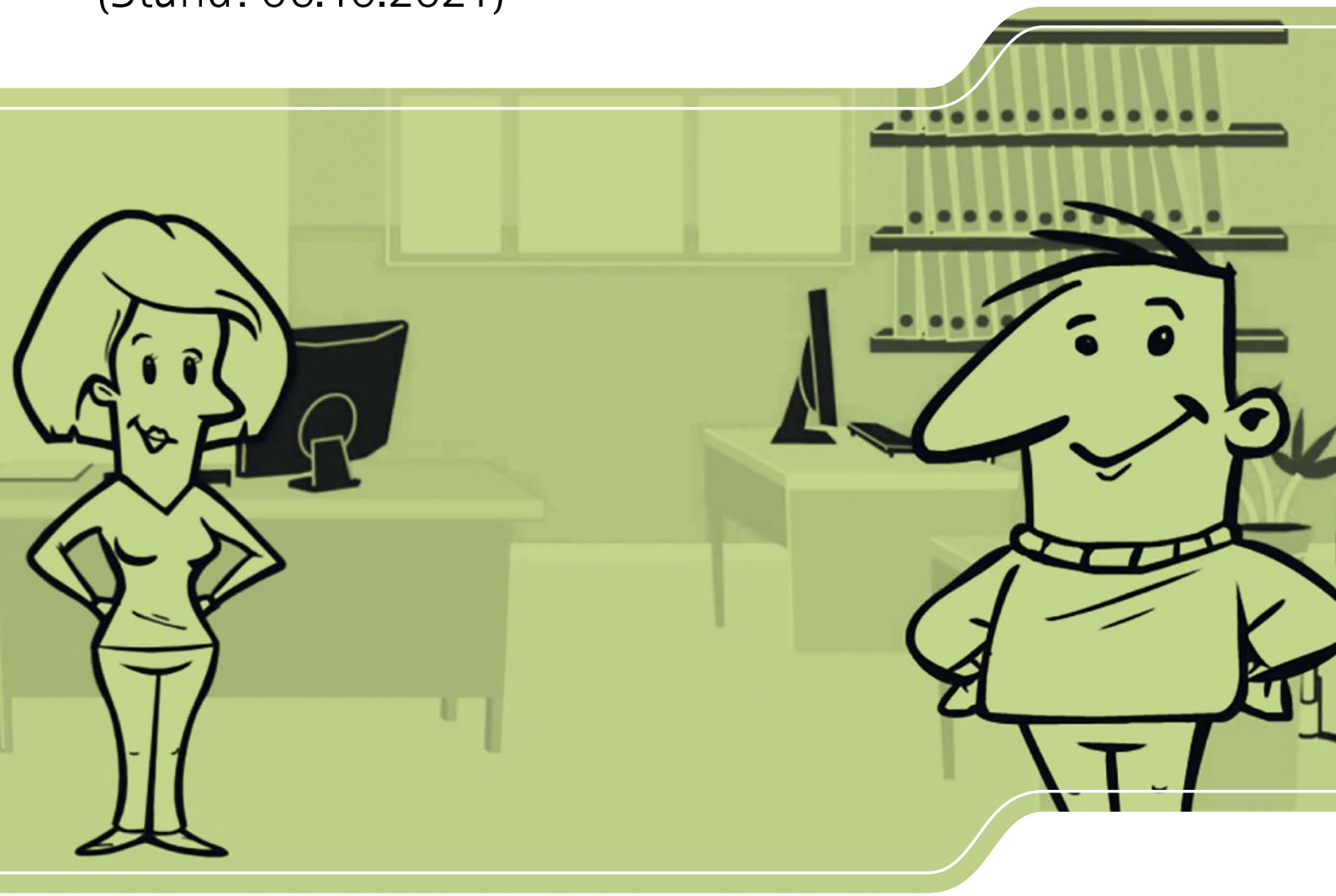
LANDESAMT FÜR
SCHULE UND BILDUNG

Freistaat
SACHSEN

Informationssicherheit an sächsischen Schulen

(Stand: 06.10.2021)



Vorwort

Sehr geehrte Damen und Herren,

spätestens seitdem wir uns in jeder Lebenslage und von allen Seiten mit der Datenschutzgrundverordnung (kurz DSGVO) konfrontiert sehen, ist allen an Schule Beteiligten klar: Lehrerinnen und Lehrer haben besonders schützenswerte Daten zu verwalten.

Die Broschüre zur »Informationssicherheit an sächsischen Schulen« versteht sich in diesem Zusammenhang als Maßnahme, die dem hohen Stellenwert der Informationssicherheit an Schulen Rechnung trägt und grundlegende Kenntnisse zum Datenschutz und zur Informationssicherheit vermittelt.

Auch wenn Beschaffung, Wartung, Pflege und Administration von informationsverarbeitenden Systemen in erster Linie in kommunaler Hand sind, müssen Sie sich dem Thema Informationssicherheit öffnen, um im Rahmen Ihrer Möglichkeiten zur Informationssicherheit beizutragen. Dabei gilt es, eigenes Handeln zu prüfen und an notwendigen Sicherheitszielen auszurichten.

In der Schule bedeutet das vor allem, die Sicherung vertraulicher schulischer Informationen und die Verhinderung unberechtigter Veränderung bzw. Erstellung solcher. Informieren Sie sich deshalb unter anderem über die Erstellung sicherer Passwörter, die Verschlüsselung von Datenträgern und Daten, die Verwendung von Virenscannern und Firewalls sowie Vorsichtsmaßnahmen beim Umgang mit E-Mails und in Sozialen Netzwerken.

Eine Auswahl spezifischer Maßnahmen soll dabei Risiken der IT-Nutzung minimieren und gleichzeitig garantieren, dass digitalisierte Arbeitsabläufe in der Schule sichergestellt werden und IT-Systeme, Anwendungen sowie Daten unversehrt bleiben und wie vorgesehen zur Verfügung stehen.

Die in der Broschüre gegebenen Empfehlungen für den Umgang mit sensiblen Daten einschließlich deren Verschlüsselung und Schutz vor Missbrauch und Verlust sind dabei eine sichere Handlungsgrundlage.

Bitte informieren Sie sich und nehmen Sie die Sache mit der Informationssicherheit ernst.

Ralf Berger
Präsident des Landesamtes für Schule und Bildung

Inhaltsverzeichnis

In sechs Kapiteln sollen wichtige Themen der Informationssicherheit und des Datenschutzes für Lehrerinnen und Lehrer in Sachsen bearbeitet werden. Es handelt sich dabei um die Themen **Passwortsicherheit, Verschlüsselung von Daten und Datenträgern, regelmäßige Datensicherung**, Umgang mit sicherer **E-Mail Kommunikation**, Verwendung von aktuellen **Virenscannern und Firewalls** sowie Bewusstsein für **Social-Engineering**-Fallen.

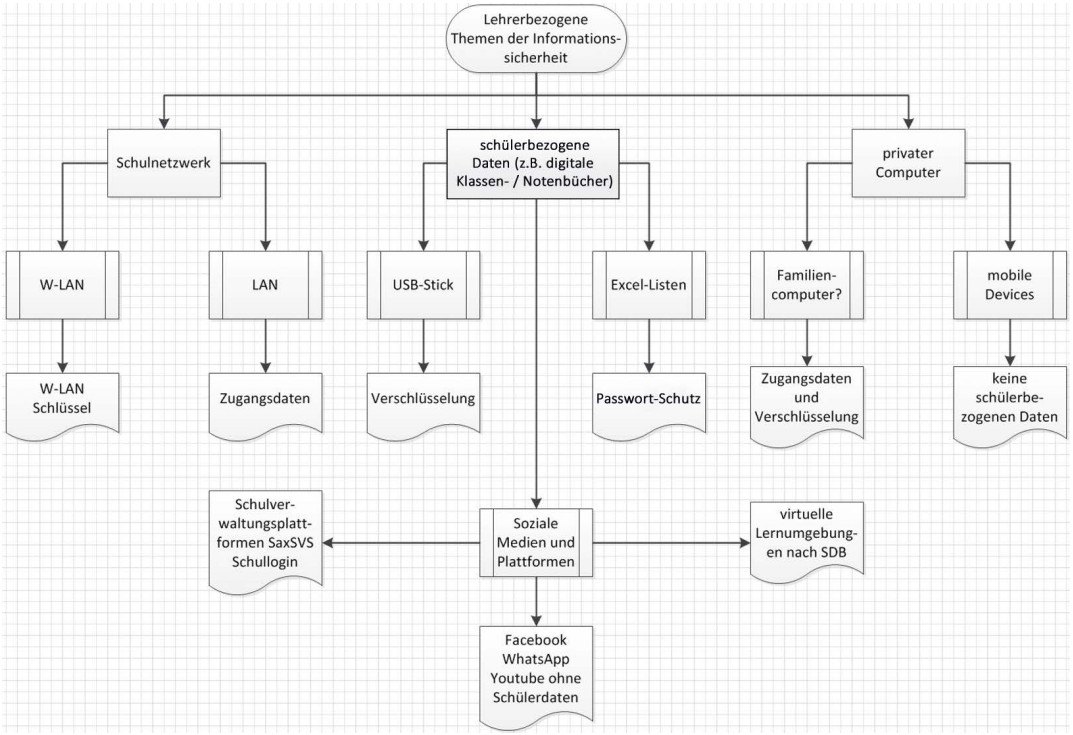

Meine Freundin und
Kollegin Petra und ich - Paul -
werden versuchen, die Fragen
rund um Datenschutz
und Informationssicherheit
zu beantworten ...

Informationssicherheit für Lehrerinnen und Lehrer an sächsischen Schulen – Einführung

Informationssicherheit, die der Sicherstellung von Verfügbarkeit, Integrität und Vertraulichkeit von Informationen dient, ist an Schulen unabdingbar.

Lehrkräfte haben in ihrer täglichen Arbeit immer mehr Anknüpfungspunkte mit Informationstechnologien. So müssen beispielsweise Schülerdaten und Datenträger verschlüsselt und Zugänge mit starken Passwörtern und ggf. zusätzlichen Faktoren wie Einmalpasswörtern geschützt werden. Das spielt nicht nur im Schulnetzwerk und in Schulclouds eine ganz entscheidende Rolle, sondern auch in den vom Land oder Schulträgern bereitgestellten Online-Anwendungen (Schullogin / LernSax / MeSax usw.).

Die abgebildete Grafik zeigt exemplarisch, an wie vielen Stellen Lehrerinnen und Lehrer Berührungspunkte mit Informationssicherheit und Datenschutz haben. Nicht immer ist Lehrkräften deutlich bewusst, wie groß die Verantwortung ist, die z. B. mit dem Umgang mit Schülerdaten verbunden ist.



Die Umsetzung der VwV Informationssicherheit SMK vom 27. Januar 2016 (SächsABl. S. 196), zuletzt enthalten in der Verwaltungsvorschrift vom 16. April 2021 (SächsABl. 2021 Nr. 15, S. 366)

→ *https://www.revosax.sachsen.de/vorschrift/19069-VwV-Informationssicherheit-SMF*

sowie der VwV Schuldatenschutz (11. Juli 2018)

→ *https://www.revosax.sachsen.de/vorschrift/17794-VwV-Schuldatenschutz*

spielen im schulischen Alltag eine wichtige Rolle beim Umgang mit schüler-bezogenen Daten.

Die vorliegende Broschüre soll den sächsischen Lehrkräften Sicherheit geben, mit den Anforderungen von Informationssicherheit und Datenschutz souverän umzugehen.

1. Passwortsicherheit

Das Thema Passwortsicherheit ist wohl eines der wichtigsten und am meisten besprochenen Themen der Informationssicherheit und des Datenschutzes. Es stellt eine Möglichkeit dar, den Zugriff auf Anwendungen und Daten zu regeln. In diesem Kapitel soll über die Benutzung von Passwörtern für die Verschlüsselung informiert werden. Was sind »schlechte Passwörter« und was sind »gute Passwörter«? Gibt es Alternativen zu Passwörtern und wie kann man sich Passwörter merken?

Stellen Sie sich diese typische Szene im Lehrerzimmer vor. Kommt Ihnen das nicht bekannt vor?

Paul: *Verflixt! Schon wieder Notenschluss. Ich muss die Fachnoten-Datei aktualisieren, damit das Zeugnisprogramm die aktuellen Daten hat. Ich habe sie bereits auf den USB-Stick kopiert, aber wo ist das Passwort? Hier nicht, hier auch nicht! Verflixt! Warum kann ich mir bloß das Passwort nicht merken?*

Petra: *Du hast das Passwort doch wohl nicht irgendwo notiert?*

Paul: *Aber klar doch! Wie soll ich mir das sonst alles merken?*

MERKE:

Je länger, desto besser. Ein gutes Passwort[1] sollte mindestens acht Zeichen lang sein und verschiedene Zeichengruppen enthalten.

Bei Verschlüsselungsverfahren für WLAN, wie z. B. WPA2 oder WPA3, sollte das Passwort beispielsweise mindestens 20 Zeichen lang sein. Hier sind so genannte Offline-Attacken möglich, die auch ohne stehende Netzverbindung funktionieren.

Ein starkes Passwort ist wichtig, damit es im Falle eines Angriffs nicht zu leicht »geknackt« werden kann. Beliebte Methoden von Hackern sind Angriffe mit Wörterbüchern. Moderne Computer können in Bruchteilen von Sekunden ganze Wörterbücher als mögliche Kombination für das Passwort abfragen. Auch die häufig genutzten Passwörter 123456 oder qwertz (Buchstabenreihe auf der Tastatur) sind natürlich nicht sicher, weil sie von einem Profi als Erstes getestet werden.

Passwörter aus alleinstehenden **Namen, Begriffen oder einfachen Kombinationen** sind also **schlechte Passwörter**, weil sie zu schnell zu knacken sind.

Auch wenn das Passwort aus beliebigen Buchstabenkombinationen besteht, ist das »Knacken« des Passwortes mit der Brute-Force-Methode einfach, wenn es zu wenige Zeichen enthält.

Brute-Force-Attacken sind Versuche eines Programms, das Passwort eines anderen Programms zu erraten, indem alle möglichen. Kombinationen von Buchstaben und Ziffern ausprobiert werden. Es ist offensichtlich, dass die Länge eines Passworts für die Sicherheit des Passwortes wichtig ist. Wenn dann noch Sonderzeichen zugelassen werden, ist die Zeichenbasis groß genug, um starke Passwörter zu generieren, die nicht unhandlich lang sein müssen.

Als Empfehlung hat sich die Methode eines **Passwort-Satzes** etabliert. Bekannt ist diese Methode bereits vielen durch die Eselsbrücke zu den Planeten:
So ist in dem Satz »Mein Vater erklärt mir jeden Samstag unseren Nachthimmel.« eine Codierung für die Reihenfolge der Planeten unseres Sonnensystems enthalten. Die Anfangsbuchstaben jedes Wortes bedeuten: Merkur, Venus, Erde, Mars, Jupiter, Saturn, Uranus, Neptun. Das Passwort, das sich aus diesem Satz ableiten ließe, wäre **MVemjSuN**.

[1] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Dieses Passwort enthält bereits Groß- und Kleinbuchstaben. Um nun noch Ziffern mit hinzuzunehmen, kann man typische Entsprechungen ersetzten: **MVe^^j5uN[2].**

[2] Hinweis: dieses Passwort bitte NICHT verwenden!

→ *https://de.wikipedia.org/wiki/Leetspeak*

Diese Methode funktioniert auch mit Zeilen aus dem Lieblingsgedicht und ähnlichen Sätzen.

Auch das beste Passwort nützt jedoch nichts, wenn jeder es kennt! Der größte Fehler im Zusammenhang mit Passwörtern ist das Aufschreiben derselben. Ein an den Bildschirm gehefteter Klebezettel mit dem Passwort ist für jedermann zugänglich und eine Einladung für jeden Hacker. Selbst wenn der Klebezettel nicht am Bildschirm haftet, sondern das Passwort irgendwo im Lehrerkalender notiert ist, ist auch das viel zu einfach zu missbrauchen. Leicht zu merkende, starke Passwörter müssen nicht notiert werden und es soll auch für jeden Account bzw. für jede Anwendung ein eigenes Passwort erstellt werden. Somit verhindert man, dass der Verlust eines Passwortes gleich alle Zugänge angreifbar macht.

MERKE:

- Nicht das gleiche Passwort für verschiedene Anwendungen verwenden.
- Passwörter nicht notieren.
- Passwörter nicht in einer unverschlüsselten Datei ablegen.
- Passwörter unbeobachtet eingeben.

Besonders wichtig ist, dass das Passwort von Dritten unbeobachtet eingegeben wird (z. B. Verzicht von On-ScreenKeyboards bei digitalen Tafeln für die Eingabe des Passwortes).

Mit dem Administrator-Passwort hat man erweiterte Rechte im Schulnetzwerk. Außerdem erlaubt die Anmeldung als Administrator die Installation von Software. Es ist also verlockend, sich als Administrator anzumelden. Die Gefahr des Missbrauchs durch Dritte ist jedoch zu hoch. Schon wenn man sich nur kurz vom Computer entfernt, ohne ihn zu sperren, können das Administrator-Passwort geändert oder Daten manipuliert werden. Die Schäden können irreparabel sein. Das gilt nicht nur für das Schulnetzwerk, sondern ebenfalls für Anmeldungen über Online-Plattformen wie zum Beispiel LernSax, MeSax, Schullogin oder OPAL-Schule. Gerade bei Anmeldungen über Online-Plattformen gibt es häufig die Möglichkeit, das Passwort sichtbar zu machen (Augen-Symbol bei der Passwort-Eingabe). Wenn der Beamer bereits gestartet und das Augensymbol aktiviert ist, dann ist die Eingabe des Passwortes für jeden sichtbar. Gleiches gilt für die Passworteingabe über die Bildschirmtastatur der interaktiven Tafel. Manche Browser bieten an, Passwörter und Online-Zugänge zu speichern. Passwortmanager in Browsern sollten durch Masterpasswörter geschützt werden.

Wer befürchtet, den Überblick über seine Passwörter zu verlieren, kann dafür einen Passwort-Manager nutzen. Das ist ein Programm, das Benutzernamen und Passwörter verwaltet. Mit Verschlüsselung und komplexem Masterpasswort werden die Passwörter sicher verwahrt. Anstatt sich viele verschiedene Passwörter zu merken, muss man nur noch eins im Kopf behalten.

[3] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html;jsessionid=0523F540DD4C480C2D2709474D11BECE.internet461

Nähere Hinweise zum Passwortmanager als technisches Hilfsmittel finden sich auf der Website des BSI.[3]

Wenn möglich aktivieren Sie für die Anmeldung noch einen zweiten Faktor, wie z.B. die aus dem Online-Banking bekannte TAN.

MERKE:

- Niemals mit dem Administrator-Passwort im normalen Schulbetrieb anmelden.
- Keine Zugangsdaten im Klartext auf Computern speichern.

2. Datenträger/ Daten verschlüsseln

Im zweiten Kapitel wird auf ein Grundproblem beim Transport von schülerbezogenen Daten eingegangen – dem Sichern von Daten auf USB-Sticks oder externen Festplatten.

Das kann im Lehrerzimmer passieren:

Paul: *Oh, Mann! Wo ist mein USB-Stick? Gestern habe ich endlich alle Noten in die Listen eingetragen und nun ist der Stick weg …*

Petra: *Halb so schlimm. Du hast die Daten doch ge-Back-up-t!? Na, und wenn jemand den Stick findet, dann kann er damit nichts anfangen – er ist doch verschlüsselt???*

Paul: *Back-up? Verschlüsselt? Wovon redest Du??? Mein USB-Stick ist WEG!!!*

Petra: *… aber wenn jemand Fremdes den Stick findet …?*

Die Notenlisten von Schülern oder Klassen sind schützenswerte persönliche Daten. Diese dürfen unter keinen Umständen Dritten zugänglich gemacht werden, ob gewollt oder ungewollt. Deshalb dürfen solche Informationen niemals auf privaten Datenträgern transportiert werden. Für den Transport von Schülerdaten auf externen Speichermedien gibt die VwV Schuldatenschutz explizit Hinweise:

VwV Schuldatenschutz
(Fassung gültig ab: 11. Juli 2018
(MBl.SMK S. 282))
Ziffer III. **Organisatorische und technische Maßnahmen**

»6. Umgang mit mobilen Datenträgern

a) Mobile Datenträger, beispielsweise CDs, DVDs, mobile Festplatten, USB-Sticks oder SD-Cards, sind so aufzubewahren, dass Unbefugte nicht auf gespeicherte personenbezogene Daten zugreifen können.

b) Soweit personenbezogene Daten auf mobilen Datenträgern gespeichert werden, sind sie zu verschlüsseln und zusätzlich [ist die Datei] mit einem Passwortschutz zu versehen. Etwaige Sicherungskopien sind verschlossen beim Schulleiter aufzubewahren.«

→ *https://www.revosax.sachsen.de/vorschrift/17794#vwv6*

Das heißt konkret, dass schülerbezogene Daten grundsätzlich so aufzubewahren sind, dass unautorisierte Personen keinen Zugriff erhalten. Wenn personenbezogene Daten auf mobilen Datenträgern gespeichert werden, sind diese mit Passwortschutz und Verschlüsselung zu versehen.

Ein hohes Maß an Datensicherheit ermöglichen für alle Systeme im Handel erhältliche, hardwareverschlüsselte USB-Sticks. Mit integrierter Tastatur zum Entsperren benötigen diese USB-Sticks mit wenigen Ausnahmen weder Treiber noch zusätzliche Software. Lassen Sie sich dazu von ihrem IT Team beraten und achten Sie auf Zertifizierung, AES-256 oder vergleichbare Verschlüsselung.

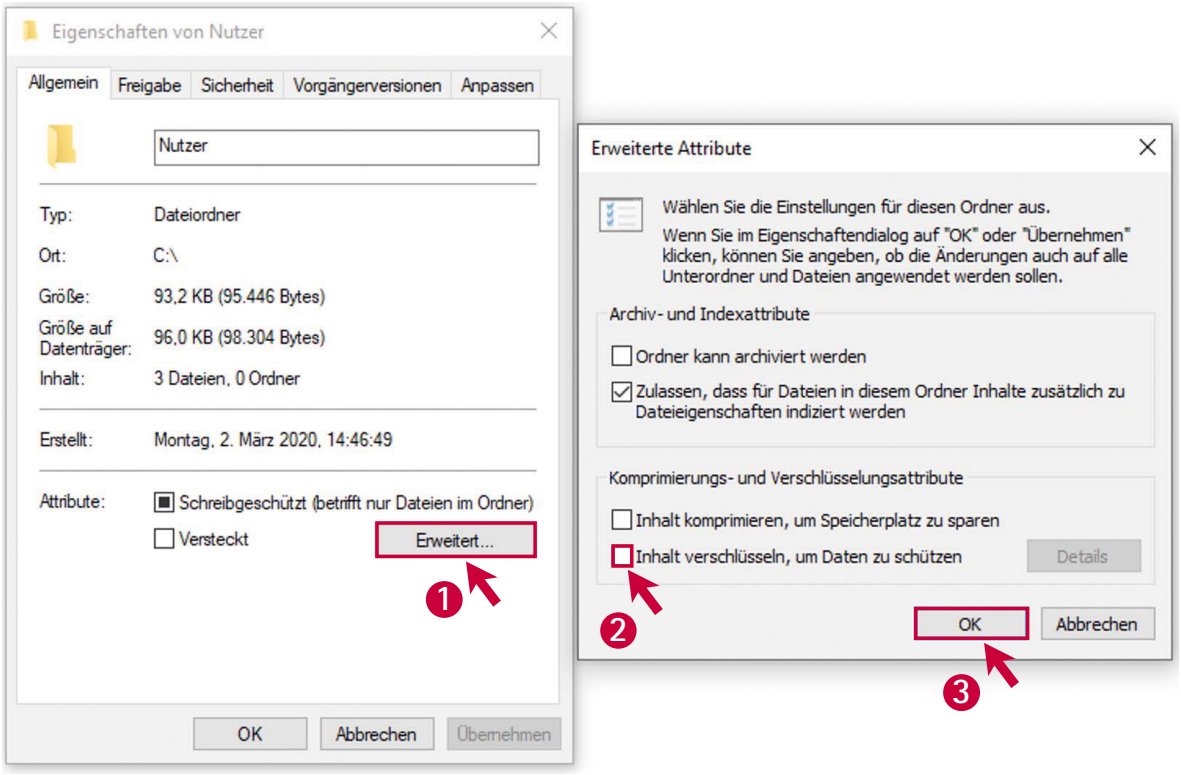
Verschlüsselung bedeutet, dass die Daten ohne einen digitalen Schlüssel nicht ohne Weiteres lesbar sind.

Zum Entschlüsseln können nun je nach Verschlüsselung verschiedene Möglichkeiten genutzt werden: Passworteingaben, Chipkarten (siehe auch Hinweise des BSI[4]).

[4] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datenverschluesselung/datenverschluesselung_node.html

Eine Variante, Ordner oder Laufwerke anhand der Nutzeranmeldung zu verschlüsseln, bietet Windows bereits in den erweiterten Eigenschaften dieser Ordner, wenn das Verschlüsselungsverfahren Bitlocker zur Verfügung steht (nicht in Windows 10 Home Edition).

Der verschlüsselte Ordner / die verschlüsselten Dateien sind dann nur noch mit dem Benutzerkonto zugänglich, von dem aus verschlüsselt wurde.



MERKE:

Der **Passwortschutz** ist für einzelne Dateien (z. B. WORD- oder Excel-Dateien ab Microsoft Office 2007) eine geeignete Option, Informationen zu sichern.

Bei Dokumenten des MS-Office-Paketes beispielsweise ist diese Option bereits integriert. Die Passwörter sollte mindestens 20 Zeichen oder mehr enthalten und die geschützte Datei im Format XLSX und DOCX, PPTX gespeichert werden.

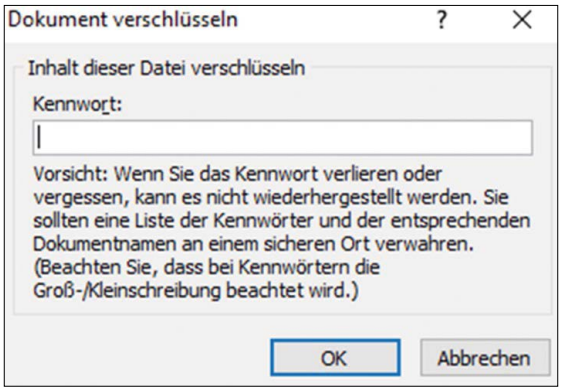
Dabei kann wie folgt vorgegangen werden:

Word-Datei: Datei –> Informationen –> Dokument schützen –>
Mit Kennwort verschlüsseln

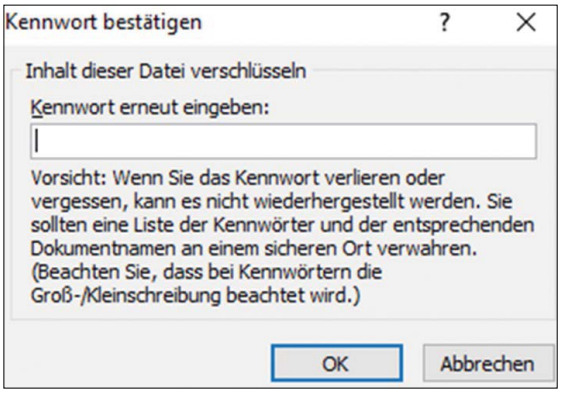
Analog geht man vor, um eine Excel-Datei zu verschlüsseln:

Excel-Datei: Datei –> Informationen –> Arbeitsmappe schützen –>
Mit Kennwort verschlüsseln.

Es öffnet sich folgendes Dialogfenster:

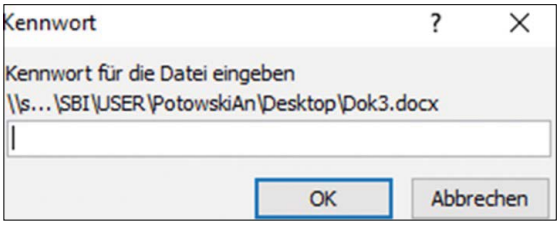


Geben Sie im Dialogfeld Kennwort das Kennwort erneut ein, das Sie im vorherigen Schritt eingegeben haben.



Die doppelte Abfrage des Passwortes dient dabei dem Schutz vor einer Falscheingabe.

Wenn Sie oder ein anderer Benutzer versuchen, die Datei zu öffnen, wird folgender Bildschirm angezeigt:



MERKE:

Dokumente des MS-Office-Paketes lassen sich über die Dokumenteninformationen mit einem Passwort schützen.

Hier kann nun mit dem zuvor eingegebenen Passwort das Dokument geöffnet werden und der Zugriff auf die Informationen steht wieder zur Verfügung.

Um sensible Daten noch besser zu schützen, ist es möglich, diese mit entsprechenden Programmen zu verschlüsseln.

Betriebssystemeigene Tools für die Verschlüsselung sind dabei z. B. Bitlocker (ab Version Pro Bitlocker) für Windows, FileVault für Mac und Luks für Linux. Zu empfehlen ist auch die eigenständige Anwendung Veracrypt.

→ *https://www.veracrypt.fr/en/Downloads.html*

Die Verschlüsselung von Dokumenten und Laufwerken ist auch mit weiteren Werkzeugen oder PortableApps möglich. Nähere Hinweise dazu finden sich auf diversen Webportalen zum Verschlüsseln von Laufwerken und USB-Sticks.

3. Daten regelmäßig sichern

Im dritten Kapitel wird auf die Sicherung von (schülerbezogenen und schulbezogenen) Daten und allgemein das Sichern von Dateien auf USB-Sticks oder anderen externen Speichern eingegangen.

Auch die folgende Szene aus dem Lehrerzimmer dürfte jeder kennen:

Paul: Hört mal! Gestern ist mein Windows abgestürzt und lässt sich nicht mehr starten. Wenn ich das jetzt neu installiere oder einen neuen Computer brauche, sind doch alle meine Daten weg, oder?

Petra: Nicht unbedingt! Wenn du die Daten ge-»Back-up«-t hast, kannst du nach der Neu-Installation des Betriebs-systems die Back-ups wieder einspielen. Das klappt auch mit einem neuen Computer …

Paul: Ich habe aber kein Back-up!!!

Petra: Tja, dann kommt jetzt eine Menge Arbeit auf dich zu …

Die regelmäßige Sicherung von Daten soll vor Datenverlust schützen. Das betrifft sowohl einzelne Dateien als auch ganze Laufwerke –also Datenträger. Für Dateien wie auch Datenträger gilt, dass ein regel-mäßiges Back-up der beste Schutz vor Datenverlusten ist. Als Back-up bezeichnet man dabei eine Sicherheitskopie, mit deren Hilfe die gespeicherten Daten im Fall eines Systemausfalls bzw. eines Datenverlustes zurückkopiert und wiederhergestellt werden können. Die Kopie kann auf einer Festplatte oder auf einem USB-Stick oder auch online erstellt werden. Bestimmte Programme helfen dabei, diese Aufgaben regelmäßig zu erledigen. Im Folgenden werden diese drei Wege konkreter vorgestellt.

Sicherung auf der Festplatte

Bei der Sicherung von Daten auf der Festplatte wird gewöhnlich ein Ordner »Back-up« angelegt und Kopien von wichtigen Dokumenten darin gespeichert. Bei vielen zu sichernden Dateien aus verschiedenen Ordnern kann das schnell unübersichtlich werden. Außerdem besteht die Gefahr, bei einem technischen Defekt nicht nur die Originale, sondern auch die Back-up-Dateien zu verlieren.

MERKE:

Ein Back-up auf demselben Laufwerk wie das Original ist besser als gar kein Back-up, bietet aber keinen Schutz vor Datenverlust.

Sicherung auf USB-Stick/externer Festplatte

Sicherer ist daher der Weg über eine externe Festplatte oder aber einen USB-Stick. In bestimmten Abständen werden alle wichtigen Daten auf einen entsprechenden externen Datenträger überspielt. Das hat den Vorteil, dass bei Datenverlust auf dem Original-Datenträger die Daten auf dem Back-up-Datenträger noch intakt sind und wiederhergestellt werden können, wenn der externe Datenträger nicht dauerhaft am zu sichernden Rechner angeschlossen ist.

MERKE:

Ein Back-up auf einem externen Laufwerk, welches nach der Erstellung separat, getrennt vom Strom und Rechnern, in einem vor Brand oder Diebstahl gesicherten Bereich gelagert wird, bietet hohen Schutz vor Datenverlusten.

Sicherung der Daten online

Die Sicherung von schützenswerten Daten online (z. B. in Cloud-Diensten) hat ebenfalls Vor- und Nachteile. Viele Online-Dienste bieten keine Gewähr für eine datenschutzkonforme und werbefreie Bereitstellung aller Funktionen ohne geschäftliche Interessen und sind deshalb für schützenswerte Daten (z. B. Schülerdaten) nicht zugelassen. Sächsische datenschutzkonforme Alternativen sind die Dateiablagen von **LernSax** oder **Schullogin**. Auch dort abgelegte Daten können zusätzlich via BoxCrpytor oder encFS verschlüsselt werden. Damit haben auch die Betreiber keine Einsicht in die Daten.

→ *https://www.revosax.sachsen.de/vorschrift/17794-VwV-Schuldatenschutz*

Möchte man ganze Datenträger als Back-up sichern, bietet sich eine externe Festplatte an. Auch NAS-Laufwerke (Network Attached Storage, englisch für netzgebundene Speicher) eignen sich hierfür und können dezentral aufgestellt werden. Die Vorgehensweise entspricht der eben beschriebenen für das Back-up von einzelnen Daten/Ordnern. Man wählt lediglich den Pfad des zu sichernden Laufwerkes als Original und ein anderes Laufwerk als Back-up. Manche Tools bieten die Möglichkeit, zwei Laufwerke oder zwei Ordner zu synchronisieren, d. h. egal in welchem der beiden Ordner sich etwas ändert, die Änderung wird in beiden Ordnern identisch gehalten.

Im schulischen Umfeld haben sich Festplattenschutzprogramme bewährt, die einen funktionsfähigen Stand der Arbeitsumgebung »einfrieren« und bei jedem Neustart abrufen. Egal, was der Nutzer vorher geändert hat, die Änderungen sind nach dem Neustart hinfällig. Das System kann also nicht »kaputtgespielt« werden

In kürzester Zeit und ohne menschliches Eingreifen wird mit jedem Neustart der stabile Originalzustand wieder hergestellt.

Trotzdem ist ein Back-up nicht entbehrlich, da es immer auch technische Ausfälle von Festplatte o. ä. geben kann. Ein Mehrgenerationenbackup, d. h. mehrere getrennte Backups zu unterschiedlichen Zeiten, sichert verschiedene Arbeitsstände und beugt Datenverlust vor.

MERKE:

Auch bei der Verwendung von Festplattenschutzprogrammen ist eine Sicherung von schützenswerten Daten als Back-up notwendig.

4. Sichere E-Mail-Kommunikation

Das vierte Kapitel – rund um E-Mails – ist von besonderer Wichtigkeit, weil niemand um die Notwendigkeit herumkommt, Mails zu empfangen und zu senden. Außerdem ist das Angriffspotenzial bei E-Mail-Anhängen beträchtlich.

Hört selbst! Gestern im Lehrerzimmer:

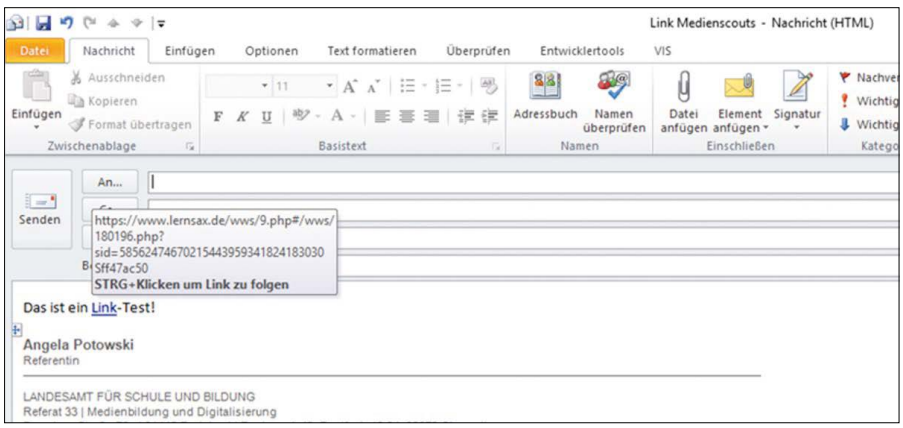
Paul: *Mein Gott, was ist nun wieder los … Gestern habe ich eine E-Mail bekommen und will gerade lesen, wie ich ganz schnell ganz reich werden kann, und plötzlich wird der Bildschirm dunkel und ich soll meine Bankverbindungsdaten eingeben. Hatte ich aber gerade nicht zur Hand. So ein Pech!*

Petra: *So ein Pech? Du meinst wohl eher: So ein Glück!!! Wenn du deine Kontodaten eingegeben hättest, wärest du heute bestimmt nicht reicher, sondern ärmer.*

Paul: *Wieso?*

Wie in der kurzen Szene beschrieben, lauern tatsächlich einige Gefahren gerade im Umgang mit E-Mails. Schon im Text einer E-Mail können sie sich verbergen. Noch schlimmer wird es bei Hyperlinks (kurz: Links) oder Anhängen, die geöffnet werden sollen. Das Problem bei Links im E-Mail-Text besteht darin, dass die eigentliche URL (Ziel-Adresse im Internet) nicht zu sehen ist und die aufzurufende Webseite nicht immer der entspricht, die der Link vorgaukelt zu sein. Wenn z. B. in einer »Mahn-Mail« einer Bank die Eingabe von persönlichen Daten über eine Webseite unter dem angegebenen Link gefordert wird, gelangt man mit Sicherheit nicht auf die Bank-Webseite, sondern auf eine mehr oder weniger geschickt gefälschte Kopie dieser Bank-Webseite. Gibt man hier nun tatsächlich seine Zugangsdaten ein, hat ein Krimineller diese Zugangsdaten »abgefischt« und kann jetzt nach Belieben Überweisungen tätigen oder Ähnliches.

Die Zieladresse eines Links erfährt man durch die Mouse-Over-Funktion, d. h. dass man mit der Maus **ohne zu klicken** über den Link fährt und so das Ziel angezeigt bekommt:



Das **»s«** am Ende von **https://**... steht bereits für eine gesicherte Internet-Adresse, d. h. alle eingegebenen Daten werden verschlüsselt **übertragen.**

TIPP:

Öffnen Sie keine Links aus Mails von Banken etc. Geben Sie die URL der Bank immer von Hand ein, oder nutzen Sie ein Lesezeichen im Browser. Prüfen Sie den Zertifikatsinhaber bei Unsicherheiten im Browser, bevor Sie personenbezogene Daten eingeben. Fragen Sie im Zweifel beim Absender über einen anderen Weg (z. B. bekannte Telefonnummer) nach, ob die Mail wirklich vom Absender stammt.

Aber Vorsicht, gefälschte Adressen können z. T. sehr ähnlich aussehen wie die Originale. Das gilt ebenso für die gefälschten Webseiten. Hat man einen gefälschten Link oder einen Anhang mit Schadsoftware erst einmal geöffnet, fangen die Probleme meistens schnell an.

Phishing: Das Wort setzt sich aus »Password« und »Fishing« zusammen, zu Deutsch »nach Passwörtern angeln«. Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen.

Folgende Auswahl von Schädlingen[5], Verschlüsselungstrojanern und Viren können den Computer befallen haben:

[5] https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_node.html

Trojaner: Ein Trojanisches Pferd, oft auch kurz Trojaner genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein Trojaner verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

Virus: Klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann (keine Schadfunktion bis hin zum Löschen der Daten auf einer Festplatte). Viren treten in Kombination mit einem Wirt auf, z. B. einem infizierten Dokument oder Programm.

Wurm: Bei (Computer-, Internet-, E-Mail-) Würmern handelt es sich um Schadsoftware, ähnlich einem Virus, die sich selbst reproduzieren und sich durch Ausnutzung der Kommunikationsschnittstellen selbstständig verbreiten.

Wenn einem eine E-Mail bereits im Posteingang suspekt vorkommt, sollte man sie zunächst nicht öffnen. Zumindest sollte man sich über die folgenden drei Punkte Gedanken machen:

ERST DENKEN – DANN KLICKEN!

- Ist der Absender bekannt und stimmt die angezeigte Mail-Adresse?
- Sind Betreff und Text der E-Mail sinnvoll?
- Wird vom Absender ein Anhang erwartet?

Da Phisher und Spammer immer häufiger mit Spearphishing Attacken[6] unterwegs sind, werden in den Mails sogar passende bzw. korrekte Anreden genutzt.

[6] https://www.kaspersky.de/resource-center/definitions/spear-phishing

Im Zweifelsfall sollte man lieber telefonisch beim Absender nachfragen, ob E-Mail und Anhang wirklich von ihm sind. Offensichtliche Rechtschreibe- oder Ausdrucksfehler in »offiziellen« Schreiben, kryptische Hyperlinks oder falsche Kombinationen von bekannten Absendern und unbekannten Telefonnummern etc. sind ziemlich sichere Anzeichen für gefälschte E-Mails, die Schadsoftware enthalten können.

Wirkliche Sicherheit bei der Kommunikation per E-Mail gelingt mit folgenden Tipps: Für eine **Ende-zu-Ende-Verschlüsselung** des E-Mail-Verkehrs gibt es zwei Standards, S/MIME und OpenPGP. Sender und Empfänger müssen denselben Standard verwenden. Einigen Sie sich in Ihrer Schule auf ein Verfahren, das Sie zur Verschlüsselung von E-Mails einsetzen möchten und kommunizieren Sie dies in der Nutzergruppe.

MERKE:

Ein Mailprogramm sollte immer aktuell sein, damit die Angriffsfläche für Schädlinge gering ist.

Die Ver- und Entschlüsselung beruht immer auf einem Schlüsselpaar von öffentlichem und privatem Schlüssel. Die Erzeugung eines solchen Schlüsselpaares zur Zertifizierung der eigenen E-Mail-Adresse benötigt beim Standard S/MIME einen entsprechenden Anbieter. Anschließend wird der öffentliche Schlüssel allen Kommunikationspartnern zur Verfügung gestellt bzw. mit ihnen getauscht.

Das Fraunhofer SIT bietet die **Volksverschlüsselung** (basiert auf S/MIME) als einfache Alternative für Mail-Programme (wie z. B. Outlook), Browser und andere Anwendungen an:

→ *https://volksverschluesselung.de/index.php*

GPG (GNU Privacy Guard) ist ein freies Kryptographiesystem. Es dient zum Ver- und Entschlüsseln von Daten sowie zum Erzeugen und Prüfen elektronischer Signaturen.

Das Tool **Mailvelope** setzt diesen Standard für Browser (FireFox und Chrome) um:

→ *https://www.mailvelope.com/de/help*

Das vom BSI für Bürger empfohlene Verschlüsselungsprogramm **Gpg4win** zeichnet sich durch eine integrierte Schlüssel-Paar-Generierung mittels seiner Komponente **Kleopatra** aus[7]:

→ *https://www.gpg4win.de*

Für MacOSX wird das Verschlüsselungsprogramm **GPG Tools** empfohlen:

→ *https://gpgtools.org/*

Hinweis: in Mozilla Thunderbird sind die beiden Verschlüsselungstechnologien **OpenPGP** und **S/MIME** bereits integriert:

→ *https://support.mozilla.org/de/kb/openpgp-in-thunderbird-leitfaden-und-faqs#w_unterstutzt-thunderbird-openpgp*

Die oben genannten Tools geben dem E-Mail-Verkehr bereits eine beachtliche Sicherheit. Doch was passiert, wenn man sich in ein offenes WLAN einloggt, z. B. um seine E-Mails zu checken?

Wichtig ist bei der Einrichtung eines Mail-Accounts, vertrauenswürdige Rechentechnik vorausgesetzt, die Einstellung einer Verschlüsselung über SSL/TLS. Damit wird die Datenverbindung über das Internet abgesichert.

Zusätzlich hilft ein VPN (Virtual Private Network), sozusagen ein »privater Tunnel« im Internet vom Sender zum Empfänger. Die VPN-Verschlüsselung[8] garantiert eine sichere Kommunikation weltweit. Leider ist die Einrichtung und Verwendung von VPN nicht trivial und zumeist auch nicht kostenfrei.

MERKE:

Das blinde Öffnen von Anhängen oder Links in E-Mails kann Schadsoftware auf den Computer bringen. Mit dem Prinzip **»Erst denken – dann klicken!«** kann man sich viel Ärger ersparen.

Mehr Sicherheit bieten E-Mail-Tools mit **Ende-zu-Ende-Verschlüsselung** wie z. B. GPG und ein **Virtuelles Privates Netzwerk.**

7 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/E-Mail-Verschluesselung-in-der-Praxis/e-mail-verschluesselung-in-der-praxis.html

8 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/Virtual-Private-Networks-VPN/virtual-private-networks-vpn_node.html

5. Verwendung aktueller Virenscanner/Firewalls

Das fünfte Kapitel gehört ganz den Virenscannern und Firewalls.

Petra und Paul haben sich gestern wieder im Lehrerzimmer getroffen:

Paul: Ich musste Klaus aus der 10b heute wieder ermahnen. Da hat er doch glatt gekontert und gesagt, ich solle lieber auf die Daten auf meinem Rechner aufpassen, sonst verschlüsselt womöglich ein Virus ganz zufällig meine Festplatte …

Kann der das?

Petra: Was meinst du? Ist dein Rechner durch eine Firewall geschützt? Ist dein Virenscanner aktuell?

Paul: Firewall? Virenscanner? Wie meinst du das???

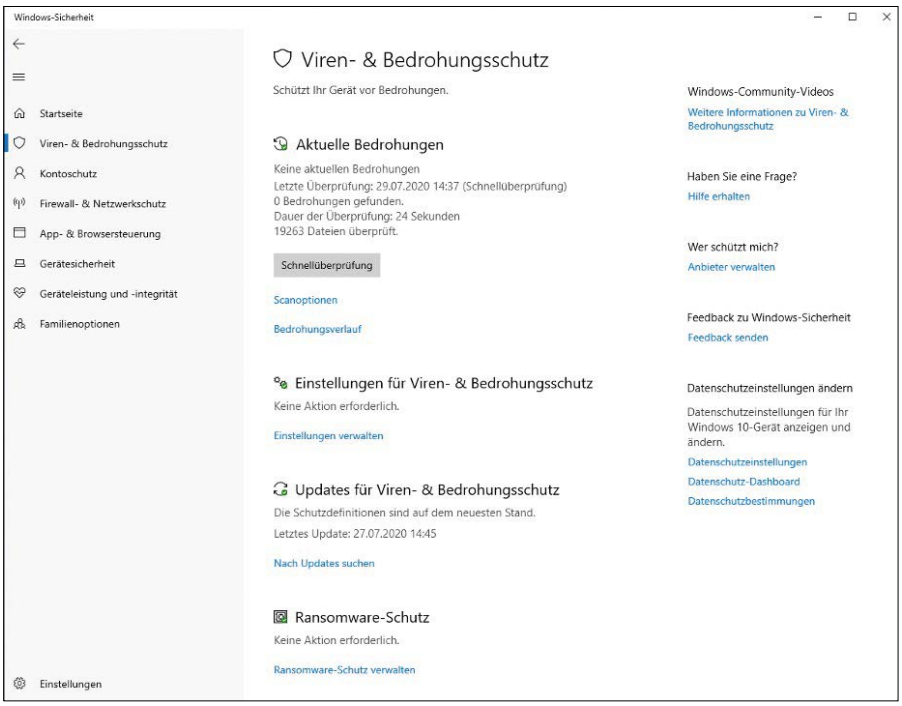
Auch in dieser kurzen Szene sieht man wieder, dass sich längst noch nicht alle Lehrerinnen und Lehrer ihrer Verantwortung beim Schutz von schützenswerten Daten, ob schulisch oder privat, bewusst sind. Virenscanner und Firewalls sind dabei unverzichtbar, arbeiten aber nur optimal, wenn alle eingesetzten Softwarekomponenten aktuell sind, d. h. Updates zeitnah gemacht werden.

Was sind **Virenscanner** und **Firewalls**?

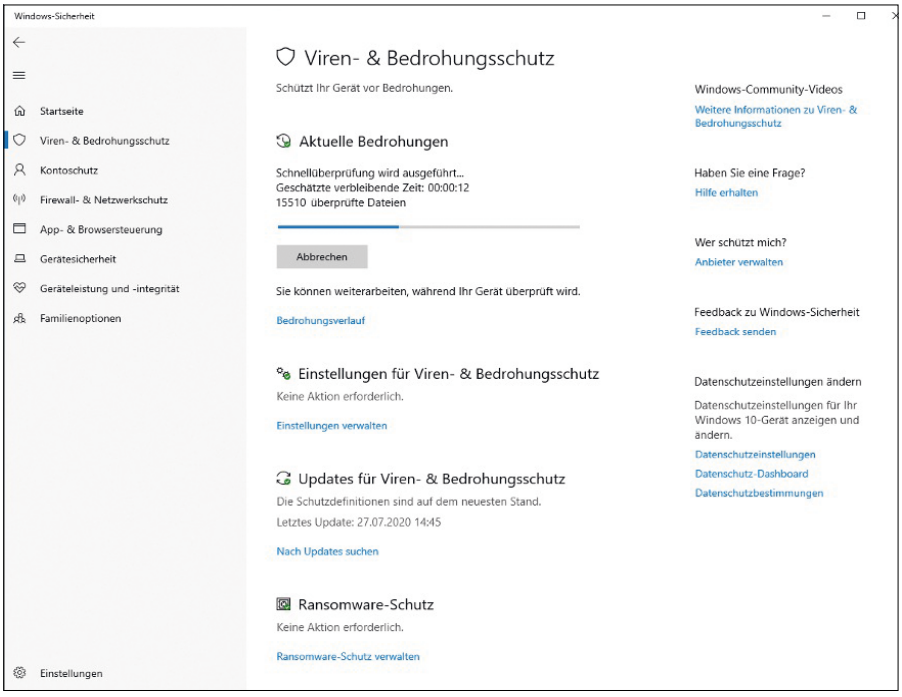
Anti-Viren-Programme – kurz Virenscanner genannt – sind Programme (sogenannte Tools), die nur eine spezielle Aufgabe haben: Sie sollen den Computer zuverlässig vor Viren schützen. Dabei überwachen sie im Hintergrund alle Wege, auf denen Informationen (Daten oder Dateien) auf den Rechner gelangen: Wechseldatenträger, E-Mail-Programme und Internetverbindungen. Je nach Einstellung warnen sie vor Problemen oder lösen sie gleich selbst, z. B. indem sie Angriffe abwehren.

Solche Anti-Viren-Programme kann man für viel Geld kaufen, aber jedes Betriebssystem hat auch On-Board-Mittel, sprich eigene Anti-Viren-Programme. Unter Windows 10 beispielsweise findet man in der Systemsteuerung den Punkt Windows-Defender. Dahinter verbirgt sich ein Anti-Viren-Programm, das von Microsoft speziell für Windows entwickelt wurde.

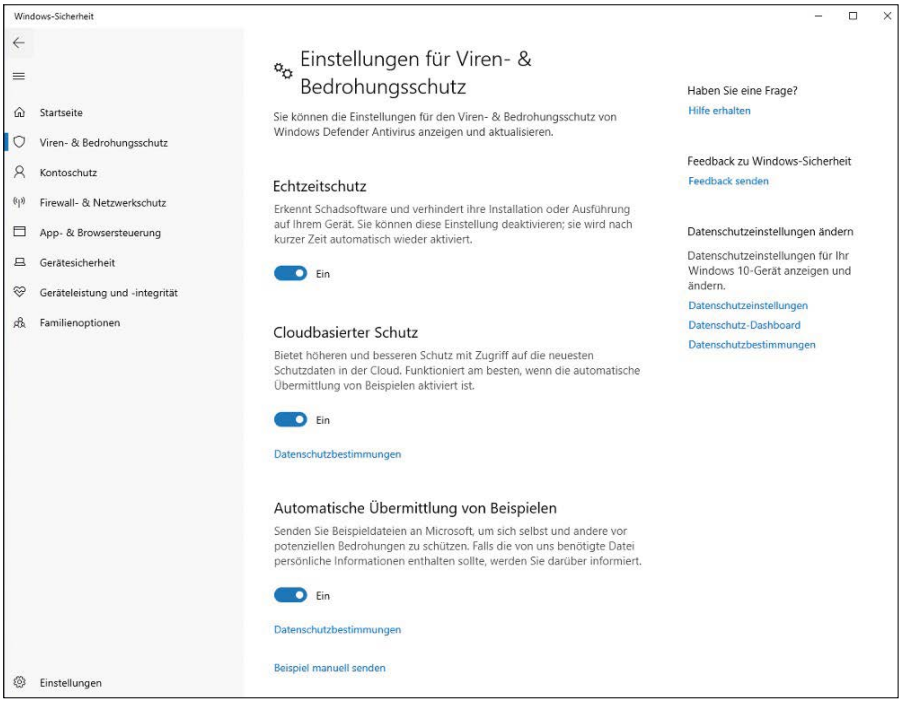
Nach dem Aktivieren dieses Programms erfolgt standardmäßig eine Aktualisierung der Viren-Definitionen, damit es auch alle neuen Computer-Viren erkennt und nicht nur die, die zum Zeitpunkt der Programmentwicklung bekannt waren. Danach kann eine erste Überprüfung gestartet werden:



Im besten Fall wird erkannt, dass keine unerwünschte oder schädliche Software ermittelt werden konnte:



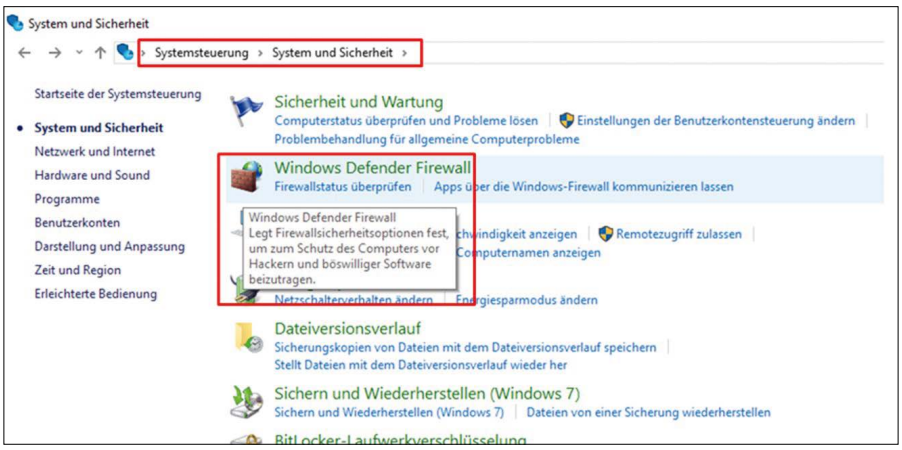
Anderenfalls bietet das Programm Optionen an, den Schädling zu entfernen. Empfehlenswert ist auf alle Fälle unter dem Menüpunkt »Extras« die Option »Echtzeitschutz aktivieren« auszuwählen, damit ein ständiger Schutz gewährleistet ist:



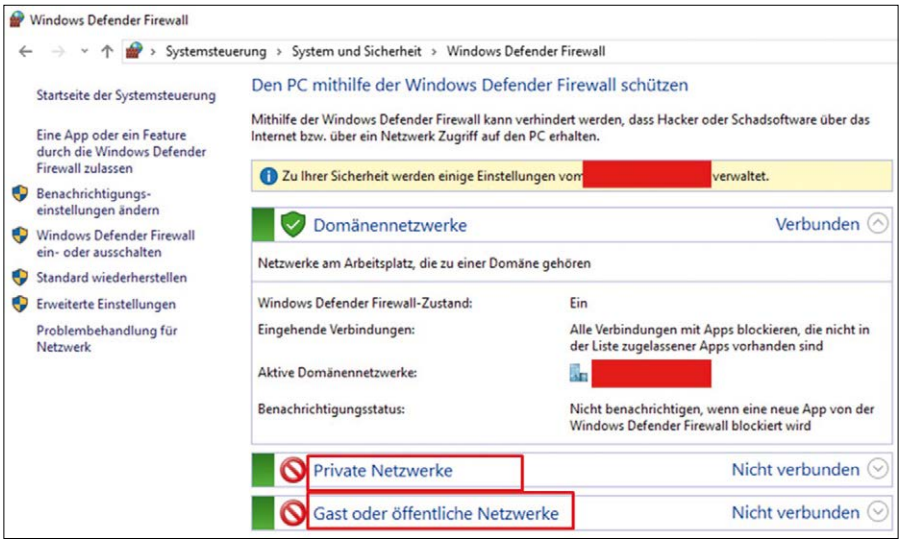
Auch für MacOS und andere Betriebssysteme sind Virenscanner erhältlich. Hersteller bieten Virenscanner zur kostenlosen Nutzung oder zum Kauf an, mit dem Versprechen höherer Sicherheit und/oder leichterer Bedienbarkeit, aber das muss letztendlich der Nutzer selber entscheiden.

Das andere Werkzeug zur Verbesserung der Sicherheit eines Computers ist die Firewall. Dabei wird unterschieden zwischen einer »Personal Firewall« auf dem Computer und einer Firewall des Netzwerkrouters. Eine Firewall analysiert den Datenverkehr im Netz und kann damit Server, PCs und Netzwerke vor Angriffen schützen. Auch nicht genehmigte Zugriffe - unabhängig vom Browser oder E-Mail-Programm - werden überwacht und z. B. Hackerattacken in den Logdaten registriert und blockiert bzw. unterbunden.

Bei Windows findet man die auf das Betriebssystem zugeschnittene Lösung in der **Systemsteuerung** unter dem Menü-Punkt **Windows-Firewall**:



Nach der Aktivierung der Windows-Firewall kann man diese beliebig ein- und ausschalten:



Die Windows-Firewall[9] ist eine einfache, sichere Lösung, Microsoft selbst spricht von einer »abgesperrten Haustür«, die guten Schutz vor Eindringlingen bietet. Kostenpflichtige Firewalls bieten in aller Regel wesentlich mehr Einstellungsmöglichkeiten, die dem Nutzer eine exaktere Definition ermöglichen, Ports zu öffnen oder zu schließen. Diese Vielzahl von Einstellungsmöglichkeiten kann Laien jedoch überfordern und falsch eingestellte Firewalls können Angriffsmöglichkeiten für Hacker bieten und die korrekte Funktion der Firewall oder des Rechners verhindern.

Auch andere Anbieter bieten kostenlose Lösungen für ihr jeweiliges Betriebssystem an, um den Schutz von Daten und Informationen sicherstellen zu können. Regelmäßige Updates von Virenscanner und Firewall werden durch die Voreinstellungen abgesichert und sollten auf alle Fälle zugelassen werden. Nur aktuelle Programme können ihre Aufgabe zuverlässig erfüllen.

[9] http://www.was-ist-malware.de/firewalls/was-du-ueber-die-windows-firewall-wissen-musst/

4-PUNKTE-PLAN FÜR EINEN GUTEN VIRENSCHUTZ[10]

1. Halten Sie Ihre Software und Ihr Betriebssystem auf dem aktuellsten Stand. Installieren Sie zeitnah neue Service Packs und Sicherheitsupdates.
2. Seien Sie aufmerksam beim Umgang mit E-Mails. Öffnen Sie keine unbekannten oder unerwarteten Dateianhänge und nehmen Sie sich in Acht vor Phishing-Mails.
3. Verwenden Sie ein aktuelles Antivirenprogramm und halten die Virendefinition stets aktuell.
4. Verwenden Sie eine Firewall, die den Netzwerkverkehr überwacht.

[10] Hinweis: es wird empfohlen, die Anti-Viren-Software des Betriebssystems zu nutzen, statt durch Werbung finanzierte Virenscanner. Diese dringen nämlich auch in die Privatssphäre der Nutzer ein.

6. Social Engineering

Social Engineering ist eine Angriffsmethode, die das Vertrauen der Nutzer ausnutzt und die Anwender zu einer Datenweitergabe verleitet. Social Engineering erfreut sich unter den Datendieben einer immer größeren Beliebtheit und zeigt sich in unüberschaubar vielfältigen Formen. Gerade Soziale Netzwerke im Internet bieten eine gute Ausgangsbasis für Social Engineering.

Eine weitere Szene aus dem Lehrerzimmer, die sich so oder so ähnlich abspielen könnte:

Paul: Hallo, Petra! Konntest du gestern noch die Zensuren ändern?

Petra: Zensuren ändern? Wovon sprichst du? Ich habe alle Zensuren lange fertig!

Paul: Aber gestern hast Du mir doch eine Facebook-Nachricht geschickt, dass Du zu Hause dein Passwort für die Zeugnisdatei nicht parat hast und noch dringend Noten ändern musst! Ich habe es dir doch gepostet …

Petra: Das war ich nicht! Ich bin nicht mal auf Facebook!!!

Das Grundprinzip ist immer dasselbe; egal ob im Sozialen Netzwerk, am Telefon, per E-Mail oder im direkten Kontakt: Der Angreifer versucht zuerst Vertrauen aufzubauen – oft durch einen kleinen Gefallen, der später wieder eingefordert wird, um dann durch geschickte Manipulation Informationen zu erlangen. Dabei werden menschliche Eigenschaften (oder Schwächen) wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität manipulativ ausgenutzt.

Wie Trickbetrüger täuschen Angreifer beim Social Engineering ihren Opfern oft eine persönliche Bekanntschaft oder besondere Umstände vor. Ziel ist es, Personen etwa durch Telefonanrufe oder Nachrichten im vermeintlichen Auftrag von Vorgesetzten oder Bekannten dazu zu bewegen, vertrauliche Informationen oder schützenswerte Daten preiszugeben oder sie zum Öffnen von Dateien oder zur Installation von Programmen auf dem Computer zu verleiten.

→ *https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html*

Das beste Anti-Viren-Programm und die sicherste Firewall können nicht helfen, wenn der Nutzer Informationen nicht sichert oder sogar freiwillig preisgibt. Gutgläubigkeit ist in dem Zusammenhang keine Tugend, sondern ein Angriffstor. An dieser Stelle soll besonders auf den Aspekt der Datensparsamkeit hingewiesen werden, d.h. dass gerade Lehrerinnen und Lehrer sich sehr bewusst machen sollten, welche Informationen sie in sozialen oder generell öffentlich Netzwerken über sich preisgeben und wer diese Informationen alles sehen darf.

Das gilt auch für »vermeintlich« kostenlose Geschenke oder Funde. Ein USB-Stick oder Kabel[11], das scheinbar zufällig vor der Tür liegt und mitgenommen und in den Computer gesteckt wird – egal, ob aus Neugier oder der hehren Absicht den Eigentümer festzustellen – stellt ein weit geöffnetes Tor für Angriffe dar. Sich automatisch installierende Schadsoftware kann den Computer in Sekundenbruchteilen übernehmen und Informationen an Hacker weiterleiten. Das gilt sogar bei »scheinbaren« Werbegeschenken, die von Firmen auf Messen oder Conventions verteilt werden. USB-Zubehör wie Sticks, Mäuse o. Ä. können Key-Logger oder andere Spyware auf dem Rechner installieren und Informationen weiterleiten.

[11] https://www.heise.de/news/USB-C-auf-Lightning-Kabel-spioniert-Nutzer-aus-6182199.html

In all diesen Fällen gilt es, aufmerksam zu sein und Gefährdungen zu erkennen und zu vermeiden. Bereits beim kurzzeitigen Verlassen eines Computerarbeitsplatzes kann man den Zugriff auf Daten durch Unbefugte erschweren, indem man ganz kurz den Rechner sperrt (bei Windows: »WIN+L« Windowstaste und gleichzeitig L-Taste drücken).

Besser ist es jedoch, den Rechner nicht unbeobachtet zu lassen und in einem nicht vertrauenswürdigen Umfeld sogar herunterzufahren.

MERKE: Sicherheit beginnt beim Anwender

- Nie aus Drucksituationen heraus handeln.
- Informationen nicht leichtfertig preisgeben.
- Trojanische Marketinggeschenke ablehnen.

7. Fazit

Lehrerinnen und Lehrer haben schützenswerte Daten zu verwalten. Weder Zensuren-Listen, noch Zeugnisbeurteilungen o. Ä. dürfen in fremde Hände geraten. Und mit Anspielung auf die Szene aus Kapitel 6: Wer sagt denn, dass jetzt nicht ein Schüler Zugriff auf die Zeugnisdatei hat?

Deswegen – und nicht zuletzt auch der Gesetzgebung folgend – müssen Lehrerinnen und Lehrer im sächsischen Schuldienst die grundlegenden Anforderungen an den Datenschutz und die Informationssicherheit erfüllen.

Die oben gegebenen Handlungsempfehlungen können zwar individuell angepasst werden, bieten aber so - vor dem Hintergrund der europäischen Datenschutz-Grundverordnung (DSGVO) – eine Handlungsgrundlage für den regelkonformen Umgang mit schützenswerten Daten.

Jede Lehrerin und jeder Lehrer im sächsischen Schuldienst ist also mitverantwortlich für den Umgang mit schützenswerten Daten sowie deren Verschlüsselung und Schutz vor Missbrauch und Verlust.

Herausgeber und Redaktion:
Landesamt für Schule und Bildung
Referat 33 | Medienbildung und Digitalisierung
Annaberger Straße 119
09120 Chemnitz
Telefon: +49 371 5366-0
E-Mail: poststelle@lasub.smk.sachsen.de
www.lasub.smk.sachsen.de
Beratung:
4viewture GmbH, Kesselsdorf
Gestaltung und Satz:
Hi Agentur e.K., Dresden
Fotos:
Abbildungen unter Verwendung von PowToon
Redaktionsschluss:
Oktober 2021
Bezug:
Dieser Artikel ist elektronisch als PDF verfügbar

Verteilerhinweis:
Diese Informationsschrift wird von der Sächsischen Staatsregierung im Rahmen ihrer verfassungsmäßigen Verpflichtung zur Informationder Öffentlichkeit herausgegeben. Sie darf weder von politischen Parteien noch von deren Kandidaten oder Helfern zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen. Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung.