Windows und Office absichern

Peter Willadt

2020-05-04

Durch die verstärkte elektronische Kommunikation mit Schülern und Schülerinnen steigt auch das Risiko, dass Sie sich Schadsoftware einfangen. Aus diesem Grund sollten Sie Ihren Rechner absichern. Bitte verstehen Sie das Folgende nicht als Microsoft-Bashing: Andere Betriebssysteme sind nicht unbedingt sicherer als Windows, andere Anwendungssoftware ist nicht unbedingt sicherer als Microsoft Office. Allerdings ist es so, dass Schadsoftware sich an die Mehrheit der Anwender richtet, und solange die Mehrheit der Anwender Microsoft Windows und Microsoft Office verwendet, ist dies eben das lohnendste Angriffsziel.

Erster Schritt ist, grundsätzlich hinsichtlich Updates immer auf dem neuesten Stand zu sein. Das betrifft nicht nur das Betriebssystem selbst, sondern auch alle Anwendungsprogramme; in erster Linie den Internet-Browser, dann aber auch alle anderen Programme, die gegebenenfalls Dateien aus dem Internet öffnen, z.B. Office-Software, Medienplayer oder ein PDF-Betrachter. Nicht jede Software verfügt über automatische Update-Funktionen, z.B. warnt der Adobe Reader XI nicht einmal, dass er schon längere Zeit nicht mehr gewartet wird. Sie sollten sich also ab und zu die Mühe machen und sorgfältig überprüfen, ob Ihre Software noch aktuell ist und aktualisiert wird.

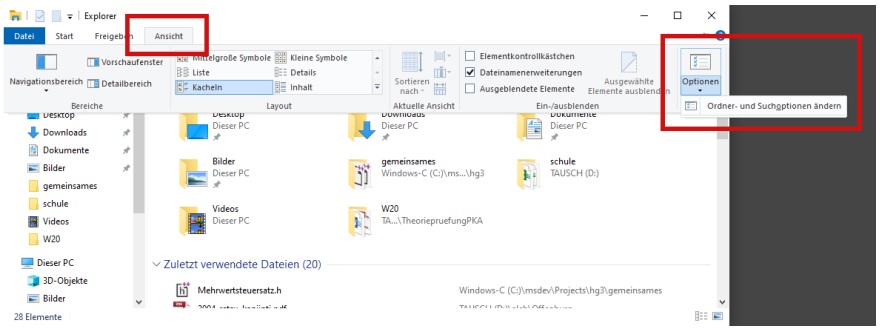
Spezielle Antivirensoftware ist nicht besser als der in Windows eingebaute Virenschutz. Falls Sie andere Antiviren-Software verwenden, benutzen Sie nur *ein* Produkt und achten Sie darauf, dass es stets aktuell ist.

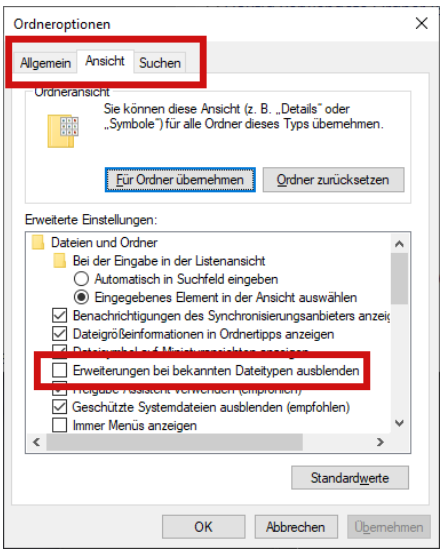
Ältere Angriffsmethoden bringen den Benutzer dazu, schädliche Programme zu starten. Eine typische Strategie der Cyberverbrecher ist es z.B., im Dateinamen zu verschleiern, dass es sich um ausführbare Programme handelt. Eine klassische Methode besteht darin, mehrfache Dateiendungen zu verwenden. So heißt dann ein Programm eben nicht `Bild.exe` sondern `Bild.jpg.exe`. Im Win-

dows Explorer wird die eigentliche Dateiendung standardmäßig weggelassen, dadurch sieht man nur den Namen `Bild.jpg` und glaubt, es handle sich um ein Bild. Sie können sich vor diesen Angriffen schützen, indem Sie die Anzeige der Dateiendungen aktivieren. Die zweite Methode verwendet Dateiendungen, die nicht geläufig sind. Beispielsweise stehen auch die Endungen `SCR`, `COM` und `MSC` für ausführbare Programme[1]. Hier hilft nur der gesunde Menschenverstand und eine gehörige Portion Misstrauen.

Anzeige der Dateiendungen im Explorer

Gehen sie im Explorer auf Ansicht und dann ganz rechts auf Optionen. Wählen Sie *Ordner und Suchoptionen ändern*, im Fenster *Ordneroptionen* gehen Sie auf die Karteikarte *Ansicht* und suchen den Eintrag *Erweiterungen bei bekannten Dateitypen ausblenden*. Entfernen Sie das Häkchen vor diesem Eintrag und gehen Sie auf *OK*. Falls Ihr Computer über mehrere Benutzerkonten verfügt, müssen Sie diese Aktion für jedes Benutzerkonto vornehmen.





[1] Diese Aufzählung ist nicht abschließend.

Angriffsfläche verkleinern

Deinstallieren Sie sämtliche Software, die Sie nicht benötigen. Jedes Programm enthält Sicherheitslücken und vergrößert damit die Angriffsfläche. Office 2019 ist in dieser Hinsicht leider problematisch: einzelne Programmteile lassen sich nicht gezielt entfernen. Es ist auch nicht einfach, sämtliche in Windows 10 vorinstallierten nicht benötigten Apps zu entfernen. Sie finden im Internet jedoch Anleitungen, die Sie – wenn sie die nötige Geduld aufbringen – berücksichtigen können.

Auswahl der Suchmaschine

Das Internet ist voll von bösartigen Programmen. Manche Anbieter von unerwünschter Software überlassen es nicht dem Zufall, dass sie gefunden werden; sie inserieren und schalten z.B. Suchmaschinenwerbung. Und hier unterscheiden sich die Suchmaschinen deutlich: Microsoft Bing veröffentlicht immer noch und immer wieder auch Werbung, mit der man sich unerwünschte Software einfängt. Google ist mir in dieser Hinsicht nicht so negativ aufgefallen. Trotzdem sollten Sie zweimal hinsehen, besonders wenn Sie die Absicht haben, ein Programm herunterzuladen. Typische Gaunereien verbinden den Download einer kostenlosen Software mit dem von unerwünschten Beigaben. Beispielsweise ist heute der erste Treffer bei der Suche nach »Gimp Download« die Seite `Gimp24.de`. Bei der Suche nach dem VLC-Media-Player landet auf der ersten Ergebnisseite auch die Seite `VLC-download.de`. Beide angeführten Seiten bringen neben der erwünschten Software zusätzlich unerwünschte Funktionen mit. Ich empfehle, kostenlose Software grundsätzlich vom Original-Anbieter oder von einer Viren-geprüften Download-Plattform herunterzuladen.

Office absichern

Die weitaus stärkste Bedrohung für den Computer in den letzten Monaten sind präparierte Office-Dokumente, die per Mail eintreffen und den Benutzer dazu verleiten, sogenannte Macros zu aktivieren. Antivirensoftware ist oftmals nicht in der Lage, solche Angriffe zu erkennen. Eine Möglichkeit, das Risiko zu verringern, besteht darin, die Ausführung von Makros innerhalb von Microsoft Office zu unterbinden. Dies wird im Folgenden beschrieben. Die Deaktivierung muss für jedes Office-Programm einzeln vorgenommen werden. Wenn Sie auf Ihrem Rechner mehrere Benutzerkonten haben, müssen Sie die Deaktivierung für jedes Benutzerkonto vornehmen. Im Schulnetz und im Lehrernetz der Ludwig-Erhard-Schule müssen Sie die Deaktivierung nach jedem Anmelden erneut vornehmen, da Sie

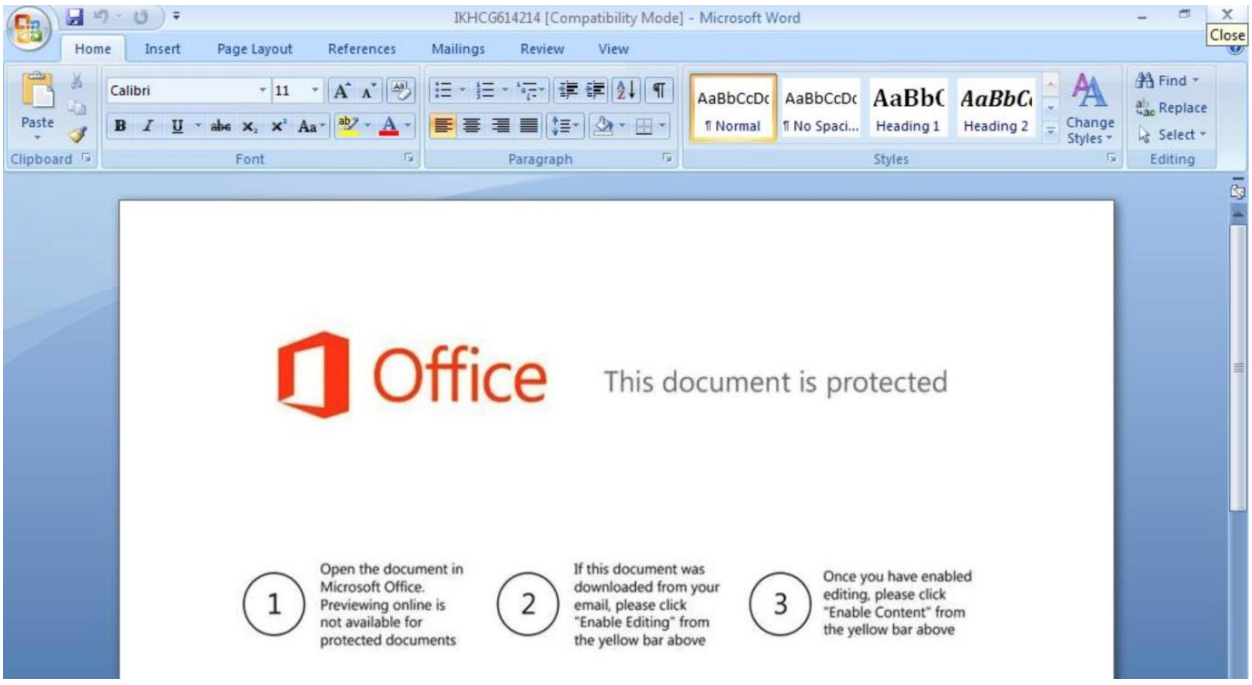
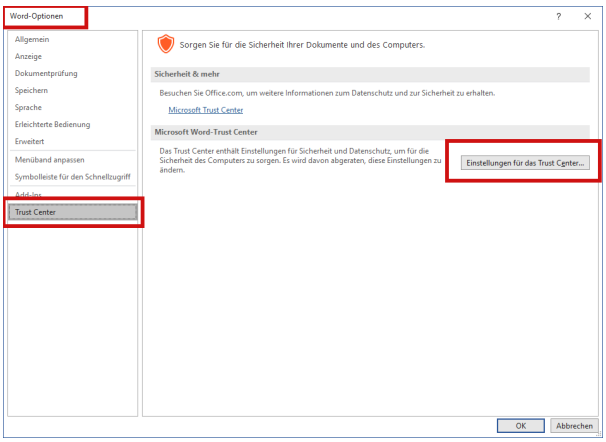


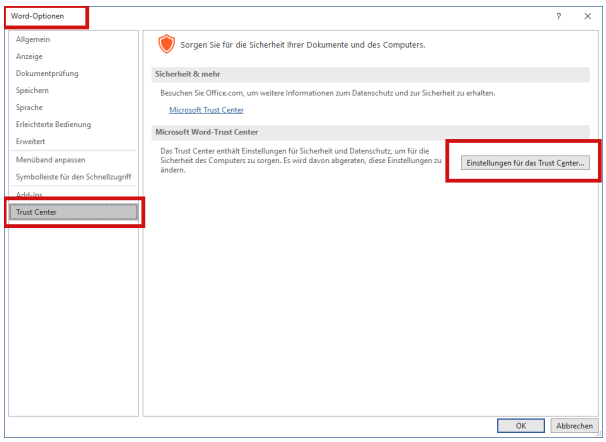
Abbildung 1: Die Abbildungen (1. GDATA, 2. Trenmicro) zeigen typische Phishing-Versuche. Anklicken führt zur Infektion.

mit jedem Anmelden ein neues Windows-Benutzerkonto erhalten. Sie sollten die Einstellungen für *jedes* Office Programm vornehmen, auch wenn Sie eines der Programme nicht verwenden; ein Doppelklick kann Sie schnell dazu bringen, dann doch ein Programm zu starten.

In Word kommen Sie folgendermaßen zu den Einstellungen:

- Gehen sie auf Datei, dort auf Optionen.
- Wählen Sie bei den Optionen das Trustcenter aus (in Office 2019 der Punkt ganz links unten, dann nochmals rechts das Trust-Center anklicken).
- Gehen sie dort auf Makroeinstellungen und wählen Sie die Deaktivierung aller Makros.
- Gehen Sie auf OK.





Auch in Excel, Access, Publisher und Powerpoint gelangen Sie durch Datei → Optionen → Trustcenter zum Trustcenter. Die Makroeinstellungen entsprechen denen in Word. Falls Sie eine *Pro*-Version von Windows besitzen, können Sie sich auch Gruppenrichtlinien konfigurieren, die das Ausführen von Office-Makros für alle Benutzer abschalten. Es sprengt den Rahmen dieser Anleitung, darauf einzugehen. Ich selbst fahre schon jahrelang gut damit, mir zugesandte Office-Dokumente nicht mit Microsoft Office zu öffnen, sondern mit einer alternativen Software wie z.b. LibreOffice. Da LibreOffice über andere Schwachstellen als Microsoft Office verfügt, entsteht ein Zugewinn an Sicherheit.

Bleiben Sie gesund, infizieren Sie sich nicht.