TECWORKSHOP

Windows 7 / 8.1 und Windows 10

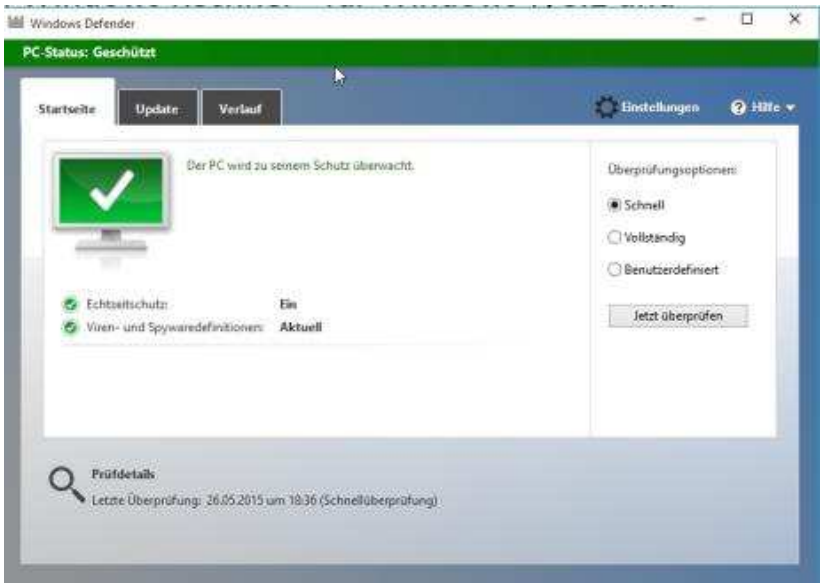
In 10 Schritten zum sicheren Windows-PC

Datum: 29.10.2015
Autor(en): Thomas Joos

Um einen Windows-Rechner möglichst sicher zu betreiben, sollten PC-Anwender ein paar Dinge beachten und sicherheitsrelevante Tools nutzen. Damit lassen sich PC-Schädlinge und Angreifer auf Distanz halten und im Falle eines Falles sogar lokalisieren und entfernen.

1. Virenschutz installieren

Windows 8.1[1] und **Windows 10**[2] haben Windows Defender an Bord, den integrierten Virenschutz. Dieser ist allerdings auch in Windows 10 weit weniger sicher als viele kostenlose Konkurrenzprodukte.



Windows 8.1 und Windows 10 verfügen über Windows Defender, allerdings ist die Software nicht sehr zuverlässig.

Wollen Sie keinen kostenpflichtigen Virenschutz installieren, können Sie auch kostenlose Tools verwenden. Achten Sie aber darauf, dass noch nicht alle für Windows 10 freigegeben sind. Setzen Sie nur Tools ein, die von Windows 10 unterstützt werden. Die bekanntesten in diesem Bereich sind:

- **AVG free**[3]

- **Avast 2015**[4]

· **Avira Free Antivirus**[5]

2. Regelmäßig mit Live CD scannen

Auch wenn Sie einen Virenscanner auf dem Rechner haben, sollten Sie in regelmäßigen Abständen, zum Beispiel wenn Sie gerade nicht mit dem Computer arbeiten, einen Scanvorgang starten. So stellen Sie sicher, dass kein Schädling auf dem Rechner vorhanden ist, und wenn doch, wird er entfernt. Die wichtigsten Tools dazu sind:

· **ADWcleaner**[6]

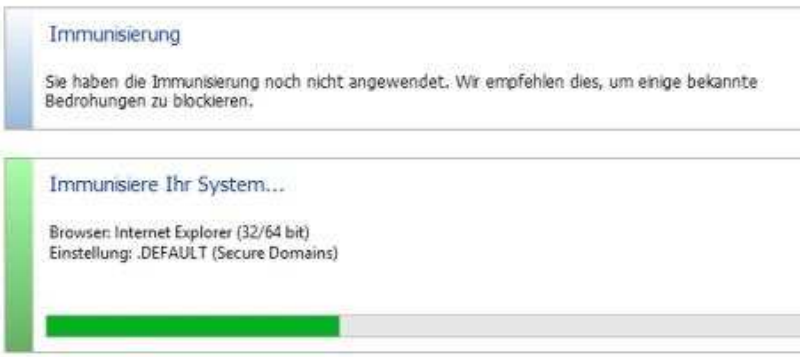
· **Spybot 2.4 Free Edition**[7]

· **Kaspersky Live-CD**[8]

Die Tools sind kostenlos und erledigen optimal Sicherheits-Scans. Spybot Free kann den PC sogar vor bekannter Werbesoftware immunisieren. Das sollten Sie bei der Installation in jedem Fall durchführen.

Adwcleaner kann Windows zuverlässig von Trojanern befreien.

Sobald Sie Spybot installiert haben, aktualisieren Sie zunächst die Definitionsdateien und lassen danach den Rechner immunisieren. Im Anschluss lassen Sie Windows durchsuchen und entfernen alle Schädlinge. Diesen Vorgang sollten Sie regelmäßig wiederholen.



Mit Spybot entfernen Sie einige Schädlinge und können Ihr System auch immunisieren.

3. Werbeblocker installieren

Nutzen Sie als Browser am besten **Google Chrome**[9] oder **Mozilla Firefox**[10]. Die Browser sind schneller als der Internet Explorer und auch sicherer. Außerdem lassen sich einfacher Add-On für das sichere Surfen installieren. Hier gibt es zwar für Sicherheitsfans auch Add-Ons, die noch zuverlässiger blocken, allerdings schränken diese auch das Surferlebnis ein. **Adblock**[11] oder die Version **Adblock Plus**[12] sind hier zu empfehlen. Sowohl für Chrome als auch für Firefox gibt es passende Add-Ons.

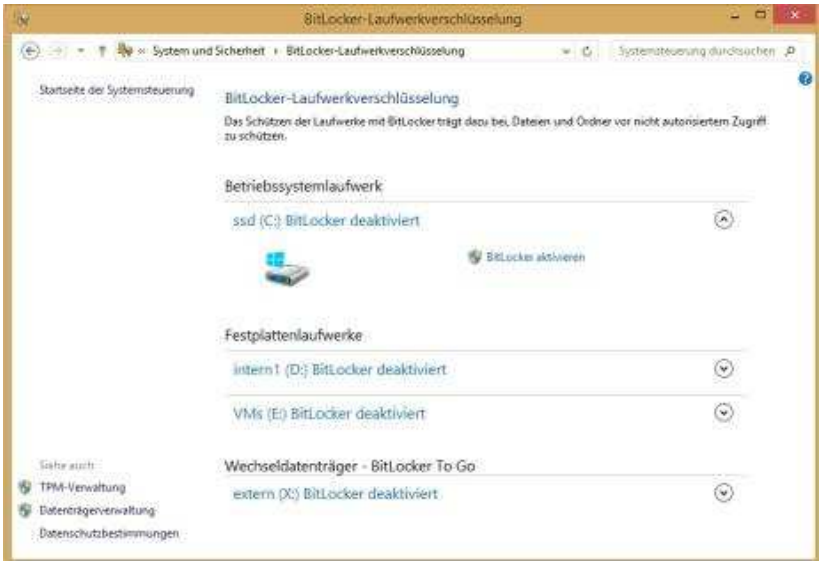
Adblock kann Werbung blockieren, aber auch den einen oder anderen Angreifer. Das Add-On verhindert zudem, dass ungeübte Anwender auf verseuchte Seiten surfen.

Ergänzend lassen sich Chrome und Firefox noch weiter absichern. Für Firefox ist hier vor allem das Add-on **NoScript**[13] ideal. Allerdings müssen Anwender in diesem Fall viele Fenster bestätigen, sodass dieses Add-On nur für erfahrene Benutzer zu empfehlen ist.

4. Laufwerksverschlüsselung Bitlocker nutzen

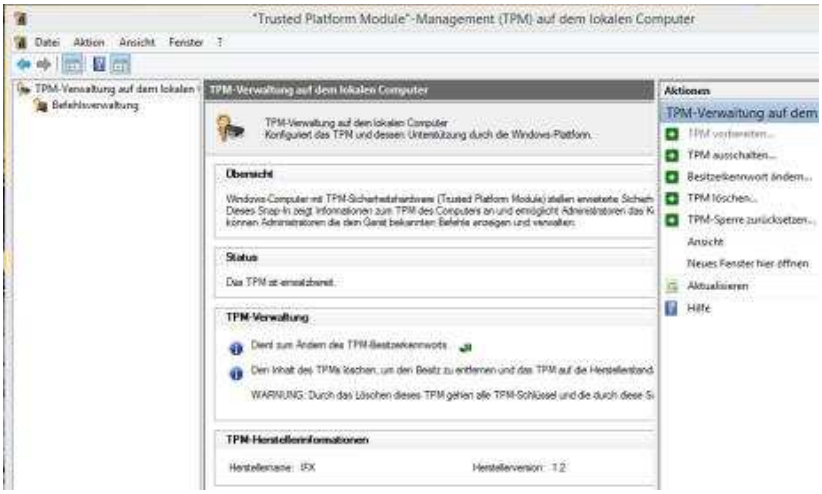
Setzen Sie Windows 8/8.1 Pro/Enterprise oder eine entsprechende Variante von Windows 10 ein, dann sollten Sie **Bitlocker**[14] aktivieren. Vor allem auf Notebooks ist das sinnvoll. Wenn Sie

einen Rechner nutzen, der über ein **TPM-Modul**[15] verfügt, lässt sich dieser in den Schutz einbinden.



Bitlocker aktivieren Sie in der Systemsteuerung. Nach der Verschlüsselung sind die Daten au der Festplatte zuverlässig gesichert, auch vor Diebstahl.

Im laufenden Betrieb bemerken Sie nichts von Bitlocker, aber die Festplatte bleibt optimal geschützt, auch wenn Ihr Rechner verloren geht. Bitlocker ist am effizientesten, wenn im Rechner ein TPM-Chip eingebaut ist. Diesen müssen Sie im ersten Schritt einrichten. Das Verwaltungsprogramm wird über tpm.msc gestartet.



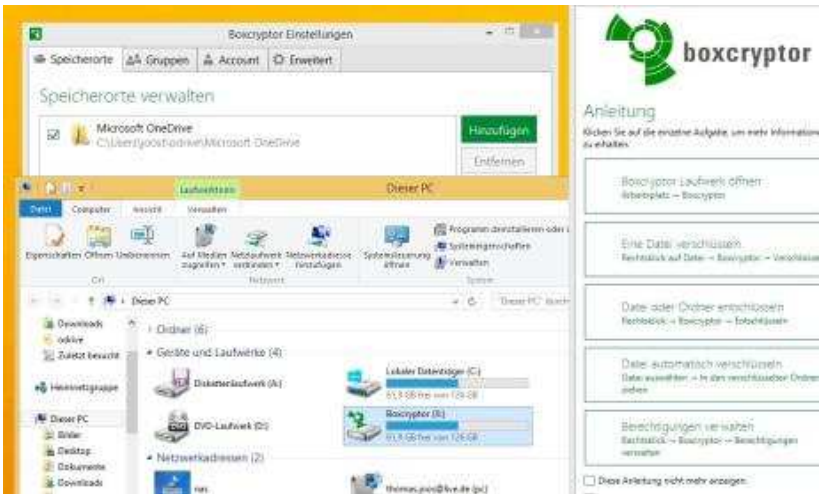
Bitlocker schützt den Rechner idea vor allem wenn Sie einen TPM-Chi eingebaut haben.

Ohne TPM-Chip müssen Sie die Richtlinie Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/BitLocker-Laufwerkverschlüsselung /Betriebssystemlaufwerke anpassen. Die Verwaltung wird über gpedit.msc gestartet.

5. Cloud-Daten mit Tools verschlüsseln

Nutzen Sie OneDrive auf Ihrem Windows-Rechner, sollten Sie nicht alle Daten einfach in die Cloud übertragen. Mit kostenlosen Tools können Sie schnell und einfach Daten in OneDrive verschlüsseln. **Boxcryptor**[16] gibt es kostenlos. Nach der Anmeldung steht ein neues Laufwerk im Explorer zur Verfügung. Alle Daten, die Sie hierhin kopieren, verschlüsselt Boxcryptor. Überprüfen Sie, ob das Laufwerk auf das Synchronisierungsverzeichnis Ihres Cloud-Speichers zeigt.

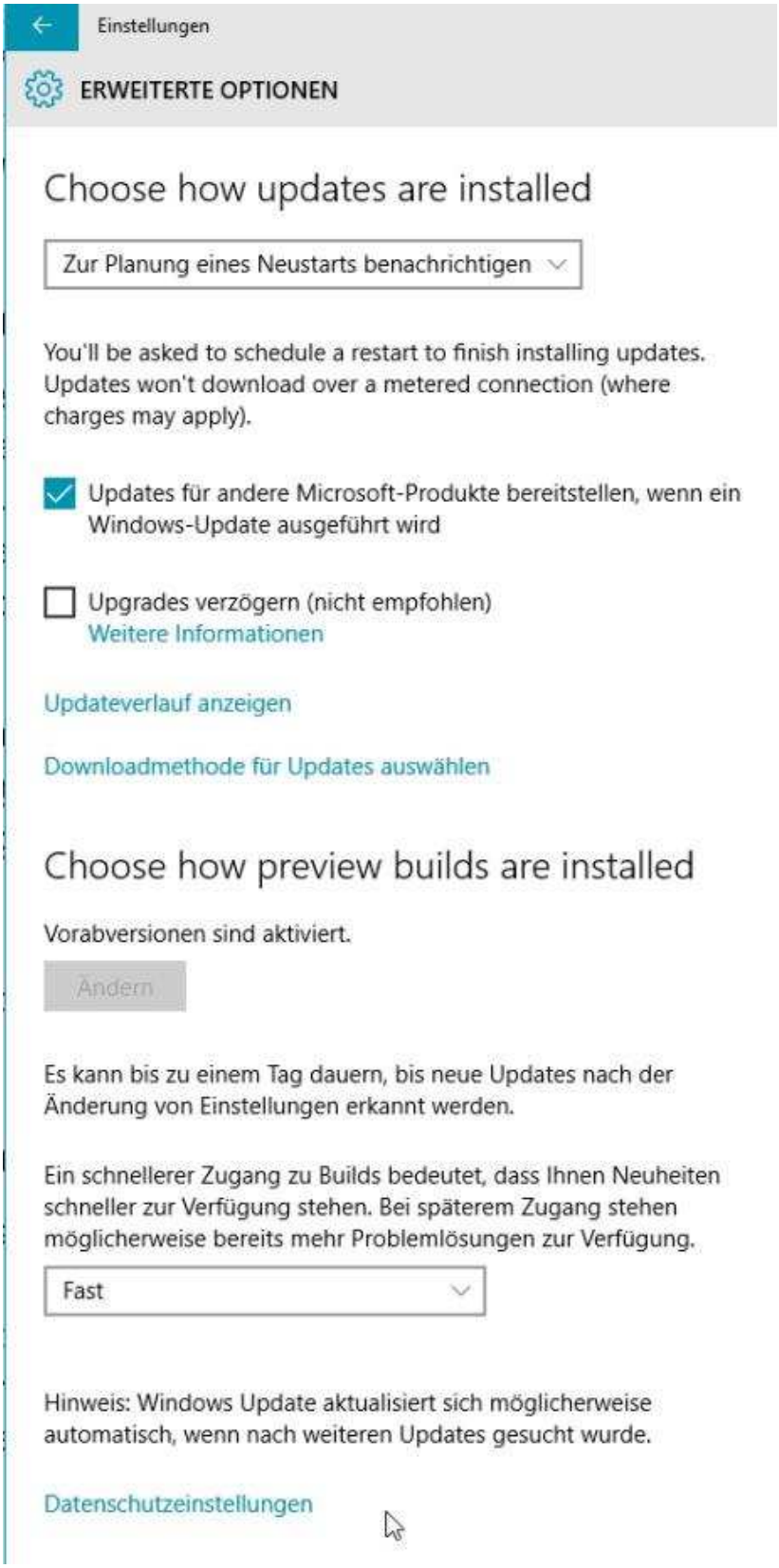
Boxcryptor verschlüsselt nur neue Dateien. Sollen auch vorhandene Dateien im Cloud-Speicher verschlüsselt werden, müssen Sie im Windows-Explorer das Boxcryptor-Laufwerk öffnen und über das Kontextmenü von Ordnern und Dateien die Verschlüsselung mit Boxcryptor aktivieren.



Mit BoxCryptor verschlüsseln Sie schnell und einfach Dateien, bevor diese in Ihren Cloud-Speicher geladen werden.

6. Updates aktiv installieren und überprüfen

Sie sollten in den Einstellungen von Windows zunächst sicherstellen, dass Windows-Updates automatisch installiert werden. Aber auch dann ist es ratsam, regelmäßig zu überprüfen, dass der Rechner auch aktuell ist. Am schnellsten finden Sie die Konfiguration von Updates, wenn Sie wuapp.exe aufrufen. In **Windows 10**[17] sollten Sie darüber hinaus noch über Erweiterte Optionen sicherstellen, dass auch für andere Produkte Updates über Windows Update installiert werden, nicht nur für Windows selbst.



Windows-Updates sollten automatisiert installiert werden. Am besten ist, Sie überprüfen die Installation regelmäßig.

7. Windows auf optimale Sicherheit einstellen

Das Einstellungsmenü in Windows 10 ist wesentlich übersichtlicher als die Systemsteuerung in den Vorgängerversionen. Sie sollten alle Einstellungen mindestens einmal durchgehen und einen Kompromiss zwischen guter Bedienbarkeit und Sicherheit finden. Klicken Sie sich einma durch alle Optionen durch und stellen Sie sicher, dass wichtige Einstellungen gesetzt sind, vor allem in den Bereichen Update, Sicherheit und Konten. Im Bereich Konten\Anmeldeoptionen

können Sie zum Beispiel festlegen, dass die Anmeldung über eine PIN oder einen Bildcode erfolgen soll.

8. Erst überlegen, dann klicken

Erhalten Sie E-Mails, überprüfen Sie zunächst deren Absender, bevor Sie sie anklicken. Das gil auch beim Besuchen von Internetseiten. Natürlich können Sicherheits-Tools und Virenscanner den Rechner schützen, aber der beste Schutz ist immer noch, wenn kein Angreifer auf den Rechner kommt. Bevor Sie ein Angebot anklicken oder eine E-Mail öffnen, sollten Sie daher immer überprüfen, um welchen Absender es sich handelt und ob er Ihnen bekannt ist.

9. Für jeden Benutzer ein eigenes Anmeldekonto

Nutzen mehrere Anwender einen Rechner, sollten Sie für jeden Benutzer ein eigenes Konto anlegen. Außerdem muss nicht jeder Benutzer über Administratorrechte verfügen. Das erhöht deutlich die Sicherheit, da nicht alle Anwender mit einem gemeinsamen Konto arbeiten. Die Einrichtung erfolgt in den Einstellungen von Windows 8.1/10 oder über den Benutzermanager in Windows 7, den Sie über lusrmgr.msc starten.

10. Tauschbörsensoftware vermeiden

Auch wenn das mittlerweile den meisten Anwendern bekannt sein sollte, nutzen viele immer noch Tauschbörsensoftware. Das Problem an dieser Art von Software ist, dass beim Herunterladen immer auch Teile der Daten für andere Anwender der Tauschbörse zur Verfügung gestellt werden.

Das lässt sich zwar teilweise deaktivieren, allerdings können Sie sich nicht auf die Deaktivierung verlassen. Außerdem gelangen über diesen Weg immer wieder **Viren und Trojaner**[18] auf den Rechner. Wenn Sie Tauschbörsensoftware nutzen wollen, dann am besten direkt in einer virtuellen Maschine und nicht auf Ihrem Produktivsystem. (hal)

Links im Artikel:

[1] **http://www.tecchannel.de/pc_mobile/windows/2075068/10_dinge_die_sie_nach_der_installation_von_windows_81_durchfuehren_sollten/**
[2] **http://www.tecchannel.de/pc_mobile/windows/3198207/so_schlaegt_sich_windows_10_gegen_windows_7_und_81/**
[3] **http://free.avg.com/de-de/homepage**
[4] **https://www.avast.com/de-de/index**
[5] **https://www.avira.com/de/index**
[6] **http://general-changelog-team.fr/en**
[7] **http://www.safer-networking.org/de/dl**
[8] **http://support.kaspersky.com/viruses/rescuedisk?level=2**
[9] **https://www.google.de/chrome/browser/desktop/**
[10] **https://www.mozilla.org/de/firefox/new/**

[11] **https://getadblock.com/**
[12] **https://adblockplus.org/de**
[13] **https://noscript.net/**
[14] **http://windows.microsoft.com/de-de/windows-8/bitlocker-drive-encryption**
[15] **http://de.wikipedia.org/wiki/Trusted_Platform_Module**
[16] **https://www.boxcryptor.com/**
[17] **http://www.tecchannel.de/pc_mobile/windows/3198207 /so_schlaegt_sich_windows_10_gegen_windows_7_und_81/**
[18] **http://www.tecchannel.de/sicherheit/spam/2056633 /die_geschichte_von_viren_trojanern/**
