Neuinstallation infizierter PC Windows 8

Ihr PC ist mit Malware infiziert. Sie wissen nicht, wie Sie Ihr System richtig neu installieren? Die folgende Anleitung hilft Ihnen Schritt für Schritt dabei, den PC neu aufzusetzen und gleichzeitig das Risiko einer Neuinfizierung zu vermindern.

Wir haben uns bemüht, eine möglichst allgemeingültige Anleitung für Privatanwendende zu verfassen. Natürlich können die erforderlichen Schritte in besonderen Fällen abweichen.

Die Anleitung basiert auf einer Windows 8.1 Professional 64-Bit-Edition, gilt aber auch für 32-Bit-Varianten.

Damit Sie Ihr System gemäss dieser Anleitung richtig neu installieren können, benötigen Sie die Windows 8 Installations-CD sowie ein externes Speichermedium zur Datensicherung.

Schritt 1: Trennen des PCs vom Netzwerk

- Wenn Ihr PC per Kabel ans Netzwerk angebunden ist, können Sie einfach den Netzwerkstecker herausziehen.
- Falls Sie ein Drahtlos-Netzwerk (WLAN) verwenden, sollten Sie den Flugzeugmodus aktivieren (Klick auf das *Netzwerksymbol* unten rechts in der Taskleiste → Klick auf den Schalter für den Flugzeugmodus).

Schritt 2: Sichern der persönlichen Daten

- Schliessen Sie ein externes Speichermedium mit gedrückt gehaltener «Shift»-Taste an und sichern Sie Ihre persönlichen Daten. Verwenden Sie dafür nicht Ihr «normales» Backupmedium, sondern nach Möglichkeit ein neues, komplett leeres.

  HINWEIS: Malware auf dem PC kann dazu führen, dass das externe Speichermedium sowie die dort abgelegten Daten ebenfalls infiziert werden. Speziell die Autorun-Funktion wird von Malware genutzt, um sich über externe Speichermedien (USB-Stick etc.) weiterzuverbreiten. Diese Autorun-Funktion lässt sich temporär relativ einfach deaktivieren. Drücken Sie hierzu die «Shift»-Taste auf Ihrer Tastatur und halten Sie diese gedrückt. Schliessen Sie dann das externe Speichermedium an Ihren Computer an und lassen die «Shift»-Taste erst nach einer kurzen Zeitspanne wieder los. Die «Shift»-Taste verhindert in diesem Fall, dass Windows automatisch Programme und Dateien auf dem externen Speichermedium ausführt.

Schritt 3: Bereinigen des Master Boot Record (MBR)

Gewisse Computerviren nisten sich im sogenannten Master Boot Record (MBR) des PCs ein. Dieser sollte deshalb neu geschrieben und auf diese Weise bereinigt werden. Verwenden Sie dazu das Hilfsprogramm «Bootrec.exe» in der Windows-Wiederherstellungsumgebung.

- Legen Sie die Windows 8 Installations-CD in das Laufwerk ein, und starten Sie den PC neu.
- Sollte der PC nach dem Neustart nicht von der eingelegten CD aus booten, so stellen Sie im BIOS das CD-Laufwerk als erstes Device ein (siehe Mainboard-Handbuch).
  Alternativ können Sie gleich nach dem Starten des PCs die Funktionstaste «F8» drücken. Sie gelangen so zum Bootmanager, wo Sie das CD-Laufwerk auswählen können.
- Drücken Sie eine Taste, wenn Sie dazu aufgefordert werden.
- Wählen Sie eine Sprache, eine Zeit, eine Währung, eine Tastatur oder Eingabemethode, und klicken Sie auf *Weiter*.

- Klicken Sie auf *Computerreparaturoptionen*.
- Klicken Sie auf *Problembehandlung*.
- Klicken Sie auf *Erweiterte Optionen*.
- Klicken Sie im Dialogfeld Erweiterte Optionen auf *Eingabeaufforderung*.
- Geben Sie «`bootrec.exe /fixmbr`» ein und drücken Sie dann die Eingabetaste (*Enter*). Dadurch wird der MBR wiederhergestellt (und somit die MBR Rootkit-Funktionalität von allfälliger Malware deaktiviert).
- Schliessen Sie die Eingabeaufforderung und fahren Sie den PC mittels *PC ausschalten* herunter. Belassen Sie die Windows 8 Installations-CD im Laufwerk.

Schritt 4: Neuinstallation von Windows 8

- Starten Sie den PC neu.
- Sollte der PC nach dem Neustart nicht von der eingelegten CD aus booten, so stellen Sie im BIOS das Laufwerk als erstes Device ein (siehe Mainboard-Handbuch).
  Alternativ können Sie gleich nach dem Starten des PCs die Funktionstaste «F8» drücken. Sie gelangen so zum Bootmanager, wo Sie das CD-Laufwerk auswählen können.
- Drücken Sie eine Taste, wenn Sie dazu aufgefordert werden.
- Wählen Sie eine Sprache, eine Zeit, eine Währung, eine Tastatur oder Eingabemethode, und klicken Sie dann auf *Weiter*.
- Nun ist ein Klick auf *Jetzt installieren* notwendig.
- Wählen Sie im weiteren Verlauf als Installationsart *Benutzerdefiniert: nur Windows installieren (für fortgeschrittene Benutzer)* aus.
- Nun können Sie die Partitionen löschen, neu anlegen und formatieren.

  ACHTUNG: Bei Partition löschen oder formatieren gehen alle Daten auf der Partition verloren!

  HINWEIS: Um sicherzustellen, dass sich auf dem PC keine Malware mehr befindet, sind die vorhandenen Partitionen zu löschen und neu anzulegen. Danach sind die neu angelegten Partitionen zu formatieren. Beachten Sie weiter, dass eventuell eine Recovery-Partition des Herstellers vorhanden ist. Diese sollte nicht gelöscht oder formatiert werden.
- Installieren Sie Windows 8 mit den empfohlenen Einstellungen zu Ende.
- Verbinden Sie den PC mit dem Internet (Netzwerkstecker einstecken).
- Aktualisieren Sie das Betriebssystem, indem Sie den Zeiger der Maus in die rechte obere Ecke des Bildschirmes führen, und klicken Sie dann auf *Suche*. Geben Sie im Suchfeld «`Windows Update`» ein. Klicken Sie auf *Einstellungen* und bestätigen Sie mit der Eingabetaste (Enter). Klicken Sie nun auf *Jetzt nach Updates* suchen und installieren Sie diese.

Schritt 5: Installation eines Virenschutzprogrammes

- Installieren Sie ein Virenschutzprogramm aus vertrauenswürdiger Quelle und aktualisieren Sie dieses mittels der integrierten Update-Funktion.

  HINWEIS: Eine Liste empfohlener Virenschutzprogramme finden Sie unter www.ebas.ch/5steps_step2.

Schritt 6: Installation und Aktualisierung von Programmen

- Installieren Sie die gewünschten Programme. Aktualisieren Sie alle Programme und schalten Sie wo möglich die Autoupdate-Funktion ein.

HINWEIS: Achten Sie darauf, Programme nur aus vertrauenswürdigen Quellen zu installieren (z. B. Download-Webseiten der Hersteller oder Software-Archive wie PCtipp, Heise etc.).

Schritt 7: Scannen der Daten

- Halten Sie die «Shift»-Taste gedrückt und schliessen Sie das externe Speichermedium mit den zuvor gesicherten Daten an den PC an.

  HINWEIS: Falls sich beim Sichern der Daten Malware auf das externe Speichermedium kopiert hat, kann der PC wieder infiziert werden! Um dies zu verhindern, muss beim Anschliessen des externen Speichermediums zwingend die «Shift»-Taste gedrückt gehalten werden (siehe Hinweis Schritt 2).

- Scannen Sie das gesamte System und das externe Speichermedium mit dem zuvor installierten Virenschutzprogramm. Falls infizierte Dateien gefunden werden, sind diese zu bereinigen oder zu löschen!

  HINWEIS: Eine bessere, aber auch aufwendigere Alternative zum Scannen vom neu installierten System aus, wäre es, das externe Speichermedium mittels einer bootbaren Live-CD oder von einem anderen Betriebssystem (z. B. Linux, macOS) aus zu überprüfen.

Schritt 8: Zurücksichern der Daten

- Spielen Sie Ihre gesicherten Daten vom externen Speichermedium auf den PC zurück.

Schritt 9: Was sonst noch zu tun ist!

- Da Malware heute sehr oft Benutzernamen und Passwörter ausspäht, sollten Sie auf jeden Fall sämtliche Passwörter auf dem System selbst, aber auch alle Passwörter auf Webseiten (z. B. E-Banking, E-Mail-Zugang, Facebook etc.) ändern.
- Ausserdem sollten Sie Ihre E-Banking-Auszüge sowie die Auszüge der Kreditkarten genau überprüfen.

Dieses Dokument wurde zu Informationszwecken und zur Verwendung durch den Empfänger erstellt. Hinsichtlich der Zuverlässigkeit und Vollständigkeit dieses Dokuments wird keine Gewähr gegeben, und es wird jede Haftung für Verluste abgelehnt, die sich aus dessen Verwendung ergeben können. Copyright © 2018 Hochschule Luzern – Informatik und Switch. Alle Rechte vorbehalten.

Diese Anleitung hat «eBanking – aber sicher!» in Zusammenarbeit mit SWITCH erstellt

eBanking aber sicher!

Auf der kostenlos zu nutzenden Webseite **www.ebankingabersicher.ch** finden Sie weitere praxisnahe Informationen über notwendige Massnahmen und Verhaltensregeln für eine sichere Anwendung von E-Banking-Applikationen.

SWITCH

SWITCH erbringt innovative, einzigartige Internet-Dienstleistungen für die Schweizer Hochschulen und Internetbenutzer.