Neuinstallation Windows 10

Suchen Sie die Anleitung für Windows 11, finden Sie diese hier (https://www.ebas.ch/neuinstallation-windows-11/) .

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

Die Anleitung richtet sich an Privatanwendende. Sie ist daher möglichst einfach und allgemeingültig gehalten. An einigen Stellen wird dennoch ein gewisses Mass an technischem Wissen vorausgesetzt. Holen Sie sich die kompetente Hilfe einer Fachperson, wenn Sie unsicher sind.

Damit Sie Ihr System gemäss dieser Anleitung richtig neu installieren können, benötigen Sie neben einer **gültigen Lizenz** ein **Windows 10 Installationsmedium**. Dies kann ein USB-Laufwerk oder eine DVD sein.

HINWEIS: Wenn Sie kein Windows 10 Installationsmedium haben, können Sie dieses auf einem Computer mit Windows 10 erstellen. Beachten Sie aber, dass Sie dies auf einem Malware-freien PC tun und nicht auf dem verseuchten System. Zur Erstellung des Installationsmediums müssen Sie das Media Creation Tool von Microsoft herunterladen und ausführen. Hier (https://www.microsoft.com/de-de/software-download/windows10) finden Sie Anweisungen mit weiteren Informationen zur Verwendung dieses Tools.

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 die Schaltfläche für den Flugzeugmodus).

Schritt 2: Sichern der persönlichen Daten und der Lizenz

- Schliessen Sie ein externes Speichermedium (externe Festplatte) mit gedrückt gehaltener «Shift»-Taste an und sichern Sie alle Ihre persönlichen Daten (https://www.ebas.ch/1-sichern-der-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-Laufwerk etc.) weiterzuverbreiten. Diese Autorun-Funktion lässt sich temporär relativ einfach deaktivieren. Halten Sie hierzu die «Shift»-Taste auf Ihrer Tastatur gedrückt, während Sie das externe Speichermedium an Ihren PC anschliessen und lassen Sie 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.

Wenn Sie nachher Ihren PC formatieren – was bei einem Malware-Befall dringend angezeigt ist – ist u.U. auch Ihre Lizenz verloren. Deshalb ist es wichtig, dass Sie diese vorgängig sichern.

- Klicken Sie unten links in der Taskleiste auf das Windows-Logo.
- Öffnen Sie ein Eingabeaufforderungsfenster, indem Sie «cmd» eingeben und die Eingabetaste (Enter) drücken.

- Geben Sie den Befehl «wmic path softwarelicensingservice get OA3xOriginalProductKey» ein und drücken Sie die Eingabetaste (Enter). Nun wird Ihnen Ihre Lizenz angezeigt.
- Speichern Sie Ihre Lizenz in einem Textverarbeitungsprogramm und sichern Sie diese ebenfalls auf dem externen Speichermedium.

HINWEIS: Sollte die Ausgabe des obigen Befehls leer sein, ist im UEFI/BIOS keine Lizenz gespeichert. In diesem Fall muss die Lizenz manuell eingegeben worden sein und steht sehr wahrscheinlich auf einem Aufkleber am Gehäuse Ihres PCs. Falls dies nicht der Fall ist, können Sie die Lizenz mit einem Programm wie z.B. Magical Jelly Bean Keyfinder (https://www.magicaljellybean.com/keyfinder/) oder Windows Product Key Viewer (https://www.heise.de/download/product/WindowsProductKeyViewer) aus der Registrierungsdatei (Registry) Ihres PCs auslesen.

Schritt 3: Bereinigen der GPT oder des MBR

Gewisse Schadprogramme nisten sich in der GPT (GUID-Partitionstabelle) oder im MBR (Master Boot Record) des PCs ein. GPT oder MBR sollten deshalb neu geschrieben und auf diese Weise bereinigt werden.

HINWEIS: Der MBR (Master Boot Record) ist ein alter, aber noch immer und häufig verwendeter Partitionsstil. Die GPT (GUID-Partitionstabelle) ist der zunehmend verbreitete neue Partitionsstil.

- Verbinden Sie das Windows 10 Installationsmedium (USB-Laufwerk oder DVD) mit dem PC und starten Sie diesen neu.
- Sollte der PC nach dem Neustart nicht vom Windows 10 Installationsmedium aus booten, so stellen Sie im UEFI/BIOS das gewünschte 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 gewünschte Start-Laufwerk auswählen können.
- Drücken Sie eine beliebige Taste, wenn Sie dazu aufgefordert werden.
- Drücken Sie in Windows Setup die Tastenkombination «Shift» und «F10», um ein Eingabeaufforderungsfenster zu öffnen.
- Öffnen Sie das diskpart-Tool, indem Sie den Befehl «diskpart» eingeben und mit der Eingabetaste (Enter) bestätigen.
- Geben Sie den Befehl «list disk» ein und drücken Sie die Eingabetaste (Enter).
- Geben Sie den Befehl «select disk ‹disk number›» ein und drücken Sie die Eingabetaste (Enter).

HINWEIS: Bei ‹disk number› ist die Nummer der Disk anzugeben, auf welche Windows später installiert werden soll. Achtung: Falls hier das USB-Laufwerk mit dem Windows 10 Installationsmedium gewählt wird, wird dieses gelöscht!

- Löschen Sie den GPT oder MBR, indem Sie den Befehl «clean [-all]» eingeben und die Eingabetaste (Enter) drücken.

ACHTUNG: Durch das Löschen des GPT oder MBR werden alle Daten auf dem System gelöscht!

- Schliessen Sie das Eingabeaufforderungsfenster und fahren Sie den PC herunter. Belassen Sie das Windows 10 Installationsmedium (USB-Laufwerk oder DVD) mit dem PC verbunden.

HINWEIS: Hier (https://docs.microsoft.com/de-de/windows-hardware/manufacture/desktop/windows-setup-installing-using-the-mbr-or-gpt-partition-style) finden Sie weitere Informationen zum Löschen des GPT und MBR sowie zur Neuinstallation von

Windows 10.

Schritt 4: Neuinstallation von Windows 10

- Starten Sie den PC.
- Sollte der PC nach dem Neustart nicht vom Windows 10 Installationsmedium aus booten, so stellen Sie im UEFI/BIOS das gewünschte 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 gewünschte Laufwerk auswählen können.
- Drücken Sie eine beliebige Taste, wenn Sie dazu aufgefordert werden.
- Installieren Sie Windows 10 mit den von Ihnen gewünschten Einstellungen.

HINWEIS: Mit dem Löschen des GPT oder MBR wurden auch die Partitionen gelöscht. Legen Sie diese wie von Ihnen gewünscht neu an.

ACHTUNG: Während der Installation von Windows 10 können Sie bereits einige Entscheidungen in Sachen Datenschutz treffen. So werden Sie gefragt, wie umfangreich Sie Diagnosedaten an Microsoft senden möchten. An dieser Stelle können Sie zunächst nur zwischen «Optionale Diagnosedaten» und «Erforderliche Diagnosedaten» wählen. Um zu verhindern, dass Windows zu viele Daten ungewollt an Microsoft sendet, wählen Sie «Erforderliche» aus. Nach der Installation von Windows 10 können Sie gewisse Einstellungen individualisieren. Warten Sie, bis Windows 10 fertig installiert ist und nehmen Sie die Einstellungen dann vor. Unsere Anleitung mit weiteren nützlichen Informationen zum Datenschutz bei Windows 10 finden Sie hier (https://www.ebas.ch/datenschutz-windows-10/).

- Installieren Sie Windows 10 mit den von Ihnen gewünschten Einstellungen zu Ende.
- Verbinden Sie den PC mit dem Internet (Netzwerkstecker einstecken).
- Aktualisieren Sie das Betriebssystem, indem Sie unten links in der Taskleiste auf das Windows-Logo klicken und «Windows Update» eingeben und mit der Eingabetaste (Enter) bestätigen. Klicken Sie anschliessend auf «Nach Updates suchen». Die Updates werden nun automatisch installiert.

Schritt 5: 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 6: Scannen der Daten

- Halten Sie die «Shift»-Taste gedrückt und schliessen Sie das externe Speichermedium (externe Festplatte) 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.

- Überprüfen Sie das gesamte System und das externe Speichermedium mit Microsoft Defender. 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 7: Zurücksichern der Daten

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

Schritt 8: Was sonst noch zu tun ist!

- Da Malware 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.