com-magazin Die Computer-Seite de

So knacken Sie Ihr Windows-Passwort

Jemand hat das Windows-Passwort geändert oder Sie haben es vergessen? Der Artikel stellt fünf Strategien vor, die Ihnen Zugriff auf jedes Benutzerkonto verschaffen - ohne dass Sie das Windows-Passwort kennen müssen.

Lesen Sie in diesem Beitrag:

Ein besonders lustiger Kollege hat am Abteilungs-Notebook rumgespielt. Ergebnis: Das alte Windows-Passwort funktioniert nicht mehr. Statt nun umständlich Windows neu zu installieren, löschen Sie einfach das unbekannte Benutzerpasswort des Spaßvogels. Anschließend legen Sie ein neues Benutzerpasswort fest.

Dieser Artikel stellt fünf Strategien vor, wie Sie Windows-Passwörter entschlüsseln und neu vergeben. Der Artikel hilft auch dann weiter, wenn Sie Ihr Windows-Kennwort vergessen haben. Sie dürfen die vorgestellten Methoden allerdings nur auf Ihrem eigenen Rechner anwenden.

Beachten Sie: Wenn Sie unter einem Benutzerkonto Dateien mit der in Windows enthaltenen Verschlüsselung EFS gesichert haben, dann können Sie auf diese Dateien nach der Änderung der Passwörter nicht mehr zugreifen.

Die Tricks auf den Seiten 2, 3 und 4 erfordern eine Installations-DVD von Windows. Falls Ihr Rechner kein DVD-Laufwerk hat – was beispielsweise bei Netbooks der Fall ist –, lassen sich die Tricks dennoch anwenden: Nutzen Sie statt der Installations-DVD dann einfach einen USB-Stick. Wie das funktioniert, lesen Sie im Abschnitt Kein DVD-Laufwerk? So starten Sie das Windows-Setup von einem USB-Stick.

Verstecktes Admin-Konto sichtbar machen

Aktivieren Sie das Administratorkonto. Damit ändern Sie alle Passwörter (für Vista/7).

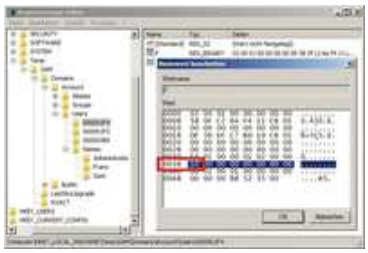
Windows Vista und 7 besitzen ein verstecktes deaktiviertes Administratorkonto. Wenn Sie dieses Konto aktivieren, lassen sich damit beliebige andere Windows-Passwörter auf dem Rechner ändern.

Beachten Sie: Das Administratorkonto besitzt standardmäßig kein Passwort. Falls jedoch auf Ihrem Rechner in der Vergangenheit über ein anderes Konto mit Administratorrechten das Passwort des Administratorkontos geändert wurde, funktioniert dieser Trick nicht.

Voraussetzung: Sie benötigen eine Installations-DVD von Windows Vista beziehungsweise 7.

So geht's: Booten Sie den Rechner mit der entsprechenden Windows-DVD. Ändern Sie dazu die Boot-Reihenfolge des Rechners im Boot-Menü oder über das BIOS.

Schritt 1: Starten Sie die Wiederherstellungskonsole. Bestätigen Sie dazu das erste Dialogfenster „Windows installieren" mit „Weiter". Klicken Sie anschließend auf „Computerreparaturoptionen". Markieren Sie im nächsten Fenster die Windows-Installation. In Windows 7 klicken Sie dazu auf „Verwenden Sie Wiederherstellungstools (…)". Bestätigen Sie mit „Weiter" und öffnen Sie die Kommandozeile mit einem Klick auf „Eingabeaufforderung".



Schritt 2: Öffnen Sie den Registrierungs-Editor, indem Sie [Windows R] drücken und **regedit** eingeben. Da Sie im nächsten Schritt die Registry über die Reparaturoptionen bearbeiten, müssen Sie zunächst die benötigten Schlüssel laden: Markieren Sie „HKEY_LOCAL_MACHINE" und wählen Sie „Datei, Struktur laden…". Markieren Sie im Ordner „C:\Windows\System32\config" die Datei „sam" und bestätigen Sie mit „Öffnen". Geben Sie einen beliebigen Schlüsselnamen ein, zum Beispiel **Temp**. Bestätigen Sie mit „OK". Im Schlüssel „HKEY_LOCAL_MACHINE" erscheint der Unterschlüssel „Temp".

Schritt 3: Aktivieren Sie das Administratorkonto. Dazu navigieren Sie zum Schlüssel „HKEY_LOCAL_MACHINE\Temp\SAM\Domains\Account\Users\Names". Markieren Sie „Administrator". Notieren Sie den im rechten Bereich im Parameter „(Standard)" in der Spalte „Typ" angegebenen Eintrag. In der Regel ist das der Eintrag „0x1f4".

Navigieren Sie zum Schlüssel „HKEY_LOCAL_MACHINE\Temp\SAM\Domains\Account\Users" und markieren Sie den Schlüssel, der genauso endet wie der zuvor notierte Eintrag. Dies ist meist der Schlüssel „000001F4". Klicken Sie doppelt auf den Parameter „F". Ändern Sie den Anfang der Zeile „0038" wie folgt ab und bestätigen Sie mit „OK" (Bild 1):

0038 10

Markieren Sie den Schlüssel „HKEY_LOCAL_MACHINE\Temp". Wählen Sie „Datei, Struktur entfernen…" und bestätigen Sie mit „Ja". Beenden Sie den Registrierungs-Editor und starten Sie den Rechner neu mit „Neu starten".

Nun können Sie sich mit dem Administratorkonto ohne Windows-Passwort anmelden. Mit dem Administratorkonto lassen sich die Windows-Passwörter beliebiger anderer Benutzer ändern.

Windows-Kennwortrücksetzdiskette verwenden

Windows Vista und 7 haben eine Funktion, die vergessene Passwörter durch neue Passwörter ersetzt.

Mit der Kennwortrücksetzdiskette lässt sich auf einfache Weise ein neues Windows-Passwort festlegen. Die Bezeichnung „Kennwortrücksetzdiskette" ist dabei irreführend: Statt einer Floppy-Disk können Sie auch einen beliebigen anderen Datenträger – etwa einen USB-Stick – verwenden.

Datenträger erstellen: Öffnen Sie in der Systemsteuerung die Einstellungen für Ihr Benutzerkonto. Klicken Sie auf „Kennwortrücksetzdiskette erstellen". Folgen Sie den Anweisungen des Assistenten.

Passwort zurücksetzen: Klicken Sie nach der falschen Eingabe eines Passworts im Anmeldefenster auf „Kennwort zurücksetzen…". Folgen Sie den Anweisungen des Assistenten.

Passwort über die Kommandozeile neu setzen

Sie booten mit der Kommandozeile und ersetzen die Passwörter beliebiger Benutzerkonten (für Vista/7).

Der folgende Trick manipuliert die Windows-Anmeldung. Sobald der Anmeldebildschirm von Windows Vista oder 7 erscheint, drücken Sie fünfmal die Umschalttaste. Statt der Einrastfunktion startet nach der Manipulation fortan die Kommandozeile. Mit ihr lassen sich die Passwörter beliebiger Windows-Benutzerkonten ändern.

Voraussetzung: Sie benötigen eine Installations-DVD von Windows Vista beziehungsweise 7.

So geht's: Zunächst brauchen Sie eine Kommandozeile. Da Sie sich ja aus Windows ausgesperrt haben, lässt sich die Kommandozeile nicht auf normalem Weg aufrufen. Starten Sie die Kommandozeile daher einfach von der Windows-DVD aus.

Booten Sie den Rechner mit der Windows-DVD. Ändern Sie gegebenenfalls die Boot-Reihenfolge des Rechners im Boot-Menü. Wenn auf Ihrem Rechner kein Boot-Menü zur Verfügung steht, dann ändern Sie die Reihenfolge über das BIOS.

Schritt 1: Starten Sie die Wiederherstellungskonsole. Bestätigen Sie dazu das erste Dialogfenster „Windows installieren" mit einem Klick auf „Weiter". Klicken Sie anschließend auf „Computerreparaturoptionen" (Bild 2).

Markieren Sie im nächsten Fenster die Windows-Installation. In Windows 7 klicken Sie dazu auf „Verwenden Sie Wiederherstellungstools (…)". Bestätigen Sie mit „Weiter" und öffnen Sie die Kommandozeile mit einem Klick auf „Eingabeaufforderung".

Schritt 2: Im Folgenden ersetzen Sie die Einrastfunktion durch die Kommandozeile. Damit Sie diesen Vorgang später aber auch wieder rückgängig machen können, legen Sie zunächst eine Sicherheitskopie der Datei „sethc.exe" an. Dabei handelt es sich um die EXE-Datei für die Einrastfunktion. Geben Sie dazu auf der Eingabeaufforderung folgenden Befehl ein, der eine Kopie dieser Datei im Verzeichnis „C:\" ablegt:

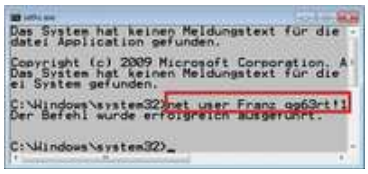
copy C:\Windows\System32\sethc.exe C:

Ersetzen Sie anschließend mit diesem Befehl die Datei „sethc.exe" der Einrastfunktion durch die Datei „cmd.exe" ,welche die Kommandozeile startet (Bild 3):

copy /y C:\Windows\System32\cmd.exe C:\Windows\System32\sethc.exe

Der Schalter /y sorgt dafür, dass die Datei „sethc.exe" ohne Rückfrage überschrieben wird.

Schließen Sie das Kommandozeilenfenster. Starten Sie dann den Rechner neu mit einem Klick auf „Neu starten".



Schritt 3: Sobald der Anmeldebildschirm erscheint, drücken Sie fünfmal die Umschalttaste. Es öffnet sich ein Kommandozeilenfenster. Die Nachfrage bezüglich der Einrastfunktion beantworten Sie mit „Nein". Mit diesem Befehl ersetzen Sie nun Windows-Passwörter (Bild 4):

net user Konto Passwort

Ersetzen Sie dabei Konto durch den Windows-Benutzernamen. Ersetzen Sie Passwort durch das neue Passwort für das Konto. Schließen Sie das Kommandozeilenfenster. Melden Sie sich anschließend mit dem neuen Passwort an.

Schritt 4: Stellen Sie nun noch den Ursprungs-zustand wieder her, indem Sie die Sicherungskopie der Datei „sethc.exe" der Einrastfunktion wieder an den ursprünglichen Speicherort kopieren. Öffnen Sie dazu die Kommandozeile mit Administratorrechten, indem Sie „Start, Alle Programme, Zubehör" wählen. Klicken Sie mit der rechten Maustaste auf „Eingabeaufforderung" und wählen Sie „Als Administrator ausführen". Geben Sie folgenden Befehl ein:

copy /y C:\sethc.exe C:\Windows\System32\sethc.exe

Beenden Sie die Kommandozeile.

Kennwort über die Systemwiederherstellung zurücksetzen

Die Systemwiederherstellung von Windows merkt sich auch Benutzer-Passwörter (für Vista/7).

Ab und zu sollte man sein Benutzer-Passwort in Windows ändern. Falls Sie dann das neue Passwort vergessen, sich aber an ein altes noch erinnern, hilft der folgende Trick: Mit der in Windows integrierten Systemwiederherstellung wechseln Sie einfach zum alten Passwort zurück.

Voraussetzung: Sie benötigen dazu eine Installations-DVD von Windows Vista beziehungsweise 7.

So geht's: Booten Sie den Rechner mit Ihrer Windows-DVD. Ändern Sie gegebenenfalls dazu die Boot-Reihenfolge im Boot-Menü. Wenn auf Ihrem Rechner kein Boot-Menü zur Verfügung steht, dann ändern Sie die Reihenfolge im BIOS.

Schritt 1: Starten Sie die Wiederherstellungskonsole. Bestätigen Sie dazu das erste Dialogfenster „Windows installieren" mit „Weiter". Klicken Sie anschließend auf „Computerreparaturoptionen". Markieren Sie im nächsten Fenster die Windows-Installation. In Windows 7 klicken Sie dazu auf „Verwenden Sie Wiederherstellungstools (…)". Bestätigen Sie mit „Weiter" und klicken Sie auf „Systemwiederherstellung".

Schritt 2: In einem neuen Fenster startet ein Assistent zum Zurückspielen eines Wiederherstellungspunkts. Wählen Sie in der Liste einen Wiederherstellungspunkt aus, der vor der Änderung des Passworts liegt (Bild 5).

Der Nachteil dieser Methode: Alle Programme, die Sie seit dem Anlegen des Wiederherstellungspunkts installiert haben, müssen Sie nun neu installieren. Welche Programme neu installiert werden müssen, teilt Ihnen Windows 7 mit, wenn Sie auf „Nach betroffenen Programmen suchen" klicken. Starten Sie das Zurückspielen des Wiederherstellungspunkts mit „Fertig stellen, Ja". Der Vorgang dauert einige Minuten.

Starten Sie den Rechner neu mit „Neu starten". Melden Sie sich anschließend mit dem alten Passwort in Windows an.

Administrator-Konto im abgesicherter Modus verwenden

XP hat ein Administratorkonto ohne Passwort. Damit lassen sich die Passwörter jedes Benutzers ändern (für XP Home).

Mit einem Administratorkonto ändern Sie die Passwörter für beliebige andere Windows-Konten. Windows XP Home bringt standardmäßig ein verstecktes Administratorkonto mit. Dieses besitzt kein Passwort.

So geht's: Booten Sie Windows im abgesicherten Modus. Drücken Sie hierfür beim Starten die Taste [F8]. Es erscheint das Menü „Erweiterte Windows-Startoptionen". Übernehmen Sie die Voreinstellung „Abgesicherter Modus" mit der Eingabetaste. Klicken Sie im Hinweisfenster auf „OK" und im Anmeldefenster auf „Administrator" (Bild 6). Bestätigen Sie die folgende Nachfrage mit „Ja".

Kennwort über eine Boot-CD knacken

Ein Tool bootet den Rechner und entschlüsselt Windows-Passwörter (für XP/Vista).

Die kostenlose Ophcrack Live-CD 2.1.0 liest in wenigen Sekunden die Passwörter von Windows-Konten aus. Dazu errechnet das Tool anhand von Tabellen aus der verschlüsselt gespeicherten Passwortdatei von Windows die Kennwörter. Diese Tabellen enthalten zuvor berechnete Passwörter in allen möglichen Kombinationen.

Da Ophcrack direkt von einer CD startet, ist keine Installation erforderlich. Die Entschlüsselung dauert je nach Kennwortlänge zwischen wenigen Sekunden und 15 Minuten.

Einschränkungen: Ophcrack entschlüsselt nur Passwörter ohne Sonderzeichen. Mit Sonderzeichen wären die benötigten Tabellen nämlich rund 50 GByte groß. Da die Passwörter unter Windows 7 anders gespeichert werden, funktioniert Ophcrack unter diesem System nicht.

Es gibt neben der vorgestellten Version 2.1.0 bereits eine Version 2.3.1 der Ophcrack Live-CD. Diese stürzte allerdings auf sämtlichen getesteten Systemen ab. Die Vorversion 2.1 entschlüsselt die Passwörter jedoch genauso zuverlässig.

So geht's: Laden Sie das CD-Abbild der Ophcrack Live-CD für Windows XP oder Windows Vista auf Ihren Rechner. Das CD-Abbild im ISO-Format brennen Sie mit einem kostenlosen Brenn-Tool wie Imgburn auf einen CD-Rohling.

Schritt 1: Installieren Sie Imgburn auf Ihrem Rechner. Wenn Sie nicht möchten, dass die Ask-Toolbar auf Ihrem Rechner installiert wird, deaktivieren Sie im Lauf der Installation im Dialogfenster „Ask Toolbar Installation" die Einstellung „I accept the license agreement (…)".

Installieren Sie anschließend die deutsche Sprachdatei für die Bedienoberfläche: Entpacken Sie das Archiv „german.zip" und kopieren Sie die Datei „german.lng" in den Ordner „C:\Programme\ImgBurn\Languages".

Schritt 2: Starten Sie Imgburn mit „Start, Alle Programme, ImgBurn, ImgBurn". Wechseln Sie auf die deutsche Bedienoberfläche, indem Sie „Tools, Settings…" wählen. Wählen Sie auf die Registerkarte „General, Page 1" und markieren Sie unter „Language" im Auswahlmenü „Deutsch (Deutschland)". Bestätigen Sie mit einem Klick auf „OK".

Brennen Sie nun das Abbild von Ophcrack auf einen CD-Rohling: Klicken Sie hierfür im Hauptfenster von Imgburn auf „Imagedatei auf Disc schreiben". Klicken Sie unter „Quelle" auf das Symbol „Nach einer Datei suchen…" und wählen Sie die ISO-Datei aus. Starten Sie das Brennen mit einem Klick auf das CD-Symbol „Schreiben".

Schritt 3: Booten Sie nun den Rechner mit der Ophcrack Live-CD für Windows XP oder Windows Vista. Ändern Sie gegebenenfalls die Boot-Reihenfolge im Boot-Menü oder über das BIOS.

Nach wenigen Augenblicken erscheint das Boot-Menü von Ophcrack. Übernehmen Sie die Voreinstellung „Ophcrack Graphic mode" mit der Eingabetaste (Bild 7). Das Tool startet. Der Vorgang dauert mehrere Minuten.

Schritt 4: Anschließend öffnet sich eine Linux-Bedienoberfläche und das Tool Ophcrack startet. Es entschlüsselt automatisch und ohne weitere Konfiguration die Passwörter aller vorhandenen Windows-Konten. In der Spalte „User" zeigt Ophcrack die Benutzerkonten an. In der Spalte „NT Pwd" steht das entsprechende Passwort (Bild 8).

Beenden Sie Ophcrack mit einem Klick auf „Exit". Starten Sie den Rechner neu.

Kein DVD-Laufwerk? So starten Sie das Windows-Setup von einem USB-Stick

Oft brauchen Sie zum Zurücksetzen von Passwörtern die Windows-DVD. Wenn Ihr Computer kein DVD-Laufwerk hat, dann nehmen Sie stattdessen einen USB-Stick.

Das Kopieren der Installations-DVD von Vista und Windows 7 auf einen USB-Stick geht in zwei Schritten: Zunächst machen Sie mit dem Kommandozeilen-Tool Diskpart Ihren USB-Stick bootfähig. Anschließend überträgt der Befehl **xcopy** alle nötigen Dateien.

Voraussetzungen: ein USB-Stick ab 4 GByte, ein zweiter Rechner mit Vista oder Windows 7 und eine Installations-DVD von Windows Vista beziehungsweise Windows 7.

Schritt 1: Stecken Sie den USB-Stick an den Rechner an. Öffnen Sie die Kommandozeile, indem Sie [Windows R] drücken, **cmd** eingeben und mit „OK" bestätigen. Geben Sie **diskpart** ein (Bild 9). Mit **list disk** erscheint eine Liste der Laufwerke. Ermitteln Sie in der Spalte „Datenträger", welche Nummer Ihr USB-Stick hat.

Geben Sie **select disk x** ein. Ersetzen Sie dabei **x** durch die Nummer des Sticks.

Geben Sie nun folgende Befehle ein und bestätigen Sie jeweils mit der Eingabetaste:

```
clean
create.partition.primary
select.partition.1
active
format.fs=fat32
assign
exit
```

Schritt 2: Legen Sie die Installations-DVD von Vista beziehungsweise Windows 7 in das Laufwerk. Geben Sie folgenden Befehl ein:

xcopy X:*.* /s/e/f Y:

Ersetzen Sie dabei **X** durch den Laufwerkbuchstaben des DVD-Laufwerks und **Y** durch den Laufwerkbuchstaben des USB-Sticks.

Nun lässt sich der Rechner mit diesem USB-Stick booten. Ändern Sie dazu die Boot-Reihenfolge des Rechners im Boot-Menü oder über das BIOS. Die Installation startet wie von der DVD.

Konstantin Pfliegl