Security Lektion 8
Datenmanagement

- ✗ Daten sichern
- ✗ Daten vernichten

✓ In diesem Kapitel dreht sich nun alles um die Fragen: Wozu Daten sichern und welche Daten sichern, wie diese Sicherung erstellen und was tun, um Daten wirklich zu vernichten.

Aufgabe

1. Daten sichern

Daten sichern Sie für Notfälle, wenn Sie aus irgendeinem Grund nicht mehr auf die Festplatte zugreifen können. Dabei können Sie sowohl Ihre Dateien als auch die installierten Programme verlieren.

Physische Sicherung

Entscheiden Sie zuerst, welche Daten zu sichern sind:

- Firmen-Datenbank, Buchhaltung und Lohnverrechnung
- Sämtliche Geschäftsagenden, Schriftverkehr, Projektdaten
- E-Mails, Favoriten / Lesezeichen exportieren und sichern
- Programme
- usw.

Aufgrund dieser Auswahl entscheiden Sie sich für physische Sicherungen. Zur Auswahl stehen unter anderem:

- Zugangskontrollen zu den Räumlichkeiten
- Sicherungskabel verwenden
  Manche Laptops sind mit einem Kensington-Schloss ausgestattet
- Inventar über die Speichermedien anlegen
  So kontrollieren Sie schnell den Bestand an Datenträgern und Geräten

Backup

Sichern Sie den Datenbestand auf externen Speichermedien:

- Externe Festplatten
- Magnetbänder
- CDs, DVDs, Blu-rays
- Server
- Online-Speicherung

Konzepte zur Datensicherung

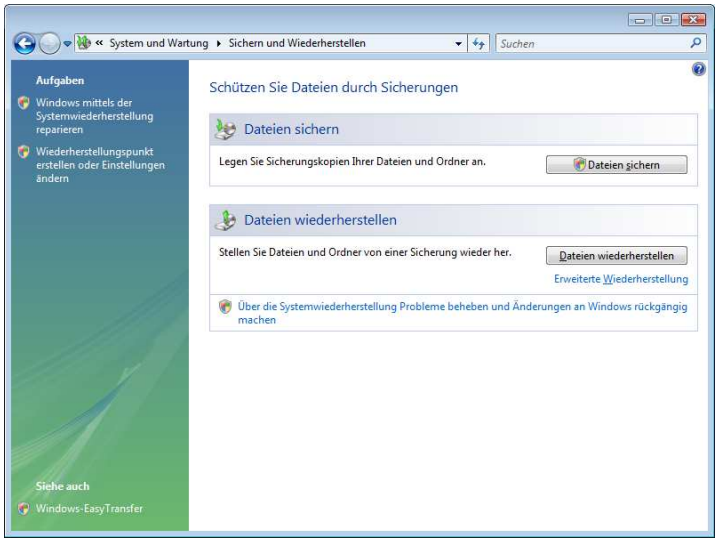
Nur eine *regelmäßige* und *häufige* Datensicherung hat Sinn. In Firmen wird dazu eine *Ablaufplanung* mit einem genauen *Zeitplan* erstellt und neben dem Speicherort auch die *Aufbewahrung* der Sicherungskopien festgehalten. Wenn es um große Datenmengen geht, wird der Speicherbedarf durch eine entsprechende *Datenkompression* verringert.

- **Regelmäßigkeit, Häufigkeit und Ablaufplanung**
  Diese Strategie hängt natürlich stark von den zu sichernden Daten ab.
  - In kleinen Büros mag es reichen, wenn eine wichtige Datei umgehend gesichert wird.
  - Eine übliche Strategie ist nach wie vor, für jeden Tag Sicherungen zu erstellen, die in der kommenden Woche wieder überschrieben werden. Die letzte Sicherung einer Woche (Freitag oder Samstag) wird behalten. Eine weitere monatliche Sicherung ebenso.
  - Fallen viele Daten an (Online-Shop) oder sind die Daten besonders sensibel (Bank), dann wird laufend gesichert.
- **Aufbewahrung**
  Bewahren Sie die Sicherungskopien so auf, dass
  - sie vor Umwelteinflüssen sicher sind (Feuer, Wasser, etc.),
  - sie vor Dieben sicher sind (Safe, abgesperrter Raum) und
  - die Lagerung den Besonderheiten des Speichermediums entspricht. Magnetische Speichermedien sind empfindlich gegen magnetische Felder und Feuchtigkeit. Optische Speichermedien sind empfindlich gegen Staub, Hitze und direktes Licht.
  - Bedenken Sie beim Sichern der Daten, dass die Speichermedien ebenfalls eine begrenzte Nutzungsdauer haben. Von Zeit zu Zeit müssen darum die gesicherten Daten überprüft und noch einmal gesichert werden.

Backup erstellen unter Windows 7

Die erste Sicherung beginnt mit einer Komplettsicherung des Datenbestandes. Unter Windows 7 verwenden Sie dazu SICHERUNG DES COMPUTERS ERSTELLEN in der SYSTEMSTEUERUNG.

Klicken Sie auf SICHERUNG EINRICHTEN (siehe Abbildung).



Folgen Sie den Schritten des Assistenten:

- Wählen Sie aus, auf welchem Speichermedium die Sicherung erstellt wird.
- Welcher Datenträger wird gesichert?
- Wie häufig möchten Sie die Sicherung erstellen? Geben Sie die Daten ein.
- Windows führt die erste Sicherung durch.

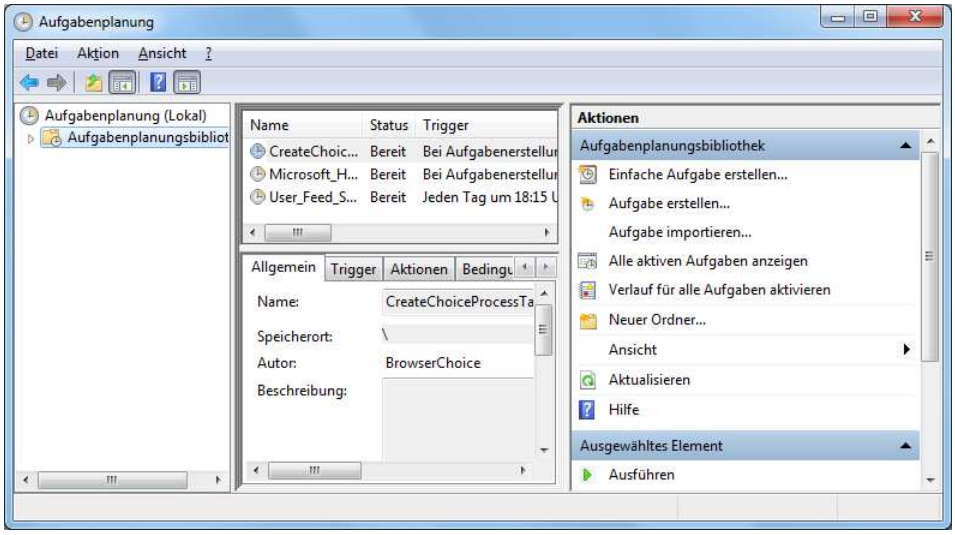
Wurden die Dateien verändert, führen Sie die nächste Sicherung durch. Nummerieren Sie diese Sicherung. (Verwenden Sie wieder den Assistenten, denn hier erkennt Windows, welche Dateien geändert wurden.)

Führen Sie so Ihre Sicherungen durch und nummerieren Sie die Versionen. Am Ende machen Sie eine zweite Komplettsicherung.

Aufgabenplanung unter Windows 7

In der VERWALTUNG erstellen Sie eine AUFGABENPLANUNG. Hier finden Sie unter anderem die erstellten Sicherungsaufträge.

Sie finden die VERWALTUNG über das Suchfeld des Startmenüs.



Sicherung wiederherstellen unter Windows 7

Beim Sichern hatten Sie die Wahl, Ihre Daten zu sichern oder zusätzlich ein Systemabbild, eine sogenannte *Image-Sicherung*, zu erstellen. Beim Wiederherstellen werden die Dateien entweder an den Originalplatz kopiert oder Sie geben im Assistenten einen neuen Ort an.

- Klicken Sie dazu in der SYSTEMSTEUERUNG den Link SICHERUNG DES COMPUTERS ERSTELLEN an.
- Klicken Sie auf EIGENE DATEIEN WIEDERHERSTELLEN.
- Folgen Sie den Anweisungen des Assistenten und starten Sie die WIEDERHESTELLUNG.

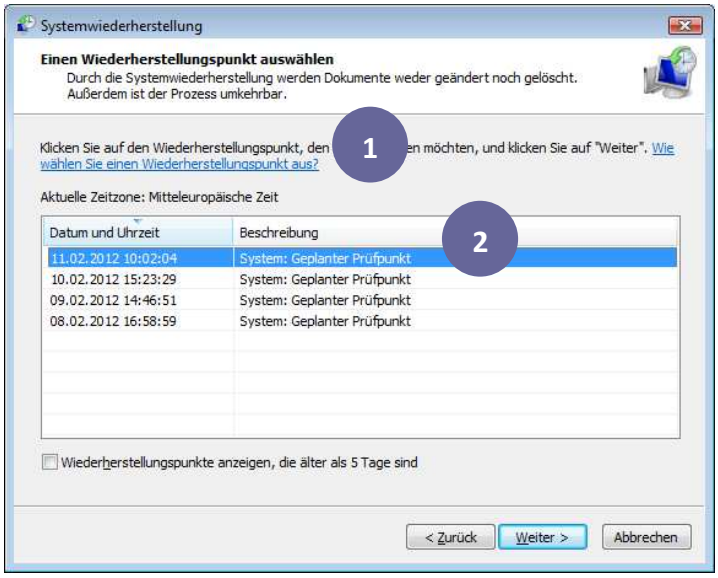
Systemwiederherstellung unter Windows 7

Öffnen Sie die SYSTEMWIEDERHERSTELLUNG. Nutzen Sie dazu auch das Suchfeld im Startmenü. Erstellen Sie im zweiten Schritt des Assistenten (siehe Abbildung) entweder

❶ einen neuen WIEDERHERSTELLUNGSPUNKT oder

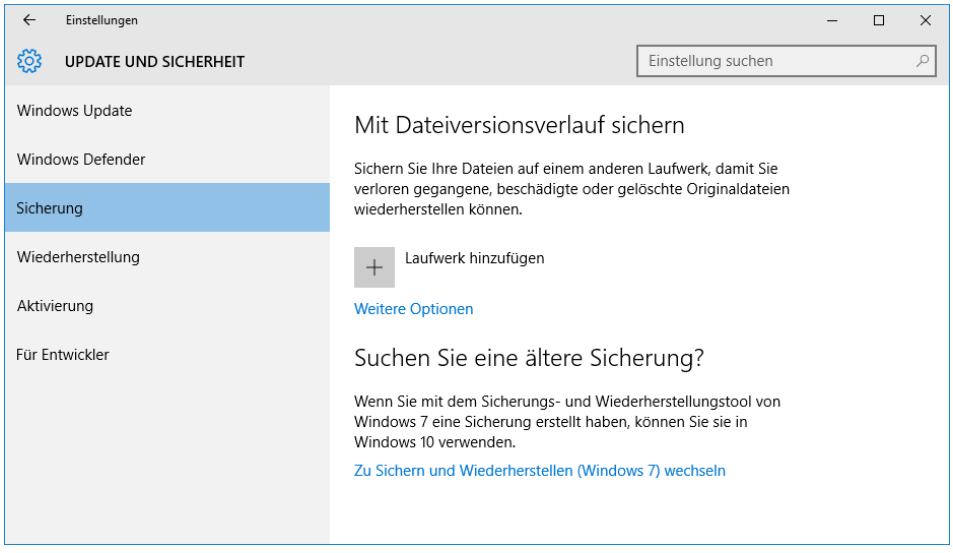
❷ wählen Sie einen Wiederherstellungspunkt aus der Liste.

Die Systemwiederherstellung betrifft das System. Sie hat keine Auswirkungen auf die Dateien!



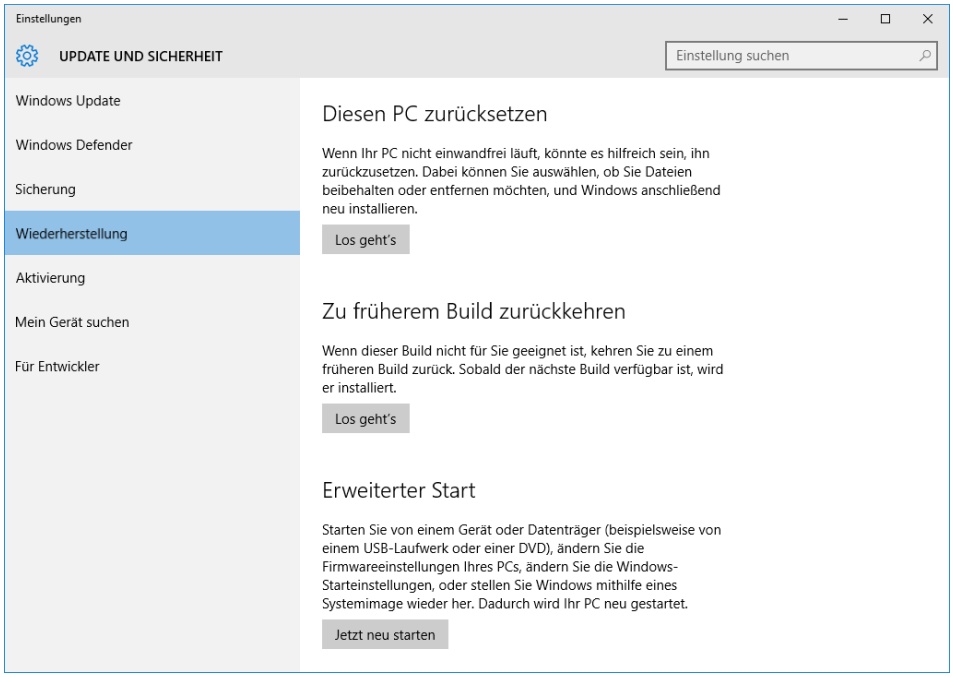
Backup erstellen unter Windows 10

Nutzen Sie die Dateiwiederherstellung, um die Daten bei Bedarf wiederherzustellen. Klicken Sie in den EINSTELLUNGEN | UPDATE UND SICHERHEIT auf SICHERHEIT (siehe Abbildung).



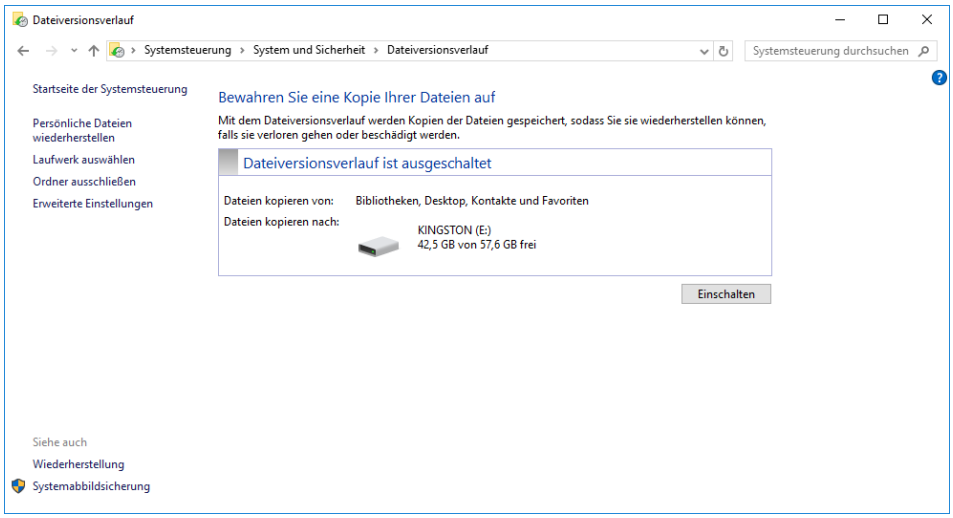
Wiederherstellung unter Windows 10

Möchten Sie den Rechner auf einen früheren Zeitpunkt zurücksetzen, dann nutzen Sie unter EINSTELLUNGEN | UPDATE UND SICHERHEIT | SICHERHEIT den Eintrag WIEDERHERSTELLUNG (siehe Abbildung).



Dateiversionsverlauf unter Windows 10

In der Systemsteuerung finden Sie den DATEIVERSIONSVERLAUF (siehe Abbildung). So können Sie persönliche Dateien auf einem externen Laufwerk sichern und im Notfall wiederherstellen



2. Daten vernichten

Wenn Sie die Dateien von einer Festplatte löschen, können die Daten mit entsprechenden Programmen wiederhergestellt werden! Sogar formatierte Festplatten lassen sich zumindest teilweise rekonstruieren. Denn Windows entfernt beim Löschen oder Formatieren in Wahrheit nur den *Verweis* auf die Dateien, nicht die Dateien selber.

Das ergibt Probleme, wenn eine defekte Festplatte weggeworfen wird und in falsche Hände kommt oder wenn Sie formatierte Festplatten weiter verkaufen möchten. Was können Sie nun unternehmen, dass Daten nicht wiederhergestellt werden können:

- Entmagnetisieren (allerdings nicht 100 % sicher)
- Shreddern
- Programme zur restlosen Beseitigung verwenden. Besuchen Sie zum Beispiel https://www.ascomp.de/ index.php?php=prog&prog=secureeraser oder www.gaijin.at/dlwipefile.php.

Sogenanntes Dumpster Diving (Mülleinertauchen) ist eine Möglichkeit, an wertvolle Daten heranzukommen. Sogar eine weggeworfene Telefonliste mag problematisch sein, weil kriminelle Personen dann wissen, wer im Unternehmen in welcher Abteilung unter welcher Nummer erreichbar ist.

Man kann es nicht oft genug sagen: Das Löschen von Inhalten ist bei vielen Diensten nicht endgültig (in sozialen Netzwerken, Blogs, Internetforen und auch Cloud-Diensten). Sind Sie sich darüber im Klaren, dass Sie Ihren Rechner und Ihre mobilen Geräte irgendwann entsorgen werden? Achten Sie unbedingt darauf, dass Sie die gespeichert Daten vernichten und nicht einfach nur löschen. Am 14. August 2016 berichtet die Online-Ausgabe von *derstandard.at* folgendes: *„Alte Rechner oder ausgetauschte Komponenten, die in Europa entsorgt werden, landen oft als Elektroschrott in Afrika. Auf Containern werden massenhafte Geräte verschifft, die dann auf Deponien landen, beispielsweise in Ghana. Was nur wenige Nutzer wissen: Lokale Händler verkaufen dann nicht nur Komponente oder Ressourcen, die sie aus den Geräten gewinnen – sondern auch intime Daten europäischer User, die sie auf den Festplatten finden.“* [1]

Sicherheit Schritt acht
Backups erstellen und Daten sicher vernichten

Übung und Selbststudium

1. Erstellen Sie auf einer CD oder DVD eine Sicherung Ihrer wichtigsten Daten. Wählen Sie die Daten dabei manuell aus.

Testen Sie Ihr Wissen

1. Wo kann man am System eine Aufgabenverwaltung einstellen, damit beispielsweise jeden Freitag eine Sicherungskopie erstellt wird?
2. Was ist der Vorteil, wenn Sie über den Assistenten Sicherungen erstellen anstatt die Daten zu kopieren?

Lösen Sie im Anschluss nun die Gesamtübung, dann haben Sie die Grundlagen in der IT-Sicherheit erworben.

[1] *Quellen: http://derstandard.at/2000042831813/Nacktfotos-Amazon-Konten-Was-auf-Altgeraeten-in-Afrika-landet und http://www.zeit.de/2014/31/elektroschrott-ghana-afrika-accraund und http://www.bild.de/bild-plus/news/ausland/ghana/hier-liegen-ihre-geheimnisse-47301698,view=conversionToLogin.bild.html*