Computersicherheit.

1. Das **Betriebssystem** und seine **Anwendungsprogramme** immer auf dem neuesten Stand halten.

- Bei **Windows** und **Mac OS X automatische Update Funktion** nutzen.
  Umfasst nicht **Updates für Programme von Drittanbietern** (Update-Funktionen der entsprechenden Programme nutzen, falls vorhanden oder zum Beispiel RSS Feeds des Anbieters für Versionsinformationen nutzen).
  Windows: Programme zur Versionsüberwachung von Drittsoftware nutzen, zum Beispiel:
  - SUMO (Software Update Monitor) http://www.kcsoftwares.com/index.php?sumo
  - PSI (Personal Software Inspector) http://secunia.com/vulnerability_scanning/personal/
- Bei **Linux** werden **alle Updates für Betriebssystem und Anwendungen der Distribution** zum automatischen Update bereit gestellt.
  Die evtl. wenigen Programme von Drittanbietern müssen manuell auf den neuesten Stand gebracht werden (RSS Feeds des Anbieters für Versionsinformationen nutzen).

2. Unter **Windows** und **Mac OS X** eine **Antiviren (AV) Software** verwenden.
   Signaturen sollten mehrmals am Tag automatisch auf dem neuesten Stand gehalten werden. AV Software sollte beinhalten:

- **Scanner-On-Demand:** Überprüfung des Systems bei Anforderung.
- **Scanner-On-Access:** Überprüfung von Dateien bei jedem Zugriff.

AV Software sollte auf folgenden Schadcode prüfen:

- Viren, Würmer, Trojaner: Programme mit Schadcode, die das Ziel haben, sich von selbst zu verbreiten.
- Makroviren: Schadcode in Bürosoftware (Textverarbeitung, Tabellenkalkulation, etc.).
- Spyware: Übermittelt Daten (Dateien) vom Rechner an Fremdrechner.
- Keylogger: Tastatureingaben werden an Fremdrechner übermittelt.
- Rootkits: Übernahme der Kontrolle des eigenen Rechners durch einen Fremdrechner im Hintergrund (Backdoor = dt. Hintertür), diese Aktivität wird verschleiert.

Bei Windows:
Übersicht und Tests von AV Software: http://www.av-test.org/en/tests/home-user/
Schutz vor Spyware, Keyloggern und Rootkits: Spybot – Search & Destroy http://www.safer-networking.org/
Bei Linux:
Bedrohung allgemein gering. AV Software für Linux untersucht in der Regel nur auf Viren des Betriebssystems Windows hin. Sinnvoll in heterogenen Netzen, wenn der Rechner als Server für Mail, Dateien etc. fungiert.
Bedrohung durch Rootkits: Scanner rkhunter.

3. Zum normalen Arbeiten am PC immer **eingeschränkte Benutzerrechte** verwenden, **Zugänge mit Passwort**:
   Passwort mindestens 8 Zeichen, Kombination aus Klein-, Großbuchstaben, Ziffern und Sonderzeichen.
   Keine Eigennamen und Begriffe verwenden, die in Wörterbüchern zu finden wären.

4. **Dateien sicher löschen**.
   Gelöschte Dateien, auch wenn sie aus dem Papierkorb gelöscht wurden, können wiederhergestellt werden! Deshalb sind gelöschte Dateien und freier Speicherplatz mit binären Mustern zu überschreiben.

- Windows: Programm Eraser http://eraser.heidi.ie/
- Mac: Kontextmenü des Papierkorbs + Befehlstaste (Papierkorb sicher löschen), "Finder" -> "Einstellungen" -> "Erweitert" -> "Papierkorb sicher entleeren" bzw. mit Festplatten-Dienstprogramm freien Speicherplatz löschen.
- Linux: Programm shred

5. **Verschlüsselung von Daten.**
   Sicherheitskritische Verzeichnisse / Dateien sind zu verschlüsseln (insbesondere auf USB Sticks und Laptops).
   - **Tresor für Passworte** - KeePass für viele Betriebssysteme inkl. mobile Geräte (Smartphones etc.) und als Portable Stick Versionen: http://keepass.info/
   - **Dateiverschlüsselung** - 7zip http://www.7-zip.org / Boxcryptor https://www.boxcryptor.com speziell für Clouds (Windows, Mac, div. Smartphone OS).

- Verschlüsselung von kompletten **Laufwerken** (auch USB Sticks) oder **Containerdateien** (virtuelle Laufwerke):
  TrueCryptNext für diverse Betriebssysteme (Windows, Mac, Linux) http://truecrypt.ch/
  Mac: Programm FileVault 2 - http://support.apple.com/kb/HT4790?viewlocale=de_DE

Datensicherung (Backup).

Was an Verzeichnissen und Dateien zu sichern ist, hängt vom Zweck der Sicherung ab. Ist es das Ziel, das komplette System eines Rechners wiederherzustellen, müssen auch sämtliche Dateien und Verzeichnisse aller Festplatten gesichert werden - **Image Sicherung** der Plattenpartitionen.

- Vorteil: Ein Rechnersystem kann komplett mit dem Stand der letzten Sicherung relativ schnell wiederhergestellt werden.
- Nachteile: Großer Zeitaufwand und sehr Speicherplatz intensiv. In der Regel können derartige Sicherungen nur über ein gestartetes zweites Hilfsbetriebssystem angelegt werden und nicht im laufenden normalen Betrieb des Rechners - deshalb auch **Cold Backup** genannt.

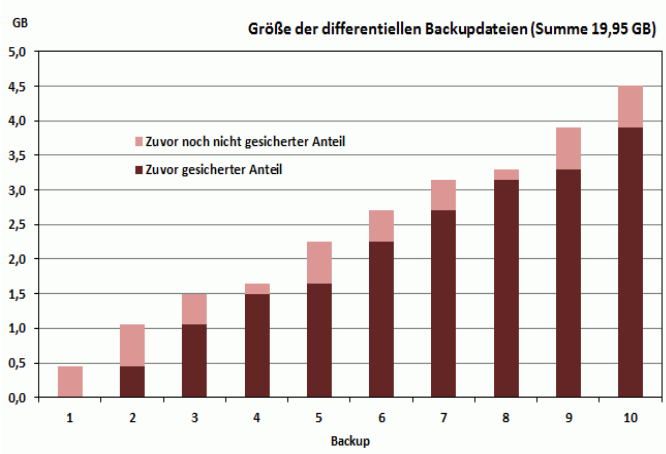
*Unter einem **Hot Backup** versteht man die Sicherung während des laufenden Betriebs, auch wenn Benutzer auf die Dateien zugreifen oder meist spezielle Programme zur Sicherung bei Servern, wie Datenbanksicherung.*

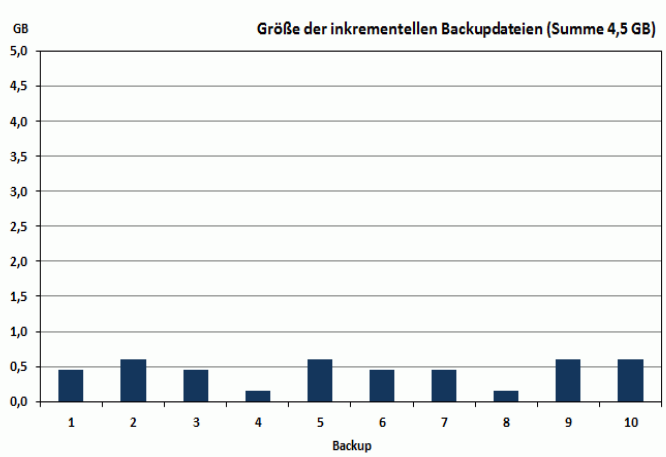
Da ein Betriebssystem im allgemeinen auch ohne größeren Zeitaufwand neu installiert werden kann, bietet es sich an, nur folgendes zu archivieren:

- **Benutzerdaten**.
  Zu den Benutzerdaten gehören alle Dateien, die ein Benutzer selbst erstellt hat.
- **Systemkonfigurationen**.
  Unter Windows die Registry Dateien bzw. das Verzeichnis /etc unter Linux/Unix.

Sicherungsstrategien.

- **Full Backup (Volle Sicherung).**
  Sicherung aller für das Backup vorgesehenen Dateien.
  - Vorteil: Einfache schnelle Wiederherstellung von Dateien.
  - Nachteil: Großer Speicherplatzbedarf, weil jedesmal auch Dateien gesichert werden, die nicht verändert wurden.
- **Differentielles Backup.**
  - Grundlage bildet ein erstelltes Full Backup. Danach werden die Dateien gesichert, die **seit dem letzten Full Backup** neu angelegt oder verändert wurden. Zur Wiederherstellung muß das letzte Full Backup und das letzte differentielle Backup eingespielt werden.
  - Vorteil: Bei Beschädigung eines differentiellen Backups kann das zuvor oder danach erstellte verwendet werden.
  - Nachteil: Mit jedem differentiellen Backup wächst die Größe der jeweiligen Sicherung an.
- **Inkrementelles Backup.**
  Grundlage bildet ein erstelltes Full Backup. Danach werden nur noch die Dateien gesichert, die **seit dem letzten inkrementellen Backup** (bei dem ersten inkrementellen Backup seit dem Full Backup) neu angelegt oder verändert wurden. Zur Wiederherstellung müssen das letzte Full Backup sowie alle inkrementellen Backups seit dem letzten Full Backup wieder eingespielt werden.
  - Vorteil: Optimale Speicherplatzausnutzung.
  - Nachteile: Ganze Folge etlicher Sicherungen sind wieder her zu stellen. Bei Beschädigung einer der inkrementellen Sicherungen können eventuell einige Dateien nicht wiederhergestellt werden.





Backup Pläne.

Bei der Planung der Backups ist zu berücksichtigen, daß nicht nur ein Backupmedium sondern mehrere verwendet werden, da ein Medium auch ausfallen kann (Beschädigung usw.). Diese Medien werden nach einem Rotationsprinzip eingesetzt, dessen Häufigkeit des Wechsels auch vom Datenaufkommen der zu sichernden Daten abhängig ist. In kommerziellen IT Einrichtungen wird das **Drei-Generationen Prinzip**

http://www.linux-community.de/Internal/Artikel/Print-Artikel/LinuxUser/2009/08/Daten-ver-sicherung/%28article_body_offset%29/2

oder das **Türme von Hanoi Prinzip**

http://www.acronis.com/support/documentation/ABR10/#1432.html

benutzt, um immer über zwei verschiedene Medien zu verfügen, mit denen man den letzten Sicherungsstand wiederherstellen kann (betrieblich beachte man die gesetzlichen Fristen!). Die Anzahl der Medien ist davon abhängig, wieweit man in der Vergangenheit liegende Sicherungsstände wiederherstellen will. Es empfiehlt sich, betrieblich auf ein kommerzielles Sicherungsprogramm zurück zu greifen.

Backup Medien.

Bei der Auswahl der Backup Medien ist auch darauf zu achten, daß diese Medien örtlich getrennt aufbewahrt werden müssen - am besten nicht in räumlicher Nähe zu den Rechnern, deren Datenbestand gesichert wird (Brand, Einbruch, Wasserschäden, etc.) und man immer mit mehreren Medien arbeitet (für den Fall, daß ein Medium zur Wiederherstellung ausfällt). Zur Datensicherung finden folgende Medien Verwendung:

- **Magnetbänder**
  Kommerziell der meistgenutzte Datenträger für Sicherungen.
  - Vorteil: Geringe Speicherkosten für Medium (ca. 10 € / 40 GB). Durch extrem große Kapazität des Bandmaterials können die Sicherungen automatisch ohne Beaufsichtigung ablaufen.
  - Nachteil: Relativ hohe Anschaffungskosten der Hardware (Consumer ab 500 €, Kommerziell ab 1500 - 5000 €).

- **Festplatten**
  Ergibt nur einen Sinn, wenn die Sicherung über ein Netzwerk auf Platten eines Servers erfolgt, der örtlich entfernt von den Rechnern mit den zu sichernden Datenbeständen steht und mehrere Festplatten am Server zur Verfügung stehen. Externe USB Festplatten sind nur eine geeignete Wahl, wenn Sie ebenfalls nicht in örtlicher Nähe zum Rechner aufbewahrt werden. Günstiger als USB Festplatten ist es, mehrere Wechselfestplatten zu verwenden (schnellere Zugriffe als bei USB, durch extrem große Kapazität heutiger Festplatten können die Sicherungen automatisch ohne Beaufsichtigung ablaufen). Backupplan im Kleinen für kleine Datenmengen mit nur 2 Medien:

	1	**2**	**3**	**4**	**5**	**6**	**...**	**...**	**...**	**...**	**...**	**...**	**...**	**...**	**...**	**...**
Platte A	**FULL**		DIFF		DIFF		...		**FULL**		DIFF		DIFF		...	
Platte B		**FULL**		DIFF		DIFF		...		**FULL**		DIFF		DIFF		...

- **USB Memory Sticks**
  Nur empfehlenswert bei kleineren zu sichernden Datenbeständen, da mehrere Sticks verwendet werden müssen

und die Anfälligkeit gegen Ausfälle relativ hoch ist. Da transportabel "in der Jackentasche" ist auch der Verlust eines Sticks zu bedenken - deshalb sollte der Inhalt auf jeden Fall verschlüsselt werden.

- **DVD**
  DVD als Backup Medien und Brenner Hardware sind zwar auch kostengünstig, jedoch sind diese Medien sehr anfällig für Datenfehler - insbesondere wieder beschreibbare Rohlinge **DVD+-RW und deshalb als Medium nicht geeignet**. Dies gilt schon für neue Rohlinge und mit der Gebrauchszeit nehmen die Schreib- und Lesefehler zu (durch Einfluss von Licht, Temperatur, Feuchtigkeit, mechanische Beschädigungen). Dagegen ist die wieder beschreibbare **DVD-RAM als Backup Medium (4,7 / 9,4 GB, Preis ab 15 €) höchst geeignet**, da für mindestens 100000 Schreibzyklen und eine fehlerfreie Speicherung von mindestens 30 Jahren durch die Hersteller garantiert wird. Einige Hersteller geben lebenslange Garantie auf das Speichermedium. Eine DVD-RAM wird wie eine Festplatte verwendet.

Festplatten RAID (Redundant Array of Independent Disk).

Ziel ist es, die Ausfallsicherheit von Festplatten zu erhöhen (die sogenannten Redundanz) und die Verfügbarkeit durch schnellere Festplattenzugriffe zu ermöglichen.

RAID kann keine Backup Sicherungen ersetzen!

Hardware RAID wird durch zusätzliche Steuerungselektronik erreicht, **Software RAID** durch softwaremäßige Organisation, in der Regel langsamer als Hardware RAID durch Belegung von Rechnerressourcen. Software RAID ist Bestandteil des Betriebssystems: bei Linux sind RAID 0, 1, 4, 5 und 6 möglich, beim Mac OSX RAID 0 und 1. bei Windows RAID 0, 1 und 5 (abhängig von der Windows Version, bei den Basis Versionen nur RAID 0).

- **RAID Level 0**
  Dateiblöcke werden zur Speicherung auf mehrere Festplatten verteilt. Durch simultane Zugriffe schnelle Datenraten - aber keine Erhöhung der Ausfallsicherheit, ist eine Platte defekt, sind alle Dateiinhalte verloren.
  Siehe Flash auf
  <http://www.tecchannel.de/storage/extra/401665/raid_sicherheit_level_server_storage_performance_festplatten_controller/index5.html>

- **RAID Level 1**
  Die Dateien werden auf jede Festplatte, mindestens 2, geschrieben (Spiegelung). Fällt eine Festplatte aus, sind die Dateien auf der/den anderen Festplatten noch verfügbar.
  Siehe Flash auf
  <http://www.tecchannel.de/storage/extra/401665/raid_sicherheit_level_server_storage_performance_festplatten_controller/index6.html>

- **RAID Level 4**
  Im Prinzip wie RAID 0, jedoch werden auf einer weiteren Festplatte (mindestens 3) Paritätsinformationen gespeichert. Eine Festplatte kann ausfallen.
  Siehe Flash auf
  <http://www.tecchannel.de/storage/extra/401665/raid_sicherheit_level_server_storage_performance_festplatten_controller/index12.html>

- **RAID Level 5**
  Im Prinzip wie RAID 4, jedoch werden auch die Paritätsinformationen auf die Festplatten verteilt, was zu schnelleren Zugriffszeiten bei großen Dateien führt, aber nicht bei kleinen. Eine Festplatte kann ausfallen.
  Siehe Flash auf
  <http://www.tecchannel.de/storage/extra/401665/raid_sicherheit_level_server_storage_performance_festplatten_controller/index13.html>

- **RAID Level 6**
  Im Prinzip wie RAID 4, die Datenblöcke einer Datei und Paritätsinformationen werden auf die Festplatten verteilt, jedoch zusätzlich werden nur die Paritätsinformationen auf eine weitere Platte geschrieben. Damit können 2 Festplatten ausfallen.

Hinweis.

Allgemeine weitergehende Hinweise, vor allem zur betrieblichen Sicherheit von IT Anlagen finden sich im **Grundschutzhandbuch** vom **Bundesamt für Sicherheit in der Informationstechnik** (BSI):

https://www.bsi.bund.de/cln_165/DE/Themen/weitereThemen/ITGrundschutzKataloge/Download/download_node.html