Maßnahmen zur PC-Sicherheit

Hardware-Maßnahmen:

- USV, Kühlung, Sauberhalten des Systems
- Raid-System
- Festplatten- und Schnittstellenumschalter
- Hardwareschutz von Festplatten
- Backup, Images auf MO, Bänder, CD/DVD, Wechselplatten

Software-Maßnahmen:

- Partitionieren der Festplatte(n)
- System aufräumen (unwichtige von wichtigen Daten trennen)
- gefährliche Dienste und Einstellungen deaktivieren
- Firewall
- Virenscanner / Anti-Dailer-Software
- Verschlüsselung, Passwörter

Stromversorgung, USV

Netzteile

Netzteile sollten mit ausreichender Leistungsreserve konzipiert werden. Ein kurzzeitiger Stromausfall (wenige Millisekunden) kann so überbrückt werden.

Überspannungsschutz

Der Überspannungsschutz hält Spannungsstöße vom System ab und schützt so z.B. gegen Blitzeinschlag in das Strom- oder Kommunikationsnetz. Einfache Systeme gibt es in Form von Steckdosenleisten, aufwendigere werden im Sicherungskasten eingebaut und schützen ganze Stromkreise.

Redundante Netzteile

Redundante Netzteile sind zwei gekoppelte Netzteile, wobei eines für die Versorgung ausreicht. Dadurch kann ein Netzteil bei Defekt, während des laufenden Betriebs, gewechselt werden.

Unterbrechungsfreie Stromversorgung (USV)

Eine USV wird zwischen Steckdose und System geschaltet. Bei Netzausfall hält sie den Betrieb des Systems für einige Minuten aufrecht.

Man unterscheidet 3 Typen:

- **Offline USV:** Die USV schaltet nur bei Spannungsausfall auf Notbetrieb um. Dadurch entstehen kurze Schaltzeiten von bis zu 4ms.
- **Line Interactive USV:** Ein Mikrocontroller überwacht die Qualität des Stroms (Frequenz, Amplitude, Phase). Wenn Anomalien auftreten, werden diese durch die USV ausgeglichen. Diese Systeme bieten auch bei Stromschwankungen sehr guten Schutz und haben kürzere Schaltzeiten.
- **Online USV:** Der Akkumulator der USV wird ständig geladen und versorgt das angeschlossene System. Damit gibt es keine Umschaltzeiten. Jedoch ist eine Prüfung und Wartung des Akkus im laufenden Betrieb nicht möglich.

Bei Aufgaben mit stark unterschiedlichen Sicherheitsanforderungen ist eine physikalische Trennung von Datenträgern und Schnittstellen zu empfehlen.

- Festplattenumschalter ermöglichen eine Auswahl zwischen mehren Festplatten und damit physisch voneinander getrennten Systemvarianten (Intranet ←→ Internet).
- Schnittstellenumschalter ermöglichen z.B. die Auswahl zwischen sensiblen Intranet und Internet (in Kombination mit den jeweiligen Festplatten).

➢ Festplattenumschalter
  - Trios II (S) Festplattenumschalter (nicht mehr im Handel)

➢ Festplatten- / Schnittstellen- Umschalter
  - Schmali-Umschaltsystem für PATA-HDs bzw. SCSI/SATA-HDs

Hardwareschutz von Festplatten

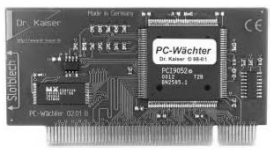
Für zu schützende Systeme, bei Gefahr von Systemmanipulationen oder für Experimente mit dem Systemen und Anwendungen ist ein Hardwareschutz von Festplatten zu empfehlen.

Ein Hardwareschutz von Festplatten (Reborn-System) schützt das Betriebssystem, Anwendungen und Einstellungen eines Computers gegen Veränderungen. Es können Dateien gelöscht, kritische Anwendungen installiert, sogar das Laufwerk C formatiert oder die Festplatte neu partitioniert werden. Beim Einschalten oder Neustart des Systems gehen alle Änderungen verloren und die Grundeinstellung ist wieder verfügbar.

- Reborn-Systeme:
  - HDD Sheriff
  - Dr. Kaiser PC-Wächter
  - HDSafe Recovery Card
  - MRS – PCI Phoenix Hardware Reborn System
  - Excelstor Gstor Plus Festplatte (GP1080)

Rebornsysteme

- **Dr. Kaiser PC-Wächter**
  - Eigentlich Software-Lösung mit Hardware-unterstützung
  - Schützt das Betriebssystem, Anwendungs-programme und Einstellungen eines PC gegen unerlaubte Änderungen
  - http://www.dr-kaiser.de



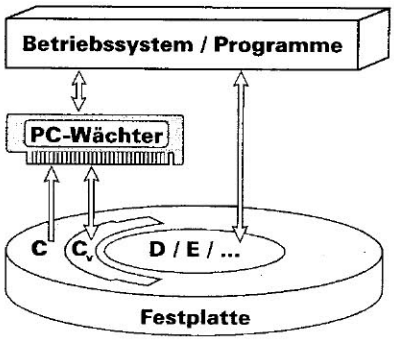
- **HDD-Sheriff**
  - Wie PC-Wächter, eher Software-Lösung
  - Daten und Konfiguration können in einer Momentaufnahme festgehalten und gezielt wiederhergestellt werden
  - http://www.hdd-sheriff.de

- **HDSafe Recovery Card**
  - Backup der gespeicherten Daten mittels Karte
  - Backup durch sichern einer Datenmenge von bis zu 12GB auf nur 1,2MB Speicherplatz
  - http://www.recoverycard.com

http://www.recoverycard.com

Funktionsweise des PC-Wächters

- Die Software des PC- Wächters richtet auf der Festplatte den versteckten Bereich **Cv** ein, in dem alle Schreiboperationen umleitet werden.
- Das Laufwerk C ist schreibgeschützt und bleibt somit unverändert.
- Wird ein Sektor von Laufwerk C gelesen, prüft der PC-Wächter, ob dieser Sektor bereits geändert (also beschrieben) wurde. Ist das der Fall, lenkt der PC-Wächter den Befehl zum Lesen auf den versteckten Bereich Cv um.
- Weitere Laufwerke, wie D, E, ... werden vom PC-Wächter nicht überwacht und dienen der Speicherung von Daten.



Datensicherung

- Da man ein System nicht absolut sicher machen kann, ist für den Fall eines Datenverlustes ein regelmäßiges Backup unerlässlich.
- Hierzu sind bei der Systemkonfiguration bereits die Laufwerke / Ordner für wichtige und unwichtige Daten festzulegen, um den Aufwand und die Datenmenge für ein Backup in Grenzen zu halten.
- Ein Backup sollte regelmäßig und auf mehreren Datenträgern durchgeführt werden.
- Um böse Überraschungen zu vermeiden, ist die Überprüfung einer fehlerfreien Rücksicherung unbedingt erforderlich.
- Nur Datenträger mit langer Lebensdauer und großer Zuverlässigkeit verwenden.
- Datenträger getrennt vom System und in geschützter Umgebung aufbewahren.

Möglichkeiten einer Datensicherung:

- Kopie
- Totales Backup
- Inkrementales Backup
- Image einer Partition
- Image eines Laufwerkes

Medien/Geräte zur Datensicherung

Gerät / Medium	Kapazität	Haltbarkeit	Kosten/GB
CD-/DVD-R	niedrig	gering	mittel
CD-/DVD-RW	niedrig	mittel	mittel
Externe Festplatte	hoch	mittel	niedrig
Bänder/ Kassetten	hoch	hoch	niedrig
Raid-System	sehr hoch	mittel bis hoch	mittel
SAN/NAS	sehr hoch	mittel	niedrig bis mittel
Flash-Speicher	mittel	mittel	mittel
MO	mittel	sehr hoch	mittel

Tipps zur Hilfe bei Datenverlust

[http://daten-web.de]

- Ruhe zu bewahren, egal was passiert ist, nicht davon ausgehen, dass Daten verloren sind
- Defekte Hardware führt oft zu Fehlverhalten der Datenträger. Schalten Sie den PC deshalb nicht ein, wenn Sie vermuten, dass es - zum Beispiel bei einem Blitzeinschlag - zu Überspannung in Ihrem Netz gekommen ist.
- Bei einem Festplattencrash hören Sie oft sehr hohe Töne, verbunden mit einem reibenden Geräusch. In diesem Fall gilt es, keinesfalls selbst Hand an die Hardware legen. Ein Neustart könnte die Festplatte endgültig zerstören. Wenden Sie sich statt dessen an ein Datenrettungslabor.
- Verwenden Sie keine Datenträger, die Hitze, Feuchtigkeit oder Verrußung ausgesetzt waren, da die Daten unwiderruflich verloren gehen können, wenn der Datenträger nicht in der staubfreien Umgebung eines Reinraums behandelt wird.
- Schütteln Sie den Datenträger nicht und entfernen Sie bei Festplatten nicht das Gehäuse.

Tipps zur Hilfe bei Datenverlust

[http://daten-web.de]

- Versuchen Sie nicht, offensichtlich beschädigte Datenträger weiter zu verwenden.
- Probieren Sie niemals, Datenträger selbst zu säubern. Am besten senden Sie den Datenträger an ein Datenrettungs-Labor.
- In vielen Fällen lassen sich die verlorenen Daten mit speziellen Software-Programmen in Eigenregie wiederherstellen. Setzen Sie solche Tools jedoch nicht ein, wenn die Anzeichen auf einen Hardware-Defekt deuten und der Computer ungewöhnliche Geräusche von sich gibt.
- Festplatten, die mit Salzwasser in Berührung gekommen sind, benötigen eine spezielle Behandlung. Salz beschleunigt die Korrosion (Zerstörung). Der Datenträger sollte daher unverzüglich in einem luftdichten Behälter an ein Datenrettungs-Labor geschickt werden.

Partitionieren der Festplatte(n)

Eine Festplatte wird in mehrer Teile (Partitionen) aufgeteilt, so dass diese logisch voneinander getrennt sind.

Es sieht dann so aus, als ob man mehrere Festplatten betreibt.

Werden Daten auf einer Partition gelöscht oder diese formatiert, hat dies keine Auswirkungen auf die anderen Partitionen.

Wird eine Partition (z.B. die Systempartition) beschädigt, hat dies keine Auswirkungen auf die anderen Partitionen.

Zu empfehlen: 5 Partitionen

- Lw C für Betriebssystem
- Lw D für Applikationen
- Lw E für sensible Daten
- Lw F für temporäre Daten
- Lw .. für Images

Empfohlene Aufteilung einer Festplatte

Physische Festplatte

Primäre Partition	**Erweiterte Partition**			
Lw C	Lw D	Lw E	Lw F	...
12 GByte	Rest	20 GByte	8 GByte	20 GByte
NTFS	NTFS	NTFS, FAT32	FAT32	FAT32
System	Applikat., Daten	Sensible Daten	Temp	Secure
aktiv	sichtbar	sichtbar	sichtbar	versteckt

Software-Maßnahmen zur PC-Sicherheit

- System aufräumen (unwichtige von wichtigen Daten trennen):
  - Temporäre Verzeichnisse einrichten (TEMP; TMP; Temporary Internet Files)
  - virtuellen Arbeitsspeicher auf X verlagert
  - Ruhezustand deaktivieren
- gefährliche Dienste und Einstellungen deaktivieren
- Systemwiederherstellung einrichten
- Remoteunterstützung deaktivieren
- Benutzerkonten einrichten
  - Support-Benutzer löschen
  - Internetgastkonto löschen
  - Hilfeassistent-Benutzer löschent
  - Administrator Passwort setzen
- Firewall (ZoneAlarm) einrichten
- Virenscanner einrichten
- Verschlüsselung, Passwörter

Sicherheitslücken von Windows XP

- **WindowsUpdate** → **deaktivieren**
- **Automatische Fehlerbenachrichtigung** → **aus**
- **Uhrzeitsynchronisation** → **aus**
- **MS Benutzer** → **entfernen**
- **MediaPlayer** → **Kontaktaufnahme deaktivieren**
- **Internet Explorer** → **Kontaktaufnahme deaktivieren**
- **ALEXA** → **deaktivieren**
- **Messenger** → **entfernen**
- **RegDone** → **setzen**
- **MS Firewall** → **deaktivieren**
- **Gemeinsame Dateien** → **Bezug löschen**
- **Aktivierung testen**

zu deaktivierende Dienste

Mit Windows werden beim Systemstart auch Dienste geladen, die eigentlich nicht benötigt werden und so das System nur unnötig ausbremsen.

Über → Verwaltung → Dienste kann man die Startart der Dienste verändern.

Es gibt für jeden Dienst 3 Startarten:

1. Automatisch: Der Dienst wird bei jedem Systemstart gestartet. Egal ob er benötigt wird oder nicht.

2. Manuell: Der Dienst wird vom System nur gestartet, wenn er benötigt wird.

3. Deaktiviert: Der Dienst wird nie gestartet, auch wenn er benötigt wird.

Beispiele zu deaktivierender Dienste

Dienste	Default-Einstellung
Automatische Updates	Automatisch
Designs	Manuell
Fehlerberichterstattungsdienst	Automatisch
Indexdienst	Manuell
Kompatibilität für schnelle Benutzerumschaltung	Manuell
NetMeeting-Remotedesktop-Freigabe	Manuell
Remote-Registrierung	Automatisch
Sekundäre Anmeldung	Automatisch
Server	Automatisch
Sicherheitscenter	Automatisch
Sicherheitskontenverwaltung	Automatisch
Taskplaner	Automatisch
TCP/IP-NetBIOS-Hilfsprogramm	Automatisch
Terminaldienste	Manuell
Windows-Firewall/Gemeinsame Nutzung der Internetverbindung	Automatisch
Windows-Zeitgeber	Automatisch

Sicherheitstools für Windows (Freeware)

Art	Name	Link
Uneraser	Recuva (ohne Installation)	http://www.recuva.com/
Antiviren-software	Avast! 4 Home Edition	http://www.avast.de/
	AntiVir Personal Edition	http://www.free-av.de/
Virtualisierungs-Software	Sun xVM VirtualBox	http://www.virtualbox.org/
Anti Spyware und Adware	Spybot – Search & Destroy	http://www.safer-networking.org/de/index.html
	XP Antispy (ohne Installation)	http://www.xp-antispy.org/
	Security & Privacy Complete	http://cmia.backtrace.org/
	Ad-Aware 2008	http://www.lavasoft.de/
Verschlüssel-lungssoftware	TrueCrypt	http://www.truecrypt.org/
Image-Software	Partition Image V 2.2 E	http://www.lab1.de/Central/Software/System-Tools/Partition_Image/
Anti MS Spy	XPY	http://xpy.whyeye.org