

# IT-NEWS KOMPAKT

## CHECKLISTE FÜR IHR UNTERNEHMEN

# EDV Risikoanalyse & IT Sicherheit

Eine Checkliste speziell für kleine und mittelständische Unternehmen.



Wir haben für Sie eine Checkliste mit den wichtigsten Punkten zum Thema IT-Sicherheit zusammengestellt - so bekommen Sie mit wenig Aufwand eine erste Selbsteinschätzung.

## Datensicherung



Die vollständige und tägliche Datensicherung ist und bleibt der wichtigste Punkt. Man kann mit seiner EDV machen was man will, solange die letzte Datensicherung verfügbar ist.

- **Zentrale Datenhaltung:** Damit optimal gesichert werden kann, sollten die Daten zentral auf dem Server und nicht auf allen PC Festplatten verteilt gespeichert werden. Dieses zentrale Verzeichnis wird dann u.a. gesichert.
- **Tägliche Sicherung:** Die Datensicherung sollte jede Nacht vollautomatisch alle Daten sichern – die Bänder sind täglich zu wechseln und der Erfolg der Sicherung muss im Sicherungsprotokoll kontrolliert werden. Bitte keine DAT Laufwerke verwenden, diese sind zu empfindlich – z.B. DLT oder Ultrium Laufwerke einsetzen, da sie betriebssicherer sind.

- **Lagerung:** Die Sicherungsbänder nicht neben dem Server liegen lassen, sondern im Tresor lagern. Mindestens einmal pro Woche sollte ein Band außer Haus gelagert werden, z.B. im Banktresor.
- **Datenbanken sichern:** E-Mail Server und Datenbanken haben besondere Anforderungen an die Datensicherung. Bitte bei dem Hersteller erfragen, wie die Daten korrekt gesichert werden können. Evtl. kann man Zusatzsoftware, sog. Sicherungsgagents, kaufen oder Datenbankdumps einrichten.

## Server



Den Servern kommt eine besondere Bedeutung zu. Wenn einer ausfällt, spüren das in der Regel alle Anwender bei Ihnen im Unternehmen.

- **Server von Markenherstellern mit Garantie:** (z.B. HP, Fujitsu-SIEMENS, DELL) Markenserver mit möglichst langer Herstellergarantie (3 oder 4 Jahre) inkl. Vor-Ort-Service für Ersatzteile kaufen. Wichtige Server nach Ablauf der Garantie durch Neue ersetzen.
- **Festplatten:** Die Server-Festplatten doppelt als Spiegelfestplatten oder Festplattenverbund (RAID5)

auslegen.

- **Benutzer:** Für jeden Benutzer sollte ein eigenes Konto mit individuellem Kennwort auf dem Server angelegt werden. Kennwörter sollten sicher sein (mind. 8 Zeichen, eine Kombination aus Buchstaben, Zahlen und Sonderzeichen). Alle 3 Monate muss das System ein neues Kennwort fordern. Nach 3-maliger falscher Anmeldung sollte das Konto gesperrt werden.
- **Benutzerrechte:** Benutzerrechte so einstellen, dass jeder nur an die Daten und Programme kommt, die er benötigt – nicht jeder sollte uneingeschränkten Zugriff haben. Benutzer dürfen keine Administratorrechte im System haben!
- **Überwachung:** (am besten durch einen externen Dienstleistungspartner) Die wichtigen Server auf freien Speicherplatz, Temperatur und Zustand der Datensicherung etc hin überwachen. Hierfür kann man Systeme wie z.B. den Microsoft Operations Manager (MOM Server) verwenden.
- **Standort:** Der Server sollte in einem separaten Raum oder in einem verschlossenen Serverschrank stehen. Der Raum sollte am Besten fensterlos und kühl sein wie z.B. der Keller. Falls der Raum im Sommer über 25 Grad warm werden sollte, bitte an eine kleine Klimaanlage denken.
- **Updates:** Die Server sollten immer aktuelle Updates erhalten, da diese regelmäßig bekannt werdende Sicherheitslücken schließen. Diese Updates sollten bei wichtigen Servern manuell eingespielt

werden, da es nach dem Update das Risiko gibt, dass der Server evtl. nicht korrekt startet.

- **Dokumentation:** Erstellen Sie eine Liste aller Kennwörter und heben Sie diese an einem sicheren Ort auf.
- **Stromschwankungen:** Schützen Sie vor allem Server durch eine vorgeschaltete USV (unterbrechungsfreie Stromversorgung). Diese fängt Stromschwankungen ab und kann bei einem längeren Stromausfall den Server korrekt herunterfahren, damit keine Daten zerstört werden. Es empfiehlt sich eine USV auch für wichtige PCs, Switches etc. zu installieren.
- **Stromgenerator:** Wenn der Strom länger ausfällt, kann man mit einer kleinen Notstromversorgung arbeiten, damit Sie die wichtigsten IT-Systeme betreiben können z.B. von Kipor. Ein mittleres Gerät mit Dieselantrieb gibt es schon ca. 1.500,- Euro.

## Internet & E-Mail



**Früher hat man sich Viren über Disketten oder CDs eingefangen. Heute kommen ca. 80% der Schädlinge per E-Mail im Unternehmen an.**

- **Zentraler Internetzugang:** Es sollte nur eine zentrale Leitung ins Internet geben. Diese muss mit einem guten Router (z.B. Lancom) oder einer Firewall (z.B. Watchguard) abgesichert werden.
- **Verschlüsselung wichtiger E-Mails:** E-Mails sind offen wie eine Postkarte. Wenn man wichtige Informationen sicher verschicken möchte, kommen diese Informationen in eine eigene Datei und diese wird verschlüsselt verschickt, z.B. mit Utimaco PrivatCrypto (sehr einfach zu bedienen).
- **Spam:** Lästige Werbe E-Mails bekommt man zum Teil mit einem Spamfilter z.B. von GFI oder mit dem IM-Filter vom MS Exchange Server 2003 in den Griff.

- **Anti-Viren-Scanner:** Auf dem Server sollte eine netzwerkweite Anti-Viren-Lösung z.B. von Trend Micro installiert sein, die insbesondere auch den E-Mail Verkehr überwacht. Sie sollte sich mehrfach täglich aktualisieren und auch alle PCs im Netzwerk in die Überwachung mit einbeziehen.
- **Einwahl ins Unternehmen:** Früher hat man sich per ISDN mit Rufnummernerkennung oder automatischem Rückruf in das EDV Netzwerk eingewählt. Heute macht man das in der Regel über einen verschlüsselten VPN Zugang, über die zentrale Firewall. Diese Zugänge sollten nur an Benutzer vergeben werden, die diesen Zugang wirklich benötigen.

## Kritische Anwendungen



**Eine Spedition muss sicherstellen, dass die Frachtbriefe immer ausgedruckt werden. Eine Unternehmensberatung kann ohne E-Mail System nicht arbeiten – und bei Ihnen?**

- **Was ist wichtig:** Listen Sie die für Sie wichtigen Anwendungen auf.
- **Wichtige Komponenten:** Welche Hard- und Software ist nötig, damit die Anwendung läuft. Diese für die Anwendung benötigten Komponenten evtl. doppelt auslegen bzw. Reserven vorhalten.
- **Kosten:** Was kostet ein Ausfall? Ab welcher Ausfallzeit wird es unternehmenskritisch?
- **Notfallplan:** Wer erledigt was und in welcher Reihenfolge bei einem Ausfall?
- **Telefonliste:** Liste mit allen Namen und Telefonnummern von Unternehmen und Personen die zur Problemlösung benötigt werden erstellen.

## PC Arbeitsplatz



**Der PC sollte nur die Programme installiert haben mit denen gearbeitet wird. Alle erstellten Dateien sollten zentral auf dem Server abgespeichert werden - im Fall eines Defektes wird nur der PC neu installiert und mit den zentral gespeicherten Daten kann sofort weiter gearbeitet werden.**

- **Anti-Virus:** Sicherstellen, dass der Client einer netzwerkweiten Anti-Viren-Lösung installiert ist.
- **Virenbefall oder Hacker:** Falls Sie glauben, dass ein Virus auf Ihrem PC wütet oder ein Hacker bei Ihnen drauf ist, bitte den PC einfach ausschalten und von allen Kabeln trennen. Anschließend umgehend den EDV Betreuer informieren.
- **Abwesenheit:** Nach ca. 15 Minuten Untätigkeit sollte der Bildschirmschoner mit Kennwortschutz automatisch aktiv werden.
- **Sicherheit:** Die integrierte Windows Firewall aktivieren. Zu finden in Windows unter Start – Systemsteuerung – Sicherheitscenter.
- **Updates:** Windows Update so einstellen, dass Sicherheits-Patches automatisch heruntergeladen und installiert werden.
- **USB Sticks:** Mit Programmen wie DeviceLock oder Safend Protector kann man den Datenklau via USB Sticks etc. verhindern.
- **Sichere Dateiablage:** Verwenden Sie für wirklich sensible Daten unbedingt einen Daten-Tresor, z.B. Utimaco PrivateDisk. Mit diesem Verfahren sind die Daten auch vor den Blicken der EDV Administratoren sicher.

## Notebooks



Für Notebooks gelten die gleichen Regeln wie für PCs. Da sie mitgenommen werden, befinden sich oft auch Daten auf den Notebook-Festplatten. Leider sind die Geräte auch bei Dieben beliebt und sensible Daten dürfen nicht in falsche Hände geraten.

- **Datensicherung:** Dateien nicht einfach auf der Festplatte speichern, sondern in einem Offline Ordner – dieser wird bei jedem Anmelden am Firmennetzwerk synchronisiert und von der zentralen Datensicherung erfasst. Für die Datensicherung unterwegs oder im Homeoffice eine USB Festplatte verwenden z.B. von Freecom.
- **Festplattenverschlüsselung:** Für den Fall eines Verlustes die Festplatte vollständig verschlüsseln z.B. mit Utimaco SafeGuard Easy. Nach dem Verlust ist zwar das Notebook weg, aber Sie stellen sicher, dass niemand die Daten auslesen kann.
- **Funkanbindung:** Bluetooth und WLAN sind unsicher. Bitte nur aktivieren, wenn es benötigt wird und danach wieder ausschalten. Besonders vorsichtig muss man vor allem an Orten mit vielen Personen sein, wie z.B. an Flughäfen oder Bahnhöfen – denn hier könnte jemand heimlich auf Datenklau via Funkverbindung unterwegs sein.

## Blackberry und Windows Mobile PDAs



Diese Geräte haben alle Outlookinformationen auf kleinstem Raum dabei – daher auch diese Informationen vor unbefugten Blicken schützen.

- **Zentrale Administration:** Die Geräte sollten im Unternehmen zentral mit einheitlichen Sicherheitseinstellungen betrieben und von den Benutzern nicht verändert werden können.
- **Bei Verlust:** In diesem Fall können die Geräte über die zentrale Administration deaktiviert und die Daten gelöscht werden.
- **Kennwortschutz:** Alle Geräte sollten nur nach Eingabe eines Kennwortes verwendet werden können. Der Kennwortschutz sollte sich automatisch nach 5 Minuten Nichtbenutzung wieder aktivieren.
- **Speicherkarten:** Wenn Sie hierauf wichtige Daten abspeichern, diese bitte extra verschlüsseln, da hier der Kennwortschutz nicht greift, sobald die Speicherkarte in einem anderen Gerät ausgelesen wird.
- **Datenfunk:** Wie bei den Notebooks bitte Bluetooth und WLAN nur aktivieren wenn sie benötigt werden, danach wieder deaktivieren.

## IHR ANSPRECHPARTNER



**Christian Dura,**  
**IT-Consultant der**  
**EICKELSCHULTE AG,**  
berät Sie gerne in allen  
Fragen rund um das  
Thema IT-Sicherheit  
Tel. 08151 - 77 04 - 17  
c.dura@eickelschulte.de