



Joachim Geffken



IT Sicherheit –
Von Ausfallschutz
bis Virenabwehr.



Mindeststandards,
Prävention und
Notfallplanung

Physischer Zugang.

Logischer Zugang.

Externe Zugriffe.

Betriebssicherheit.

Ausfallsicherheit.

Datensicherheit.

Datenschutz.

Wiederanlauf.

Katastrophenfall.





Mindeststandards
physischer Zugang

Zugang streng limitieren.

Server in den verschlossenen
Systemschrank.

Schlösser vor die Wechsel-
datenträger (Diskette, CD).

Tastaturen sperren.

Screen-Saver mit Passwort und
kurzer Einschaltzeit.

Datenträger in den Safe.





Mindeststandards
logischer Zugang

Passworte überall.

Wirkliche Passworte!!!

Alle Mitarbeiter auf Passwort-
Sicherheit verpflichten.

Gestufte Berechtigungen.

Passwort-Dokumentation in
den Safe in einen versiegelten
Umschlag.

Mitarbeiterwechsel =
Passwortwechsel.

Passworte vierteljährlich wechseln.





Mindeststandards externe Zugriffe

Dial-in Ports nur bei Bedarf öffnen.

Service-Zugänge nur bei Bedarf öffnen.

Service-Partner zur Protokollierung ihrer
Arbeiten verpflichtet.

Service-Partner auf Datensicherheit und
Haftung für Schäden vertraglich verpflichtet.

Mindestens einen externen Sicherheitscheck
pro Jahr.





Mindeststandards Betriebssicherheit

Email- und Web-Server bevorzugt
auslagern.

Firewall und Viruswall sind Muß für
den Web-/Email-Serverbetrieb.

Viruscheck für ein- und
ausgehende Emails und für
Webseiten.

Sicherheitsstandards in der Regel
auf "Mittel" setzen.

Problembewußtsein für
Attachments, Active-X und
dergleichen schaffen.





Mindeststandards
Ausfallsicherheit

Überspannungsschutz.

Unterbrechungsfreie
Stromversorgung.

Ersatzsystem mit gleichem
Softwarestand.

Stand-alone System beim
Serverbetrieb.

Datensicherung (Disc-Image und
Medien Backup z.B. auf DDS
Band).

Restore (Ernstfall) halbjährlich
proben. Vorher Extrasicherung!!





Mindeststandards Datensicherheit

Tägliche Datensicherung
(Medien).

Monatliche Disc Image
Sicherung (außerdem nach
Umstellungen).

Restore halbjährlich proben.

Wiederanlauf vom Disc Image
1xjährlich testen. (Achtung:
Spezialistenarbeit!).

Datensicherungsmedien täglich
auslagern.





Mindeststandards Datenschutz

Mitarbeiter auf Einhaltung des
Datengeheimnisses verpflichten.

Sofern erforderlich, einen
Datenschutzbeauftragten
schriftlich bestimmen.

Auch Aushilfen, die mit perso-
nenbezogenen Daten arbeiten,
zählen bei der 4-Personen-
Grenze gem. §4f BDSG mit!

DGV Merkblatt „Datenschutz im
Golfclub“ beachten. Im Zweifel
Rechtsrat einholen.





Mindeststandards Wiederanlauf

Systeme regelmäßig (täglich-
mindestens aber wöchentlich)
rebooten.

USV auf geordnetes Herunter-
fahren der Systeme testen.

Notverarbeitung innerhalb einer
Stunde (notfalls auf einem stand
alone System) ohne Einsatz von
Spezialisten sicherstellen.

Rekonstruktion innerhalb von 24
Stunden (ggffls mit Expertenhilfe)
gewährleisten.





Mindeststandards Katastrophenfall

Notfallplan für den totalen Systemuntergang (Feuer, Überschwemmung etc.) erstellen und extern bereithalten.

Potenziellen Ersatzraum mit Strom- und Netzanschluss festlegen.

Not-Ersatzsystem bereithalten.

Experten für Rekonstruktionshilfe bestimmen.

Ach ja – und was ist mit den
papiernen Unterlagen?



