



Technische Schutzmaßnahmen
(z.B. Firewalls, Virens Scanner, Spam-Filter etc.)

Bestimmung eines IT-Verantwortlichen



Berechtigungsmanagement



PCI-DSS-Regeln bei Kredit- oder Debitkarten-Transaktionen

Physische Sicherungsmaßnahmen
(z.B. für den Zugang zu Serverräumen)



Überspannungsschutz

Abwehrstrategien gegen DoS-Attacken



Tägliche Datensicherung (Back-up) sowie deren sichere Aufbewahrung



Passwort-Richtlinien



Verschlüsselung schützenswerter Daten



Sensibilisierung der Mitarbeitenden und Sicherheits-Trainings

Cyber-Risiken

Checkliste.
Überprüfen Sie Ihren Sicherheitszustand.

Haben Sie an diese Punkte gedacht?



Patch- und Update-Management