FIREWALL CHECKLISTE

- [ ] **Whitelisting statt Blacklisting**
- [ ] **Top down Regeln**
- [ ] **Implicit Deny all**
- [ ] **Firewall Zugriff reglementieren**
- [ ] **Updates durchführen**
- [ ] **Change Management**
- [ ] **Logs sichten**
- [ ] **Physische Sicherheit beachten**

INMODIS
IT-Sicherheit für Ihr Unternehmen

FIREWALL CHECKLISTE

Whitelisting statt Blacklisting

Whitelisting definiert was erlaubt ist, alles andere ist explizit verboten. Dieses Vorgehen sollte gegenüber Blacklisting bevorzugt werden.

Top down Regeln

Oben sollten die spezifischsten Regeln stehen, weiter unten Allgemeine. Grund ist, dass Regeln von oben nach unten ausgewertet werden.

Implicit Deny all

Implicit Deny sollte immer die letzte Regel sein, dadurch wird alles, was nicht vorher erlaubt wurde, verboten.

Firewall Zugriff reglementieren

Nur ausgewählte Mitarbeiter mit dem nötigen Fachwissen sollten Veränderungen an der Firewall vornehmen können.

Updates durchführen

Angriffe verändern sich mit der Zeit, die Firewall sollte deshalb immer auf dem aktuellsten Stand der Technik sein.

Change Management

Firewall Regeln müssen evtl. angepasst werden, wenn neue Geräte dem Netzwerk hinzugefügt werden. Hierfür sollte ein Prozess existieren.

Logs sichten

Logs liefern Aufschluss über erfolgte Angriffe und mögliche Kompromitierungen und sollten deshalb regelmäßig gesichtet werden.

Physische Sicherheit beachten

Eine perfekt eingestellte Firewall bringt wenig, wenn sie für jeden zugänglich und somit auch manipulierbar ist.