mdexExperts
IP-Sicherheit Checkliste

ISO 27001 datenschutz cert gültig bis: 08/17 DSC.265.08.2014 ULD Datenschutz

Wie Sie Ihre öffentlichen IP-Zugänge richtig absichern

1. Passwortsicherheit erhöhen

Ändern Sie bei Ihren Netzwerkgeräten und Routern unbedingt die werksseitig voreingestellten Passwörter und stellen Sie ein sicheres Passwort ein.

2. Firewall aktivieren

Sichern Sie Ihre erreichbaren Netzwerkgeräte mit einer Firewall ab. Falls Sie einen mdex Mobilfunk-Router einsetzen, informieren Sie sich über die jeweiligen Firewall-Einstellungen in der mdex Router Dokumentation.

3. Nicht benötigte Dienste abschalten

Deaktivieren Sie alle nicht benötigten Dienste auf Ihren erreichbaren Endgeräten. Achten Sie insbesondere auf administrative Dienste, wie z.B. SSH (Port 22), Telnet (Port 23) oder bei einem Windows Server den RDP Port 3389 für „Remote Desktop“.

4. Weiterleitung nur erforderlicher Ports

Deaktivieren Sie die Weiterleitung (Forwarding) aller Ports und aktivieren Sie ausschließlich die Weiterleitung tatsächlich benötigter Ports. Mögliche Forwarding-Einstellungen entnehmen Sie der Dokumentation Ihres Routers.

5. Regelmäßige Softwareupdates durchführen

Mit regelmäßigen Softwareupdates des verwendeten Routers werden nicht nur Gerätefunktionen optimiert, sondern auch bekannt gewordene Sicherheitslücken geschlossen. Schützen Sie so Ihre angeschlossenen Endgeräte vor den Zugriffen Unbefugter und anderen IT-Bedrohungen.

6. Datenübertragung verschlüsseln

Die Datenübertragung über das Internet sollte verschlüsselt erfolgen. Die meisten Router und Netzwerkgeräte unterstützten entsprechende Verschlüsselungsprotokolle, wie z.B. IPsec oder OpenVPN.

7. Mitarbeiter sensibilisieren

Weisen Sie Ihre Mitarbeiter auf mögliche Gefahren aus dem Internet hin, so dass diese keine Dateianhänge von unbekannten Absendern öffnen oder Dateien von unbekannten Internetseiten herunterladen. Reduzieren Sie so das Risiko einer Infizierung Ihrer Netzwerkgeräte durch Schadprogramme (z.B. den Verschlüsselungstrojaner Locky).