

**Computer****Sicherheit im WLAN optimieren****Archiv-Nr. 214**

- Bei Neueinrichtung: WLAN-Netz wird per Kabel konfiguriert oder zumindest mit verschlüsselter Funkverbindung (HTTPS oder SSH).
- MAC-Filter (Media Access Control) wird zugelassen, um nur ausgewählten Rechnern den Zugang zum Netz zu gestatten.
- Automatische Zuweisung von IP-Adressen per DHCP (Dynamic Host Configuration Protocol) ist zu Gunsten der MAC-Filtertabelle deaktiviert.
- Router-Passwort des Auslieferungszustandes wurde durch eine sichere Kombination (Zahlen, Groß- und Kleinbuchstaben sowie Sonderzeichen) ersetzt.
- Fernkonfiguration ist abgeschaltet.
- SSID (Service Set Identifier = Netzwerkname im Auslieferungszustand) ist geändert.
- SSID Broadcast ist abgeschaltet, um ständiges Senden des Netzwerknamens zu unterbinden.
- Verschlüsselung per WPA oder WPA2 wird statt des weniger sicheren WEP verwendet.
- Geräte, die kein WPA beherrschen, wurden ersetzt.
- Stärke des WLAN-Funksignals wurde per Administrations-Tool (und/oder Positionierung der Antenne) so eingestellt, dass der Funk das Gebäude nicht oder nur minimal verlassen kann.
- WLAN-Netz wird nur eingeschaltet, wenn es wirklich gebraucht wird.
- Firewall ist aktiviert
- Paketfilter ist aktiviert
- Speicherung von Statusinformationen (Logs) ist aktiv; die erstellten Berichte werden regelmäßig auf unberechtigte Zugriffsversuche geprüft.
- Support-Seiten des Herstellers werden regelmäßig auf Software-Updates geprüft.

Erstellt: Juni 2007