Sichere Funknetze

Funknetzwerke werden in Verwaltung, Wirtschaft und im Privatbereich immer beliebter. Mit ihrem Einsatz sind Risiken verbunden, die die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der im Netzwerk übertragenen und verwalteten Daten gefährden.

Neben den heute bekannten technischen Schwächen der WEP-Verschlüsselung und der Überwindbarkeit anderer herstellerseitiger Absicherungsmethoden sind oftmals die mangelnden Kenntnisse der Betreiber sowie die vermeintlich einfach einzurichtenden Geräte Hauptursachen für ungesicherte oder schwach gesicherte Funknetze.

Selbst bei Aktivierung aller herstellerseitigen Sicherungsfunktionen können damit nur Gelegenheitsangriffe abgewehrt werden. Einem ernsthaften zielgerichteten Angriff muss darüber hinaus mit zusätzlichen technischen und organisatorischen Maßnahmen begegnet werden.

Diese Checkliste bietet einen Überblick über verfügbare Absicherungsmöglichkeiten. Dazu gehören herstellerseitige technische Möglichkeiten der Access Points selbst sowie die Absicherung des drahtlosen Netzwerkverkehrs bis hin zur Sicherung der mobilen Endgeräte (Notebook, PDA, etc.). Eine Client-Sicherung ist insbesondere bei Nutzung von Hotspots erforderlich.

Für bereits existierende WLAN-Netze kann anhand dieser Checkliste leicht überprüft werden, welche Maßnahmen bereits ergriffen wurden. Für geplante WLAN-Netze stellt sie ein geeignetes Hilfsmittel zur Produktauswahl dar. Die organisatorischen Maßnahmen sollten in einem Sicherheitskonzept schriftlich fixiert und regelmäßig geprüft werden.

Weiterführende Hinweise finden Sie im Internet unter:
www.lfd.niedersachsen.de

Sichere Konfiguration

Durch einfaches Ankreuzen können Sie überprüfen, ob Ihr Access Point richtig konfiguriert ist bzw. den sicherheitstechnischen Mindestanforderungen entspricht.

- ☐ Standard SSID geändert (kein Rückschluss auf Betreiber)
- ☐ SSID Broadcast am Access Point abgeschaltet
- ☐ Standard Kennwort für die Access Point Konfiguration geändert
- ☐ Konfiguration des Access Points ist nur von Clients aus dem LAN möglich sein
- ☐ MAC Adress-Filterung am Access Point eingeschaltet
- ☐ WEP Verschlüsselung aktiviert (mindestens 128 Bit)
- ☐ WEP-Authentifikationsmethode von „Shared Key“ auf „Open“ gewechselt
- ☐ DHCP-Server am Access Point deaktiviert
- ☐ Aufstellungsort und Antennencharakteristik des AP optimiert
- ☐ Reichweite des AP durch Reduzierung der Sendeleistung beschränkt

Sicherer Betrieb

Diese Maßnahmen sollten Sie ergreifen, um einen sicheren Betrieb zu gewährleisten.

- ☐ Regelmäßiger Wechsel der WEP-Schlüssel auf allen Geräten
- ☐ Sicherheitsrelevante Firmware-Upgrades durchführen
- ☐ WLAN nur bei Bedarf einschalten
- ☐ Protokollierung und regelmäßige Protokollauswertung

Absicherung

Erst durch zusätzliche Maßnahmen kann das Funknetz wirksam geschützt werden.

- ☐ Verwendung kryptografischer Verfahren (IPSec, SSL)
- ☐ Zertifikatsbasierte Authetifikation der Clients
- ☐ Anbindung der Access Points über eine Firewall (VPN)

Client-sicherung

Durch geeignete Tools sollte das an das WLAN angebundene Endgerät zusätzlich gesichert werden. Hier ist insbesondere die lokale Verschlüsselung der Daten zu empfehlen.

- ☐ Personal Firewall
- ☐ Virenscanner (regelmäßig aktualisiert)
- ☐ Verschlüsselungstool für gespeicherte Daten

Diese Aufzählung stellt die Mindestanforderungen an die Client-Sicherheit dar. Hinzu kommen die Sicherungsmaßnahmen für Betriebssysteme und Anwendungen.

Notizen:

Glossar

AP	Access Point; Funkschnittstelle des Netzwerkes
Client	An das Netzwerk angeschlossene Endgeräte wie PCs, Notebooks oder PDA
DHCP	Dynamic Host Configuration Protocol; ermöglicht die automatische Vergabe von IP-Adressen
Hotspot	Bereich, der mit einem Funknetzwerk ausgestattet ist, oft auch öffentlich.
IP	Internet Protocol
IPSec	Internet Protocol Security; dient der Verschlüsselung
LAN	Local Area Network
MAC-Adresse	Media Access Control; Seriennummer einer Netzwerkkomponente, die durch den Hersteller vergeben wird
PKI	Public Key Infrastrukture
SSID	Service Set Identity; „Netzwerkname“ des Funk-LANs
SSID-Broadcast	Möglichkeit, den Namen des Funknetzwerkes bei einer Suche anzeigen zu lassen.
SSL	Secure Socket Layer; dient der Verschlüsselung
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	WiFi Protected Access

Wenn Sie mehr

wissen | wollen

Der Landesbeauftragte für den Datenschutz Niedersachsen

Schreiben	Postfach 221 30002 Hannover
Persönlich	Brühlstr. 9
Anrufen	(0511) 120-4500
Faxen	(0511) 120-4599
Surfen	www.lfd.niedersachsen.de
E-mailen	poststelle@lfd.niedersachsen.de

Der Landesbeauftragte für den Datenschutz Niedersachsen

daten schutz

Sichere Funknetzwerke

Der Landesbeauftragte für den Datenschutz Niedersachsen