CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Sicherheit in drahtlosen Netzwerken

Typen drahtloser Netzwerke

Wireless Local Area Network (WLAN):

- WLANs ermöglichen die drahtlose Vernetzung innerhalb eines begrenzten Bereichs wie eines Hauses, Büros oder Campus.
- Am häufigsten basieren sie auf den IEEE 802.11 Standards (z.B. Wi-Fi).
- Verwendung in Haushalten, Büros, öffentlichen Hotspots.

Wireless Personal Area Network (WPAN):

- WPANs sind für die Vernetzung von Geräten innerhalb einer sehr kurzen Reichweite (typischerweise ein paar Meter) gedacht.
- Beispiele sind Bluetooth und Infrarot-Technologien.Verbindung von persönlichen Geräten wie Smartphones, Kopfhörern, Computermäusen.

Typen drahtloser Netzwerke

Wireless Wide Area Network (WWAN):

- WWANs bieten Netzwerkabdeckung über große geografische Bereiche, oft national oder international.
- Sie nutzen Mobilfunktechnologien wie 3G, 4G LTE, 5G.
- Beispiele: Mobiltelefondienste, mobiles Internet.

Mobile Ad-hoc Network (MANET):

- MANETs sind selbstkonfigurierende Netzwerke, die aus mobilen Geräten bestehen, die dynamisch Netzwerke ohne feste Infrastruktur oder zentrale Verwaltung bilden können.
- Verwendet werden sie meist für Militärische Einsätze, Katastrophenhilfe, temporäre Veranstaltungen.

WEP (Wired Equivalent Privacy)

- Ältestes Sicherheitsprotokoll für drahtlose Netzwerke.
- Verwendet den RC4 Verschlüsselungsalgorithmus, der leicht zu hacken ist.
- Gilt als **äußerst unsicher**, wird von modernen Routern nicht mehr angeboten.
- Hat statische Sicherheitsschlüssel bis zu 256 Bit.
- Wurde 2004 offiziell durch WPA abgelöst.

WPA (Wi-Fi Protected Access)

- Kann auf WEP-fähigen Geräten durch Software-Update aktiviert werden.
- Nutzt TKIP (Temporal Key Integrity Protocol), basiert auf RC4, aber mit dynamischen Schlüsseln und Integritätschecks.
- Einsatz von EAP (Extensible Authentication Protocol) in größeren WLANs.
- Pre-Shared Keys (PSK) in kleinen Installationen und im privaten Bereich.
- PSK erfordert starke Passwörter zur Vermeidung von Brute-Force-Attacken.
- TKIP/WPA gilt heute aufgrund von Anfälligkeiten als **unsicher**.

WPA2 (Wi-Fi Protected Access 2)

- Zweite Generation von WPA, schließt Sicherheitslücken
- Einführung der AES (Advanced Encryption Standard) Verschlüsselung
- AES ist ein symmetrisches Verschlüsselungsverfahren, gilt als **State of the Art**
- Verwendung von dynamischen Keys zur Absicherung gegen Cyberattacken
- Wird auch für Ende-zu-Ende-Verschlüsselung bei Messenger-Diensten verwendet

WPA3 (Wi-Fi Protected Access 3)

- Entwickelt 2018, wesentliche Verbesserungen gegenüber WPA2
- Neues Schlüsselaustauschprotokoll, schützt gegen Brute-Force-Angriffe
- Basierend auf AES, ersetzt PSK durch SAE (Simultaneous Authentication of Equals)
- SAE ermöglicht sicheren Schlüsselaustausch und schützt selbst bei schwachen Kennwörtern
- Unterscheidung zwischen „Enterprise Mode“ für große Netzwerke und „Personal Mode“ für private Nutzung

Sicherheitsmaßnahmen

Sichere Passwörter:

- Starke, komplexe Passwörter wählen
- Regelmäßige Änderung

Netzwerkname (SSID) anpassen und verbergen:

- Ändern des Standardnamens (SSID) des Netzwerks, um es weniger erkennbar zu machen
- Verbergen der SSID, damit sie nicht in der Liste verfügbarer Netzwerke erscheint

Sicherheitsmaßnahmen

Zugriffskontrollen implementieren:

- Beschränken des Zugriffs auf Ihr Netzwerk (MAC Filterung)
- Einrichten eines separaten Netzwerkes für Gäste (DMZ)

Firewall und Sicherheitssoftware:

- Sicherstellung der Aktivität der Firewall
- Absicherung der Endgeräte durch Anti-Viren- und Anti-Malware-Programme

Sicherheitsmaßnahmen

Regelmäßige Updates und Patches

- Firmware des Routers regelmäßig aktualisieren
- Software-Patches kontinuierlich installieren

Physische Sicherheit:

- Platzieren des Routers an einem sicheren Ort, um unbefugten physischen Zugriff zu verhindern

Sicherheitsmaßnahmen

Netzwerküberwachung:

- Regelmäßiges Überwachen der Netzwerkprotokolle auf verdächtige Aktivitäten

VPN für sichere Verbindungen:

- Einrichten eines VPNs für den sicheren Zugriff von außen

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm