



Abhörsicherheit von NEC Richtfunksystemen

NEC Richtfunksysteme entsprechen der neuesten Generation der digitalen Mikrowellen Übertragungstechnik und sind grundsätzlich abhörsicher.

Hierbei kommen mehrere Faktoren für die Sicherheit zum Einsatz welche nachfolgend einzeln beschrieben werden.

- **Der Antennen Standort**

Basierend auf dem Standort der Antennen und die Ausbreitung der elektromagnetischen Welle wirkt sich dieser Faktor wie folgt aus. NEC Richtfunksysteme arbeiten mit speziellen Parabolantennen welche punktgenau aufeinander ausgerichtet werden. Diese Antennenbauform verhindert eine weite Streuung der gesendeten Funksignale durch Fokussierung ähnlich einer Linse. Der typische Öffnungswinkel dieser Antennen ist hierbei kleiner drei Grad. Ausserhalb dieses kleinen Öffnungswinkels ist der Empfangspegel zu niedrig, um nutzbare Funksignale zu erhalten. Um die Funksignale generell abfangen zu können, muss also parallel zu der vorhandenen Antenne und innerhalb des Öffnungswinkels auf jeder Seite eine absolut identische Antenne aufgebaut und ausgerichtet werden. Da sich die Antenne meistens an einem exponierten Standort mit beschränktem Zugang befinden, kann eine Zutrittskontrolle einfach realisiert werden und die Errichtung einer weiteren Abhörantenne verhindern.

- **Die technischen Geräte**

Sollte der Angreifer das Hindernis überwunden haben und Antennen errichten können, steht der Angreifer vor einem technischen Problem. Der Angreifer benötigt zum Aufzeichnen der übertragenen Daten eine baugleiche NEC Sende- und Empfangsanlage (ODU) sowie die identische NEC Baugruppe (IDU) mit der entsprechenden Schnittstelle, dem Modulator / Demodulator, der passenden Firmware Version und die entsprechende Systemkonfiguration. Die IDU befindet sich meistens innerhalb von Gebäuden und ist in der Regel nicht frei zugänglich.



- **NEC eigene Übertragungsstandards**

Ein zusätzlicher Sicherheitsfaktor für die Kundendaten ergibt sich durch die NEC eigene Entwicklungen und Optimierungen. Die interne Verarbeitung und Modulierung der Daten ist mit keinem anderen Richtfunksystem vergleichbar. Durch die Optimierung dieser Prozesse ist eine sichere und effizientere Datenübertragung garantiert. Hierdurch hebt sich das NEC Richtfunksystem von anderen Produkten ab.

Die zu übertragenden Daten (SDH, PDH, Ethernet, ect.) werden mit Hilfe eines Scramblers in proprietäre Pakete für die Modulatorstufe umgewandelt. Anschliessend werden in dem mit 21 Stufen arbeitenden Time-Domain-Equilizer diese Daten moduliert und zusätzlich mit einem FEC-Schlüssel (Forward-Error-Correction) versehen. Bei den NEC Richtfunksystemen steht als FEC-Schlüssel wahlweise der Algorithmus nach RS (Reed Solomon) oder LDPC (Low Density Parenty Check) zur Verfügung. Eventuell nicht genutzte Übertragungskapazität wird mit zufällig generierten Bitraten aufgefüllt. Diese werden zur erweiterten Bit-Error Analyse verwendet um eine höchstmögliche Zuverlässigkeit zu jedem Zeitpunkt zu gewährleisten.

Nun wird dieser eigens für diesen Übertragungsmoment kreierte Datenstrom über die Luftschnittstelle mit einer Radio-Link-ID zur Gegenseite übertragen. Auf der Gegenseite werden diese Arbeitsschritte in umgekehrter Reihenfolge durchgeführt bis der ursprüngliche Datenstrom ohne Verluste und fehlerfrei wieder an der Schnittstelle der IDU zur Verfügung steht.

- **Einzel zugeteilte Sendefrequenzen**

An dieser Stelle ergibt sich für den Angreifer ein zusätzliches Hindernis. Die genutzten Sende- und Empfangsfrequenzen sind nicht öffentlich bekannt und werden im Einzelzuteilungsverfahren für jede Richtfunkstrecke separat durch die Regulierungsbehörde berechnet und beurkundet. Zudem wird das Modulationsprinzip sowie die Kennung der Radio-Link-ID benötigt, um die Funksignale mit den darin emulierten Datenpaketen erkennen und aufzeichnen zu können.



- **Benötigte Rechenleistung zum Entschlüsseln**

Spätestens an dieser Stelle scheitert ein Aufzeichnen der Daten, da der Angreifer niemals alle bisher aufgeführten Daten und Umstände wissen und realisieren kann. Eine spezielle Software zum Aufzeichnen solcher kryptischen Daten und die Entschlüsselung in eine lesbare Form, ist nicht im Computerhandel oder im Internet erhältlich. Die benötigte Rechenleistung, welche aufzubringen wäre um diese Daten zu entschlüsseln, hätte die Kapazität eines mittleren Rechenzentrums.

- **Abgeschlossenes System**

NEC Richtfunksysteme bieten Schutz vor dem Eindringen in ein Kundennetzwerk durch Identifikation. Die Sende- und Empfangsanlage von NEC Richtfunksystemen akzeptiert nur Datenpakete, welche die richtige Radio-Link-ID haben und von der verifizierten Partnerstation stammen. Eine sogenannte Multipoint Anbindung über eine Funkstrecke wird nicht unterstützt und Pakete von unbekanntenen Stationen werden ignoriert. Somit ist es einem Angreifer nicht möglich, über ein NEC Richtfunksystem in ein bestehendes Netzwerk zu gelangen und Daten gezielt abzufragen.

- **Einfachere Wege für Datendiebstahl**

Wenn es das Ziel eines Angreifers ist, sensible Daten oder Informationen zu erhalten, wird er sicherlich angesichts der hier aufgeführten Faktoren einen einfacheren Weg suchen, um sein Ziel zu erreichen. Beispiele hierfür sind ungesicherte Kabelanbindungen oder eingeschleuste Schadsoftware. Bereits eine ungesicherte Netzwerkdose innerhalb eines Gebäudes bietet jedem Angreifer die Möglichkeit, mit einem handelsüblichen Notebook gezielt nach Daten und Informationen zu suchen oder Programme einzuschleusen.

Aus diesen Gründen gelten NEC Richtfunksysteme als abhörsicher.

Hans-Erik Frank
Technical Solutions Engineer
NEC Deutschland GmbH

Düsseldorf, 1. September 2009