Sichere Kommunikation mit DECT-kompatiblen Lösungen.

Plantronics bietet die einzigen Headsets der Branche mit DECT-Kompatibilität und optimiertem zentralisiertem Management.

„Digital Enhanced Cordless Telecommunications" (DECT) ist eine 1,9-GHz-Technologie, die in einem dedizierten Bereich des schnurlosen Spektrums sendet und so hohe Sicherheit und Audioqualität für Arbeitsumgebungen in Unternehmen und im Homeoffice liefert. Die DECT-Technologie wird häufig als „frei von Interferenzen" beschrieben, da sie sich anders als WLAN-Netzwerke kein Frequenzbereich mit anderen Technologien teilt.

Sicherheit ist eine der vielen Vorteile der DECT-Technologie. DECT nutzt digitalen TDMA (Time Division Multiple Access) und eine dynamische Kanalauswahl über 10 Trägerfrequenzen und 24 Zeitschlitze in Kombination mit einem mehrstufigen Sicherheitssystem. Dieses mehrstufige Sicherheitssystem mit anmelden, verschlüsseln und ausweisen gewährleistet ein hohes Maß an Abhörsicherheit. In bestimmten Branchen wie im Gesundheitswesen und dem Finanzsektor ist eine DECT-basierte schnurlose Kommunikation zur Gewährleistung maximaler Sicherheit und Vertraulichkeit erforderlich.

ERFÜLLUNG DES BEDARFS AN ERWEITERTER DECT-SICHERHEIT

Die schnurlosen DECT-Lösungen von Plantronics sind die einzigen Produkte der Branche, die sowohl Basis- als auch erweiterte Sicherheitsanforderungen nach DECT-Standard wie vom ETSI (European Telecommunications Standards Institute) festgelegt erfüllen.

Nachdem 2009 eine Gruppe von Hackern Sicherheitslücken einfacher DECT Produkte erkannten, ist ersichtlich geworden, dass der DECT Standard verbessert werden muss. Unter anderem zeigte die Hacker-Gruppe die Gefahr von Verstößen auf, wenn DECT-Produkte nicht die Standard-Authentifizierungs- und Verschlüsselungsmethoden wie in den ETSI-Standards beschrieben sind verwendeten. Plantronics nutzt bei den DECT-Geräten schon immer die integrierte Authentifizierung und Verschlüsselung.

Das DECT-Forum, bei dem Plantronics Mitglied ist, prüfte die Ergebnisse der DeDECTed-Gruppe und führte in Antwort darauf 2013 das DECT Security Zertifizierungsprogramm ein. Dieses Programm stellt unabhängige Produkttests und -verifizierungen in einem zugelassenen Labor sicher.

NUR PLANTRONICS BIETET ERWEITERTE DECT-SICHERHEIT

Der neue DECT-Standard umfasst Richtlinien für Verbesserungen in vier neuen Bereichen (siehe unten), womit die Anzahl der Sicherheitskategorien auf acht ansteigt. Tatsächlich ist Plantronics der erste Anbieter von schnurlosen Produkten, der sämtliche vom DECT-Forum beschriebenen Sicherheitsstandards erfüllt. Die Plantronics CS500-Serie mit den erweiterten Sicherheitsfunktionen wurde ab Oktober 2013 ausgeliefert.

Seit Januar 2016 sind die Plantronics Savi 400- und Savi 700-Serien mit erweiterter DECT-Security zertifiziert. Plantronics ist nach wie vor der einzige Anbieter schnurloser Headsets mit DECT Security und erfüllt damit alle acht Sicherheitsfunktionen des DECT-Forums im Sortiment.

STANDARD-DECT-SICHERHEITSFUNKTIONEN

1. Registrierungsverfahren und Zeitlimits zur Einrichtung eines 64-Bit-Authentifizierungsschlüssels: Die Basisstation bleibt maximal 120 Sekunden „für die Registrierung geöffnet". Hierdurch wird sichergestellt, dass der Versuch, ein Headset bei der Basisstation zu registrieren, nur stattfinden kann, wenn der Nutzer die Registrierung gestartet hat. Der Vorgang muss innerhalb von 120 Sekunden abgeschlossen sein.
2. Verschlüsselungsaktivierung gestartet (Basisstation und Headset): Sowohl die Basisstation als auch das Headset unterstützen die Verschlüsselungsaktivierung. Die Basisstation aktiviert die Verschlüsselung bei allen Anrufen. In der Vergangenheit wurde die Verschlüsselung bei einigen DECT-Geräten nicht bei allen Anrufen gestartet.
3. Live-Schlüsselzuweisung: Die Basisstation erstellt bei der Registrierung des Headsets einen (64-Bit) Nutzerauthentifizierungsschlüssel (User Authentication Key, UAK) und weist diesen zu. Hierdurch wird sichergestellt, dass Basisstationen und Headsets nicht für Man-in-the-Middle-Angriffe anfällig sind. Sowohl die Basisstation als auch das Headset verwenden den Authentifizierungsschlüssel bei der Kommunikation.
4. Authentifizierung von Headsets: Die Basisstation kann das Headset authentifizieren und somit sicherstellen, dass es sich um ein echtes Headset handelt und nicht um einen Eindringling oder einen Versuch, das echte Headset zu imitieren. Mit dieser Funktion wird sichergestellt, dass zwischen Headset und Basisstation keine Kommunikation stattfindet, wenn keine gegenseitige Authentifizierung möglich ist.

NEUE DECT SECURITY FUNKTIONEN

5. Verbesserter Zufallszahlengenerator: zuverlässigerer Algorithmus, durch den verhindert wird, dass die bei der Generierung von Verschlüsselungsschlüsseln verwendeten Seed-Zahlen doppelt vorkommen. Durch diese Verbesserung wird es unmöglich, eine Zufallszahl durch wiederholte Versuche zu erraten und dann zum Erstellen von Schlüsseln zu verwenden.
6. Bewertung des Peer-Verhaltens hinsichtlich der Verschlüsselungs-Timeoutwerte für die Auslösung einer Anruffreigabe: Wenn der Peer sich nicht wie erwartet verhält, d. h. wenn er die Verschlüsselung nicht rechtzeitig startet, geht das Gerät davon aus, dass eine versuchte Sicherheitsverletzung vorliegt. Der Anruf wird daraufhin abgebrochen.

   Ein Hacking-Versuch müsste jedes Mal in jeder Hinsicht fehlerlos sein, weil jede Kommunikation zwischen Headset und Basisstation, die vom erwarteten Muster abweicht, zum Abbruch der Verbindung führt.
7. Frühzeitige Verschlüsselung: Garantiert die Aktivierung der Verschlüsselung sofort nach der Herstellung der Verbindung und vor dem Austausch von Protokollnachrichten einer höheren Ebene (einschließlich Anrufer-ID, gewählter Ziffern usw.), sodass keine Informationen unverschlüsselt ausgetauscht werden.
8. Verfahren für Re-Keying mit einem neu abgeleiteten Cipher-Schlüssel während eines Anrufs: Der vom Verschlüsselungsmodul verwendete Cipher-Schlüssel wird alle 60 Sekunden mindestens einmal aktualisiert. Hierdurch werden alle Versuche vereitelt, den Cipher zu ermitteln, beispielsweise durch Supercomputer.

DECT 101: Der Plantronics DECT-Vorteil

ANMELDUNGSVERIFIZIERUNG
Basis- und Mobilteile werden so miteinander gepaart, dass sie das richtige Basis- bzw. Mobilteil leicht identifizieren können. Ein geheimer Authentifizierungsschlüssel wird mit Hilfe des DECT Standard Authentication Algorithm (DSAA) berechnet. Die vollständige Spezifikation dieses Algorithmus ist nur den Geräteherstellern bekannt. Die Zeitdauer der Anmeldung ist für zusätzliche Sicherheit beschränkt.

AUTHENTIFIZIERUNG
Basis- und Mobilteil überprüfen, ob der richtige Authentifizierungsschlüssel verwendet wurde, und erstellen darüber hinaus Codeschlüssel unter Verwendung des DECT Standard Ciphers (DSC) für die Verschlüsselung der über Funk übertragenen Daten. Die Definition dieses Algorithmus ist nur den Geräteherstellern bekannt.

VERSCHLÜSSELUNG
Der 64-Bit-Codeschlüssel wird zur digitalen Verschlüsselung der Sprachdaten verwendet, die per Funk übertragen werden. Auf Empfängerseite wird der in der Authentifizierungsphase berechnete Schlüssel zur Entschlüsselung der Daten verwendet.

DYNAMISCHE KANALFLEXIBILITÄT
Im Rahmen des DECT-Protokolls wechseln Geräte bei Interferenzen automatisch zu neuen Kanälen. Da Zeitpunkt und Ziel des Hops nicht vorhersagbar sind, wird die Übertragung dadurch noch sicherer.

DYNAMISCHE LEISTUNGSKONTROLLE
Die DECT-Produkte der Plantronics Savi®-Familie und CS500-Serie nutzen die typische adaptive Leistungskontrolle, um die Leistungsstufen von Radiofrequenzen zur Kommunikation zu senken, wenn der Nutzer sich in der Nähe der Basis befindet. Potenzielle Cyber-Attacken müssten sich in diesem Bereich bewegen oder hochempfindliche Richtantennen verwenden, wodurch das Risiko von Abhörattacken reduziert wird.

EINHALTUNG DER SARBANES-OXLEY-BESTIMMUNGEN
Die DECT-Geräte von Plantronics erfüllen die Bestimmungen des Sarbanes-Oxley Acts (2002), Art. 404. Diese Erklärung basiert auf der Einhaltung der US-Verordnung 45 CFR 164.312(a)(2)(iv) in Bezug auf produktintegrierte Verschlüsselungsmaßnahmen.

EINFACHES MANAGEN UND VERWALTEN IM UNTERNEHMEN

Neben den Headsets der Savi 400- und 700-Serie, die mit den aktuellen DECT-Funktionen geliefert werden, können auch die DECT-Funktionen vorhandener Plantronics Headsets per Firmware-Update aktualisiert werden. Mit Plantronics Manager Pro, einer Cloud-basierten Anwendung mit einzigartigen Audiogerät-Management-, Überwachungs-, Richtliniendurchsetzungs- und Nutzersupportfunktionen, kann die Unternehmens-IT dies ganz einfach umsetzen.

Als Teil des Plantronics Spokes-Software-Portfolios bietet Plantronics Manager Pro IT-Managern unkomplizierte Tools, die sie unternehmensweit zur Einrichtung von Audiogeräten und zur Aktualisierung der entsprechenden Software sowie Firmware für Endnutzer einsetzen können. Plantronics Manager Pro verfügt über Berichttools, mit denen IT-Manager ihre DECT-Umgebung besser verstehen und sicherstellen können, dass alle Headsets die Bestimmungen erfülen.

Schlüsselfunktionen:

- Aktivierung oder Deaktivierung von Geräteeinstellungen zur Einhaltung firmeninterner Vorgaben oder gesetzlicher Vorschriften
- Möglichkeit für einzelne Nutzer, DECT-Einstellungen zu einem passenden Zeitpunkt zu aktualisieren, während gleichzeitig die Rechenschaftspflicht durchgesetzt wird
- Überwachung der Einstellungen und Nutzung von Audiogeräten fast in Echtzeit
- Generierung von Inventar- und Nutzungsberichten zwecks leichterer Geräteverwaltung
- Übersicht über alle vorhandenen Geräte, auch von Drittanbietern

Plantronics ist der einzige Hersteller, der Management-Software zum Updaten von DECT Headsetfirmware bietet und damit eine gleichförmige Headsetkonfiguration sicherstellt. Diese Möglichkeiten kombiniert mit der DECT Security Zertifizierung macht Plantronics zum führenden Anbieter in der schnurlosen Kommunikation.

Weitere Informationen finden Sie auf der Website plantronics.com

[1] Frühere Savi 400- und Savi 700-Modelle können per Firmware-Update auf die aktuellen DECT-Sicherheitsfunktionen aktualisiert werden.

Gilt nicht für die CS500-Serie.