Bluetooth® Sicherheit

Bluetooth® Sicherheit

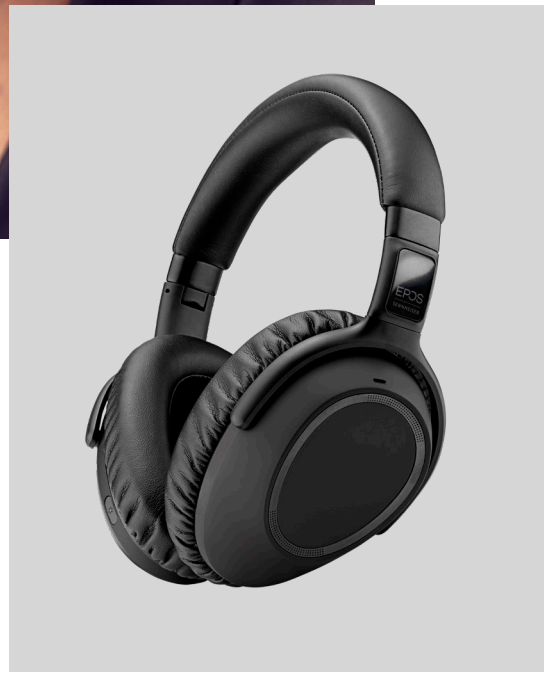
Bei EPOS haben Komfort, Qualität und Sicherheit höchste Priorität. Dieses Whitepaper befasst sich mit der Sicherheit der Bluetooth®-Technologie im Allgemeinen und den zusätzlichen Sicherheitsfunktionen der Contact Center & Office-Headsets von EPOS.

Einleitung

Bluetooth® ist ein Standard für die kabellose Übertragung von Sprache und Daten zwischen Bluetooth®-fähigen Geräten über kurze Entfernungen. Die Firma Ericsson brachte Bluetooth® 1994 auf den Markt, um verschiedenste Gerätetypen mit diversen Kommunikationsprotokollen über eine einheitliche Technologie miteinander verbinden zu können.

Seit der Einführung von Bluetooth® haben sich mehr als 20.000 Unternehmen in der Bluetooth® Special Interest Group zusammengefunden, und der Bluetooth®-Standard ist zu einem weit verbreiteten und beliebten Verbindungsverfahren geworden. Mehr als 2 Milliarden Geräte können mittlerweile die Bluetooth®-Technologie nutzen. Daher sind Sicherheitsbelange zu Recht immer wichtiger geworden.

Bevor wir uns den Sicherheitsaspekten von Bluetooth® zuwenden, muss betont werden, dass das Risiko unbefugter Zugriffe auf die Bluetooth®-Kommunikation vergleichsweise gering ist. Im Allgemeinen bietet Bluetooth® ein sehr hohes Maß an Sicherheit, und EPOS hat darüber hinaus in die eigenen Produkte intelligente und innovative Sicherheitsfunktionen integriert.



So funktioniert Bluetooth®

Der Bluetooth®-Standard ermöglicht die drahtlose Verbindung von Geräten, die sich in der Nähe zueinander befinden. Um eine Verbindung herzustellen, müssen die beiden Geräte zunächst gekoppelt werden. Dieser Vorgang wird als „Pairing“ bezeichnet. Beim Pairing registrieren sich die beiden Geräte gegenseitig und können anschließend miteinander kommunizieren.

Dieser Vorgang setzt voraus, dass beide Geräte einander erkennen – sie müssen „sichtbar“ gemacht werden. Bei den meisten Bluetooth®--Geräten muss der Pairing-Modus vom Benutzer aktiviert werden. In diesem Modus werden die Geräte für eine kurze Zeit sichtbar und tauschen zur Authentifizierung ihren Sicherheitsschlüssel miteinander aus.

Sobald der Sicherheitsschlüssel übertragen wurde, sind die Geräte erfolgreich gekoppelt. Der geheime Schlüssel ist die „Brücke“ zwischen den Geräten, die bei dem ersten Pairing gebildet wird. Die Geräte nutzen ihn auch weiterhin, das heißt, der Vorgang braucht nicht bei jedem Verbindungs-aufbau wiederholt zu werden.

Verschlüsselte Kommunikation

Nach dem erfolgreichen Austausch der geheimen Schlüssel können die zwei Bluetooth®-Geräte miteinander kommunizieren. Alle EPOS Produkte nutzen die höchste Verschlüsselungsstufe mit einem 128-Bit-Schlüssel, der beim Pairing erzeugt wird. Dank der Verschlüsselung können die zwischen den Geräten gesendeten Daten nur vom beabsichtigten Empfänger gelesen werden. Die Empfangseinheit entschlüsselt mit demselben Algorithmus die Daten zurück in das ursprüngliche Format.

Hohe Sicherheit

Wie bereits erwähnt, bietet die Bluetooth®-Technologie ein hohes Maß an Sicherheit für den Anwender. Lausch- oder Störangriffe sind daher bei der Bluetooth®-Kommunikation aus vielen Gründen extrem schwierig, unter anderem wegen der kurzen Reichweite und der Authentifizierung, die vor der Nutzung der Geräte stattfinden muss.

Die verwundbarste Stelle von Bluetooth®-Geräten ist das Pairing selbst, da sie zu diesem Zeitpunkt sichtbar sind. Trotz des geringen Sicherheitsrisikos hat EPOS an dieser Stelle mehrere intelligente Sicherheitsfunktionen integriert.

Arten von Bedrohungen

Um die Sicherheitsvorteile von EPOS Headsets zu erläutern, werden die verschiedenen Arten von Bedrohungen im Folgenden kurz dargestellt.

Man-in-the-Middle-Angriff: Ein Angreifer versucht mit seinem Gerät, ohne Wissen des Angegriffenen Informationen abzufangen. Solche Angriffe sind in der Praxis äußerst schwierig, da sich der Angreifer in unmittelbarer Nähe der Geräte aufhalten muss.

Viren: Kabellose Übertragung von schädlichen Viren. Bluetooth®-Headsets und Bluetooth®-Dongles von EPOS übertragen nur Sprache und keine Daten wie andere Bluetooth®-Geräte. Daher gibt es für einen Virus keine Umgebung, in der er wirken kann.

Lauschangriff: Ein Angreifer hört ein Gespräch mit. Der Angreifer müsste beim Pairing anwesend sein und darüber hinaus ein extrem hochentwickeltes Gerät besitzen. Die Sprache wird verschlüsselt und in einen digitalen Datenstrom verwandelt.

Moderne Geräte nutzen vor allem für die Sprachübertragung den Bluetooth®-Standard 4.0 oder höher, der ein hohes Maß an Schutz bietet.

Zusätzliche Sicherheit durch EPOS

Bei der Produktentwicklung spielt die Sicherheit des Benutzers für EPOS eine wesentliche Rolle. Wir haben weitere Sicherheitsfunktionen integriert, um zusätzlichen Schutz für Bluetooth® zu bieten. Hier einige Beispiele:

Intelligentes Energiemanagement: Bei Bluetooth®-Geräten von EPOS wird während des Pairings die Sendeleistung herabgesetzt. Das bedeutet, dass die Reichweite beim Pairing wesentlich geringer ist als im Normalbetrieb. Man-in-the-Middle-Angriffe sind dadurch extrem schwierig geworden, da sich der Angreifer mit seinem Gerät in unmittelbarer Nähe der Pairing-Geräte befinden muss.

Zugriffssicherheit für Host-Geräte: EPOS Headsets und die entsprechenden USB-Dongles unterstützen nur Audio-bezogene Bluetooth®-Profile. Dateninhalte, die auf dem Host-Gerät gespeichert sind, können nicht zum Headset oder zu anderen Geräten übertragen werden. Dies bedeutet, dass auch keine Viren übertragen werden können.

Kleines Zeitfenster für Pairing: Headsets von EPOS sind nur für einen sehr kurzen Zeitraum während des Pairings ermittelbar.
Nach dieser Zeit wird der Bluetooth®-Zugang automatisch abgeschaltet, bis er durch einen autorisierten Benutzer erneut aktiviert wird.

Haftungsausschluss von EPOS Bluetooth®

EPOS ist bestrebt, seine Bluetooth®-Produkte so sicher wie möglich zu machen. Wir übernehmen jedoch keinerlei Haftung hinsichtlich Schadenersatz oder Aufwandsentschädigungen aufgrund von Sicherheitsverstößen seitens des Kunden durch die Verwendung unserer Bluetooth®-Produkte.

Auch wenn EPOS für ein hohes Maß an Sicherheit Vorsichtsmaßnahmen getroffen hat, liegt es in der Verantwortung des Kunden, zur Wahrung der Sicherheit geeignete Einstellungen an seinem Bluetooth®-Gerät vorzunehmen bzw. diese zu überprüfen. Die in dem Gerät von EPOS implementierten Sicherheitsmaßnahmen werden unter Umständen nicht von dem Gerät des Kunden unterstützt, sodass sich die Sicherheit einer Bluetooth®-Verbindung verringern kann.

Der Kunde erkennt an, dass die Verschlüsselung der Bluetooth®-Verbindung nur für die drahtlose Verbindung von gepaarten Geräten gilt.

Die Kommunikationsverbindungen und Inhalte, die über eine verschlüsselte Bluetooth®-Verbindung übertragen werden (z.B. Telefonanrufe), werden von dem Bluetooth®-Gerät von EPOS nicht verschlüsselt. Der Kunde erkennt weiterhin an, dass keine Technologie umfassende Sicherheit bieten kann. Falls der Bluetooth®-Standard den Sicherheitsanforderungen nicht genügten sollte, müssen vom Kunden zusätzliche Maßnahmen implementiert werden.

Nichtsdestotrotz haftet EPOS für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit durch fahrlässige Pflichtverletzung seitens EPOS bzw. für Schäden aufgrund eines Verstoßes, der auf grobe Fahrlässigkeit oder vorsätzliches Handeln seitens EPOS zurückzuführen ist.

Des Weiteren haftet EPOS bei der fahrlässigen Pflichtverletzung wesentlicher Vertragspflichten. Wesentliche Vertragspflichten sind Pflichten, deren Einhaltung eine grundlegende Voraussetzung für die ordnungsgemäße Erfüllung des Vertrags ist und auf die ein Vertragspartner vertrauen darf.

In diesem Fall ist eine Entschädigung auf vorhersehbare, typische Schäden begrenzt.

Obige Bestimmungen gelten auch für Schäden, die durch gesetzliche Vertreter oder einen Erfüllungsgehilfen von EPOS entstehen.

Die Haftung seitens EPOS bleibt durch das dänische/europäische Produkthaftungsgesetz unberührt.

406839258

EPOS Group A/S
Industriparken 27
2750 Ballerup, Denmark
eposaudio.com