Endnutzeranleitung

Nutzung von Bluetooth in den Behörden und Organisationen mit Sicherheitsaufgaben in Niedersachsen

Stand	Version	Autor/in
05/2025	1.0	P. Gallo, L. Laux

Inhaltsverzeichnis

1 Einleitung

Diese Anleitung stellt die Anforderungen an Endnutzende und den Umgang mit Bluetooth im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) in Niedersachsen inklusive einer Bewertung von Bluetooth mit Verwendung mobiler Endgeräte und dortiger Nutzungsszenarien dar. Die Basis bildet die Risikoanalyse zur Nutzung von Bluetooth im Digitalfunk der BOS in Niedersachsen. Zur sicheren Anwendung von Bluetooth als Ersatz oder Erweiterung kabelbasierter Verbindungen und deren Nutzungsszenarien beschreibt diese Anleitung die (technischen) Grundlagen, die einen Einfluss auf die Sicherheit haben können, sowie umzusetzende Maßnahmen, um die Risiken bei korrekter Anwendung zu minimieren.

2 Geltungsbereich und Abgrenzung

Es werden die entstehenden Risiken durch die Nutzung von Bluetooth-Zubehör in Kombination mit BOS-Funkendgeräten aus vorher definierten Anwendungsfällen sowie verschiedene mögliche Nutzungen von Bluetooth im generellen Digitalfunkkontext zur Datenübertragung und die Nutzung von Bluetooth-Verbindungen mobiler Endgeräte betrachtet. Konkrete Anwendungsfälle schließen

- Funkendgeräte: Verschiedene Funkendgeräte der Hersteller Motorola und Sepura, ggf. Bluetooth-fähig

- Headsets: Verschiedene Headsets z. B. der Hersteller Jabra, Plantronics, Motorola, Selectric, Yamay, Bowers & Wilkins sowie Kradhelme von Schuberth und BMW
- Push To Talk Adapter und Seitenadapter für Bluetooth-Nutzung der Funkendgeräte: Verschiedene Endgeräte z. B. der Hersteller CopTech, Motorola, Selectric, ProEquip, 3M
- Mobile Endgeräte: Smartphones und Tablets z. B. von Samsung, Apple
- Peripherie-Geräte: Verschiedene Eingabegeräte wie drahtlose Tastatur, Maus, Handscanner und Grafiktablet
- IoT-Geräte[1]: Schnittstelle zu Telefonie-, Navigations- und Infotainment-System der Dienstwagen VW Passat, Drohne, Wetterstation, Digitalkamera inklusive Stativ

ein. Diese Liste ist nicht abgeschlossen und kann bei Neubeschaffung von Endgeräten ergänzt werden. Anwendungsfälle mit einer besonders hohen Vertraulichkeit oder der Notwendigkeit der Geheimhaltung eines Einsatzes sind nicht Teil dieser Anleitung. Organisationen der nichtpolizeiliche BOS können diese Anleitung anwenden, sofern die zugrundeliegenden Maßnahmen der Risikoanalyse eingehalten werden.

3 Hintergrundinformationen: Bluetooth als Funktechnologie zur Datenübertragung

Bluetooth ist ein Funkstandard zur Übertragung von Daten zwischen Endgeräten über kurze Distanzen, der auf dem 2,4 GHz-Frequenzband arbeitet. Hier sind neben Bluetooth weitere Technologien wie WLAN, Zigbee oder potentiell weitere spezifische Endgeräte wie funkgesteuerte Garagentore oder Mikrowellen aktiv. Dabei kann es sich um Störfaktoren für Bluetooth handeln, die die Funktionalität einschränken können. Generell ist die Reichweite von Bluetooth begrenzt – je nach örtlichen Gegebenheiten und Sendeleistung können zwei Endgeräte mit Bluetooth-Verbindung eine Reichweite von wenigen Metern bis zu hundert Metern aufweisen.

Zur Übertragung von Daten mittels Bluetooth werden diese in definierte Datenpakete mit fester Größe umgewandelt. Da es sich bei Bluetooth um ein Funkprotokoll handelt, ist es jeder Person in der Nähe mit entsprechender technischer Ausstattung und Kompetenz möglich, diese Pakete abzufangen und zu interpretieren. Durch Verschlüsselungsmaßnahmen können die Nutzdaten geschützt werden.

[1] IoT = Internet of Things – IoT-Geräte sind physische Gegenstände mit Sensoren, Software und Internetverbindung, die Daten erfassen, austauschen oder auf Befehle reagieren können.

Vor einer Übertragung von Daten ist es notwendig, dass zwei Endgeräte miteinander gekoppelt werden. Endgeräte, die miteinander gekoppelt sind, können Daten untereinander austauschen, inklusive Steuerungsinformationen, die beispielsweise Lautstärke, Push To Talk oder Anrufe betreffen können. Die Kopplung zwischen Endgeräten führt daher eine Schnittstelle zwischen den Systemen ein, die weitreichende Berechtigungen haben kann und damit ein großes Risiko für Sicherheitseinschränkungen bietet. Somit hat die Kopplung einen besonderen Schutzbedarf, der in dieser Anleitung adressiert wird. Grundsätzlich existieren mehrere Modi zur Kopplung von Endgeräten, die über eine bestimmte Sicherheit verfügen. Diese sind (geordnet von unsicher zu sicher):

- Just Works: Zwei Endgeräte werden in den Kopplungsmodus versetzt und diese versuchen sich gegenseitig zu finden. Hier findet keine weitere Überprüfung der Kopplung statt. Das heißt, dass jedes weitere Bluetooth-fähige Endgerät in der Nähe eine Kopplung durchführen kann.
- Numeric Comparison: Beide Endgeräte bilden basierend auf dem geheimen Schlüssel, der während der Kopplung berechnet wird, eine 6-stellige Nummer als PIN, die auf beiden Endgeräten verglichen wird. Darauf basierend wird der Schlüssel zur weiteren Verschlüsselung für jede weitere Verbindung berechnet. Durch den manuellen Vergleich durch Nutzende ist eine höhere Sicherheit anzunehmen als für Just Works. Hier liegt die Verantwortung in Nutzerhand, den PIN tatsächlich zu überprüfen.
- Passkey Entry: Dieser Modus ist analog zu Numeric Comparison, wobei hier ein Endgerät einen 6-stelligen PIN anzeigt, der auf dem zweiten Endgerät eingegeben wird. Hier muss explizit der korrekte PIN eingegeben werden, sodass hier nicht trotz unterschiedlicher PIN eine Kopplung mit einem beliebigen Endgerät erfolgen kann.
- Out of Band: Endgeräte, die weitere Protokolle verwenden können, können diese zur Kopplung verwenden. NFC (Near Field Communication) stellt hier eine besondere Rolle dar: Die Reichweite von NFC ist sehr limitiert auf wenige Zentimeter, sodass die Endgeräte sehr nah aneinander sein müssen, um eine Kopplung durchzuführen, was es für Angreifer in der Nähe sehr schwierig macht, in die Kopplung einzugreifen. NFC wird beispielsweise auch für Kreditkarten und kontaktlose Zahlungen verwendet.

Daher ist Just Works als Kopplungsmodus nur in Ausnahmefällen zu nutzen, sofern andere Kopplungsmodi zur Verfügung stehen. Sofern eine Out of Band-Kopplung mit NFC zur Verfügung steht, sollte diese bevorzugt werden. Für Numeric Comparison und Passkey Entry ist eine entsprechende Eigenverantwortung der Nutzenden gegeben.

Als Resultat der Kopplung haben beide Endgeräte einen sogenannten Link Key generiert, der zur Authentifizierung und zum künftigen Datenaustausch verwendet werden kann. Auf dessen

Basis und Zufallszahlen wird für Datenkommunikation ein Encryption Key generiert, der beim Datenaustausch individuell ist.

Vorläufer von Bluetooth als Protokoll existieren seit 1940, wobei die explizite Entwicklung an Bluetooth seit 1998 stattfindet. Dementsprechend wurden verschiedene Versionen von Bluetooth entwickelt, die Funktionalität, Datenrate und Sicherheit des Protokolls erweitern. Die wichtigsten Neuerungen der verschiedenen Versionen sind:

- Bluetooth 2.1 + EDR (Enhanced Data Rate): Einführung von Secure Simple Pairing als Schutzmechanismus für einfach zu berechnende PINs zur Kopplung in Abgrenzung zu Legacy Pairing mit Anfälligkeit für Abhören z. B. Sepura SC-Serie
- Bluetooth 4.0: Einführung von Bluetooth Low Energy mit geringerer Datenrate und Reichweite, dafür mit deutlich höherer Energieeffizienz, insbesondere zur Übermittlung geringer Datenmengen im IoT-Kontext, Einführung von AES-Verschlüsselung für generelle Bluetooth-Kommunikation z. B. Motorola MTP 6650
- Bluetooth 4.2: Einführung von Secure Connections als Weiterentwicklung von Secure Simple Pairing mit aktuellen Verschlüsselungsalgorithmen
- Bluetooth 5.0: Funktionalität zur Standortübermittlung z. B. Motorola MXP 600
- Bluetooth 5.2: Verbesserungen im Audio-Bereich wie mehrere empfangende Kopfhörer von einer Quelle
- Bluetooth 5.3: Einführung einer minimal festlegbaren Schlüssellänge
- Bluetooth 5.4: aktuellste Version, Verschlüsselung für bestimmte Metadaten

Die Funktionalitäten, die Bluetooth für Datenübertragung und Steuerungsbefehle verwendet, sind in Bluetooth-Profilen festgelegt. Hier existiert eine Vielzahl von Profilen. Für die Anwendung von Bluetooth im Digitalfunk und zur sicheren Verwendung mobiler Endgeräte ist beispielsweise A2DP (Advanced Audio Distribution Profile) für Übertragung von Audiodateien, HFP (Hands Free Profile) zur Telefonie oder HSP (Headset Profile) für die Ausgabe von Sprache über Headsets möglich. Diese Aufzählung dient als beispielhafte Referenz, was mit Bluetooth standardmäßig möglich ist.

Über die generelle Funktionsweise hinaus treten Schwachstellen auf, die entweder im Design von Bluetooth-Versionen und der Spezifikation begründet liegen oder in der Implementierung des jeweiligen Herstellers. Im Allgemeinen werden solche Schwachstellen entweder durch Software-Updates oder in späteren Versionen eines Endgerätes gepatcht. Eine Ausnutzung der Schwachstellen erfordert zudem eine gewisse Angriffskompetenz sowie einen mutwilligen Angreifer. Hier ist neben gezielten Angriffen davon auszugehen, dass Angriffe in die Breite gegen beliebige Endgeräte mit aktiver Bluetooth-Schnittstelle ein entsprechendes Risiko darstellen.

Neben der Gefahr einer unautorisierten Kopplung, während sich Endgeräte im Kopplungsmodus befinden, besteht die Gefahr der Übernahme von Verbindungen durch Schwachstellen in der Bluetooth-Kommunikation zwischen Endgeräten. Ein aktuelles Beispiel ist die Schwachstelle BLUFFS[2], die mittels Angriff auf die Verschlüsselung zwischen Endgeräten diese schwächen und in der Konsequenz ein Brechen der Verschlüsselung ermöglicht. Eine so während des Einsatzes übernommene Verbindung kann daher trotz einer ordnungsgemäßen vorherigen Kopplung zu einem Sicherheitsrisiko führen.

Je nach Art der Schwachstelle ist es auch denkbar, dass ein Angreifer, der über eine Bluetooth-Schwachstelle Zugriff auf ein Endgerät gewonnen hat, unter Umständen Zugang zu weiteren Teilen des Systems hat und dieses angreifen kann.

Während der Nutzung von Bluetooth und einer aktiven Bluetooth-Schnittstelle kann ein Monitoring von Endgeräten bzw. eine Überwachung bestimmter Eigenschaften stattfinden, die anhand von technischen Parametern identifiziert und somit getrackt und zumindest Metadaten festgestellt werden können. Die Aufzeichnung von zusammengehörigen Bluetooth-Paketen ist erschwert, da Bluetooth-Verbindungen während der Kommunikation die genaue Frequenz wechseln. Dennoch kann ein Tracking erfolgen, da Endgeräte mit aktivierter Schnittstelle permanent Daten senden und empfangen können.

Neben aussendenden Daten ist Bluetooth als Funkprotokoll anfälliger gegenüber Störungen als kabelbasierte Verbindungen. Das erhöht die Chance, dass weitere Funkprotokolle oder Verbindungen die Bluetooth-Kommunikation stören können, genauso wie Objekte, Wände, Gebäude oder räumliche Gegebenheiten. Dies sollte beim Einsatz entsprechend beachtet werden.

4 Grundsätze zur Verwendung von Bluetooth

Die folgenden Grundsätze bilden den Rahmen der Anleitung zur konkreten Nutzung von Bluetooth und stellt dabei Kontext und Verantwortungen dar:

- **Eigenverantwortung der Nutzenden:**
  Viele vorgesehene Maßnahmen basieren darauf, dass Endnutzende diese korrekt und gewissenhaft umsetzen, um so zu einem sicheren Betrieb von Bluetooth mit Funkend-

[2] https://www.heise.de/news/BLUFFS-Neue-Angriffe-gefaehrden-Bluetooth-Datensicherheit-auf-Milliarden-Geraeten-9544862.html

geräten und mobilen Endgeräten beitragen zu können. Für bestimmte Anwendungsfälle wie die Nutzung eines dienstlichen Smartphones mit persönlicher Zuordnung sind Endnutzende in besonderer Verantwortung.

- Verwendung von Endgeräten und Zubehör:
  Nur Endgeräte, die explizit für den internen Gebrauch mit Bluetooth autorisiert sind, dürfen verwendet werden. Dies schließt die Nutzung von privaten Endgeräten und Zubehör vollständig aus. Private Endgeräte und Zubehör können ein Einfallstor für Angriffe darstellen, da diese potentiell keinem regelmäßigen Patchmanagement (zur Aktualisierung der Software und Bereinigen von Konfigurationsfehlern) und Sicherheitsevaluationen unterliegen. Zusätzlich schließt dies Überprüfungen der gekoppelten Endgeräte und weitere Vorsichtsmaßnahmen ein. Die autorisierten Endgeräte dürfen zudem nur von dazu befugten Personen verwendet werden.
  Generell gilt: Die Verwendung sollte nur so lange dauern, wie zur Erfüllung einer Aufgabe notwendig ist und die Berechtigung der verwendenden Person sollte nur so lange aufrecht erhalten bleiben, wie notwendig.
- Validierung von Informationen:
  Informationen oder Eingaben, die in ihrem Verbindungsweg Bluetooth-Kommunikation enthalten, sollten auf ihre Plausibilität geprüft werden, insbesondere, wenn diese widersprüchlich sind oder Anlass für Misstrauen geben. Hintergrund ist der eine angemessene Reaktion auf Fälle, in denen eine Bluetooth-Verbindung von einem Angreifer übernommen wurde oder sich ein unrechtmäßig gekoppeltes Endgerät in die Bluetooth-Verbindung dazu schaltet, um explizit Fehlinformationen zu verbreiten. Dies gilt auch für sich plötzlich verändernde Informationen zur Bluetooth-Nutzung oder scheinbaren Kontaktaufnahmen von Herstellern, da es sich um Phishing handeln kann. Eine generelle Wachsamkeit im Einsatz zur Erkennung möglicher lokaler Angreifer kann dazu beitragen, Angriffe zu detektieren.
  Zugleich fällt hierunter, die aktive Bluetooth-Verbindung während eines Einsatzes zu überprüfen, sodass kein Ausfall unerkannt bleibt. Potentielle Probleme kann eine Einschränkung der Verfügbarkeit oder der Funktionalität darstellen, beispielsweise durch ausbleibende Funkkommunikation, sodass eine Wachsamkeit im Einsatz auch auf die Bluetooth-Endgeräte notwendig ist.
- Vertraulichkeit personenbezogener Daten und Datensparsamkeit:
  Generell gilt, dass personenbezogene Daten entsprechend vertraulich behandelt werden sollten, insbesondere auch bei Kommunikation über Funksprüche und dem erhöhten Angriffsvektor des Abhörens durch die Verwendung von Bluetooth. Sämtliche personenbezogenen Daten, die über Bluetooth übermittelt werden, als auch auf Endgerä-

ten mit aktivierter Bluetooth-Schnittstelle verfügbar sind, sind dadurch gefährdeter. Daher ist ein genereller Aufruf zur Datensparsamkeit enthalten: Daten, die nicht vorliegen, können nicht missbraucht werden, sowohl die eigenen Daten als auch die von anderen Personen.

- Sensibilisierung und Weiterbildung:
  Um die Sicherheitsmaßnahmen und Anforderungen umsetzen zu können und diese samt ihrer Hintergründe zu verstehen, wird hier empfohlen, sich regelmäßig weiterzubilden und mit Maßnahmen der IT-Sicherheit (sowohl in Bezug auf Bluetooth als auch im Allgemeinen) auseinander zu setzen. Dazu gehört die eigenständige Weiterbildung, aber auch die Teilnahme an entsprechenden Seminaren und Fortbildungen, punktuelle Aktionen zur Förderung der Aufmerksamkeit auf IT-Sicherheit als auch regelmäßige kurze Auffrischungen in Rahmen von Informationen in Newslettern oder auf sozialen Medien.

5 Regeln zur Verwendung von Bluetooth für die Allgemeinnutzung

Im Folgenden werden konkrete Regeln aufgelistet, die zur Verwendung von Bluetooth eingehalten werden müssen, um einen sicheren Betrieb zu gewährleisten. Es wird unterschieden zwischen Anforderungen, die zwingend erfüllt sein **müssen**, erwünschten Anforderungen, die erfüllt sein **sollen** und Empfehlungen, die einen sicheren Betrieb gewährleisten und eingehalten werden **sollten**, falls möglich.

- Redundanzmaßnahmen zur Wiederherstellung einer Verbindung (für personenbezogene Endgeräte):
  Ist ein Endnutzer für die Verwaltung seines eigenen Endgerätes zuständig, so soll sichergestellt werden, dass eine Verbindung auch ohne Bluetooth wiederhergestellt und verwendet werden kann. Für Endgeräte kann kabelgebundenes (Audio-) Zubehör als Redundanzmaßnahme verwendet werden. Hier ist relevant, dass vor einem Einsatz eine Einheit festlegt, wie sie eine (Digitalfunk-) Kommunikation im Falle eines Bluetooth-Ausfalls wiederherstellen kann.
- Deaktivierung von Bluetooth bei Nichtverwendung:
  Wird Bluetooth aktuell nicht verwendet oder ist für einen bestimmten Einsatz nicht notwendig, so sollte die Bluetooth-Funktionalität an den beteiligten Endgeräten deaktiviert

werden, sofern möglich, um den Angriffsvektor zu verringern und keine Informationen nach außen dringen zu lassen.

- Regelmäßige Namensänderung der Bluetooth-Endgeräte:
  Namen der Bluetooth-Endgeräte können potentiell Informationen preisgeben wie Typ, Modellbezeichnung, Hersteller, etc. Zudem kann anhand des Namens ein Tracking erfolgen, wann welches Gerät wo vorhanden ist. Daher sollten die Namen der Endgeräte, sofern möglich, auf unverfängliche Namen (wie z. B. Device) geändert werden, die aber dennoch eine generelle Nutzbarkeit der Endgeräte ermöglichen. Für selbst verwaltete Endgeräte wie personenbezogene dienstliche Smartphones sind die jeweiligen Personen zuständig. Für Poolendgeräte sind die jeweiligen verwaltenden Personen für Einsatzmittel einer Dienststelle zuständig. Personenbezogene Informationen dürfen nicht Teil des Namens sein.
- Regelmäßige Überprüfung gekoppelter Endgeräte:
  Die Gerätelisten der Endgeräte sollten in Intervallen auf gekoppelte Endgeräte überprüft werden regelmäßigen (mindestens einmal im Quartal, bestenfalls einmal im Monat). Nicht mehr benötigte Endgeräte sollten entfernt werden, sodass nur aktiv genutzte Kopplungen bestehen bleiben. Unautorisierte Endgeräte sollen entfernt werden, falls vorhanden. Dies kann als eine Art Aufräumarbeit des digitalen Arbeitsplatzes gesehen werden. Für Endgeräte ohne personenbezogene Daten, insbesondere Endgeräte, die von mehreren Personen als Poolgeräte verwendet werden, ist hier die zuständige Person für die Sachbearbeitung der Einsatzmittel pro Stelle verantwortlich.
- Kopplung von Endgeräten in gesicherter Umgebung:
  Eine Kopplung von Endgeräten, die von Endnutzenden durchgeführt wird, ist nur in einer gesicherten Umgebung zulässig. Eine gesicherte Umgebung ist z. B. eine polizeiliche Dienststelle, eine Feuer- oder Rettungswache. Die Kopplung von Endgeräten muss durch berechtigtes Personal erfolgen. Vorher wird festgelegt, welche Endgeräte miteinander gekoppelt und eingesetzt werden. Die Kopplung erfolgt in einem geschützten Raum mit mindestens zwei anwesenden berechtigte Personen oder durch die Person, die ein Endgerät verwaltet. Die Beurteilung der sicheren Umgebung liegt in der Verantwortung der Endnutzenden, die die Kopplung durchführen. Insbesondere für Endgeräte zur Steuerung von weiteren Endgeräten oder Maschinen mit einem hohen Potential der Verletzung anderer Personen oder Objekte, beispielsweise von Drohnen, muss sichergestellt sein, dass die Kopplung in einer kontrollierten physischen Umgebung vor dem Einsatz stattfindet. Diese kontrollierte Umgebung muss die Nähe weiterer potentiell koppelnder Endgeräte ausschließen und unter Aufsicht von mindestens zwei befugten Personen stattfinden. Eine Kopplung am Einsatzort ist nicht zulässig, diese muss vorher erfolgen.

Es sind logistische Maßnahmen zu treffen, die dafür sorgen, dass ein Zubehör nur einem Endgerät zugeordnet ist. Digitalfunkendgeräte dürfen nur nacheinander bzw. räumlich getrennt gekoppelt werden. Nach Abriss der Bluetooth-Verbindung im Einsatz ist darauf zu achten, dass beim erneuten Pairing kein Sicherheitsproblem besteht.

- Minimierung der Nutzung interner Infrastruktur mit Bluetooth-Endgeräten:
  Endgeräte mit aktivierter Bluetooth-Schnittstelle haben ein höheres Risiko, einem Angriff zum Opfer zu fallen und mit beispielsweise Schadsoftware infiziert zu werden, sodass hier ein Angriff auf weitere interne Systeme möglich ist, sofern diese genutzt werden. Daher ist die Verwendung von internen Systemen wie Mails oder Zugriff auf ein Intranet zu minimieren.
- Regelmäßige Überprüfung gespeicherten Bluetooth-Informationen und freigegebener Funktionalitäten:
  Für von Nutzenden verwaltete Endgeräte sollten diese regelmäßig (mindestens einmal im Quartal, bestenfalls einmal im Monat) die freigegebenen Informationen und Funktionalitäten auf Notwendigkeit überprüfen, um das Missbrauchspotential zu verringern.
- Einhaltung der BDBOS-Richtlinie zu Bluetooth im Digitalfunk:
  Die Sicherheitsrichtlinie zu Bluetooth im Digitalfunk schreibt den Mindeststandard Bluetooth 2.1 + EDR vor. Zugleich sind die Kopplungsmodi Numeric Comparison und Passkey Entry zulässig, wobei weitere Kopplungsmodi eine Risikoanalyse benötigen. Diese Risikoanalyse wurde durchgeführt. Somit sind andere Kopplungsmodi möglich, wenn keine der hier aufgeführten realisierbar sind.
- Bevorzugung sicherer Kopplungsmodi:
  Sichere Kopplungsmodi wie Numeric Comparison und Passkey Entry sind zu bevorzugen, sofern diese vom jeweiligen Endgerät unterstützt werden.[3]
- Verwendung einer Maximallautstärke für Audioverbindungen:
  Wird Bluetooth zur Übertragung von Audio verwendet, so soll eine maximale Lautstärke als Gehörschutzmaßnahme eingestellt werden, da ein Angreifer beliebig laute Geräusche abspielen könnte.
- Speicherung von Daten auf mobilen Endgeräten und Backups:
  Endgeräte mit Bluetooth-Schnittstelle sind einem Risiko eines potentiellen Eindringens eines Angreifers ausgesetzt, sodass hier Daten verändert oder gelöscht werden können. Dies betrifft dienstliche Daten, aber auch personenbezogene Daten, weshalb diese nicht nur auf Endgeräten mit Bluetooth gespeichert sein sollten.

[3] Im geschützten Bereich befindet sich eine entsprechende Liste.

- Geschützter Einsatzbereich für Peripherie-Geräte:
  Peripherie-Geräte zu mobilen Endgeräten wie Tastaturen sollten nur in geschützten und kontrollierten physischen Bereichen eingesetzt werden, da diese als Eingabegeräte besonderen Gefahren unterliegen und vergleichsweise häufiger von Schwachstellen betroffen sein können als Geräte, die häufig in der Breite verwendet werden.

Sollte es zu einem häufigen Verstoß gegen die Regeln kommen, was insbesondere die Missachtung der Sicherheitsanforderungen oder die Verwendung von unerlaubten Endgeräten betrifft, und sich daraus eine erhöhte Anzahl an Sicherheitsvorfällen ergeben, dann kann die Verwendung von Bluetooth (temporär) für eine bestimmte Einheit oder einen bestimmten Standort eingeschränkt werden.

6 Regeln zur Verwendung von Bluetooth für die Einsatzleitung

Über die Regeln für die Allgemeinnutzung existieren bestimmte Maßnahmen, die für die Einsatzleitung relevant sind, sodass hier verschiedene Entscheidungskriterien vorliegen, die eine bestimmte Nutzung in deren Verantwortung legt. Konkret handelt es sich dabei um:

- Bevorzugte Verwendung von Endgeräten mit möglichst rechtebeschränkter Konfiguration in kritischen Einsatzfällen:
  Für kritische Einsatzfälle sind Endgeräte mit möglichst beschränkter Konfiguration zu bevorzugen, da hier im Falle einer übernommenen oder unautorisierten Bluetooth-Verbindung möglichst wenig Rechte ausgenutzt werden können, beispielsweise ein möglicher Zugriff auf den AT-Befehlssatz.
- Besondere Vorsicht bei Nutzung von Bluetooth für kritische Einsätze:
  Wird ein Einsatz anhand der Kritikalitätskriterien als kritisch eingestuft, so sind die Vorsichtsmaßnahmen wie die Wachsamkeit auf die Umgebung zur Detektion von Angriffen oder die Sicherstellung von Redundanzmaßnahmen zur Wiederherstellung einer Verbindung bei Störungen besonders zu beachten. Hier soll vor einem Einsatz besonders dafür sensibilisiert werden. Zudem kann die Nutzung von Bluetooth eingeschränkt werden, je nach Ermessen der Einsatzleitung.

- Sicherstellung von Maßnahmen zum Schutz der Vertraulichkeit bei Bluetooth-Nutzung für vertrauliche und geheime Einsätze:
  Hängt der Erfolg eines Einsatzes davon ab, dass dieser geheim abläuft oder ist der Einsatzerfolg durch eine Erkennbarkeit und Identifizierbarkeit polizeilicher Akteure gefährdet, so ist besonders die Sicherstellung der Maßnahmen zur Einschränkung der Detektion wichtig. Darunter zählt das Umbenennen des Namens des Bluetooth-Endgerätes als auch die Deaktivierung der Sichtbarkeit des Bluetooth-Endgerätes.

Die Kriterien zur Bestimmung der Kritikalität eines Einsatzes liegen vor als:

- Eskalationspotential eines Einsatzes:
  Das allgemeine Gefahrenpotential eines Einsatzes sollte bewertet werden anhand der angenommenen Gewaltbereitschaft der dem Ort anwesenden Personen, des Hintergrundes des Einsatzes und des allgemeinen Gefahrenpotentials. Je höher das Eskalationspotential eines Einsatzes ist, desto seltener sollte Bluetooth eingesetzt werden. Dies ist zurückzuführen auf die geringere Verfügbarkeit von Bluetooth und höhere Störungsanfälligkeit im Vergleich zu kabelbasierten Verbindungen.
- Echtzeitanforderungen der (Digitalfunk-)Kommunikation:
  Die Anforderungen an die Kommunikation und ihre Echtzeit sowie Fehlertoleranz und Wiederholbarkeit sollte bewertet werden. Dabei einzuschließen ist die Möglichkeit und Tolerierbarkeit der Wiederholung eines Funkspruches und einen kurzzeitigen Ausfall der (Digitalfunk-)Kommunikation. Dies ist zurückzuführen auf die geringere Verfügbarkeit von Bluetooth und höhere Störungsanfälligkeit im Vergleich zu kabelbasierten Verbindungen.
- Technische Kompetenz der (physischen) Umgebung eines Einsatzes:
  Schadhafte und explizite Bluetooth-Angriffe benötigen eine gewisse technische Kompetenz von Angreifern. Dementsprechend sollte für einen Einsatz bewertet werden, wie technisch versiert die Personen in der Umgebung sind. Darunter fällt zudem die Anzahl an Personen an einem Einsatzort. Je mehr Personen vor Ort sind, desto höher ist auch die Wahrscheinlichkeit, dass entsprechend technisch versierte Personen vor Ort sind. Daher ist diese Bewertung eine Abschätzung zur Angriffswahrscheinlichkeit. Je höher hier die Gefahr für einen Angriff ist, desto zurückhaltender sollte Bluetooth eingesetzt werden.
- Örtliche Gegebenheiten hinsichtlich Funkverbindungen im Allgemeinen und Bluetooth im Besonderen:
  Je nach örtlichen Gegebenheiten herrscht ein gewisses Potential zur Störung der Bluetooth-Verbindungen durch örtlich bedingte Gegebenheiten. Diese Störung kann generelle Kommunikation auf dem 2,4 GHz-Band, beispielsweise durch WiFi, Zigbee oder

weitere Bluetooth-Verbindungen sein, aber auch physische Objekte oder bauliche Gegebenheiten. Je höher hier das Störungspotential eingeschätzt wird, desto zurückhaltender sollte Bluetooth eingesetzt werden.

- Vertraulichkeit der zu erwartenden Funksprüche während des Einsatzes:
  Die während eines Einsatzes übermittelten Informationen können verschiedene Vertraulichkeitsstufen aufweisen. Je vertraulicher die Informationen sind, desto größer ist der potentielle Schaden beim Abhören von Verbindungen. Dieser Angriffsvektor ist bei Bluetooth in einem höheren Maße gegeben vergleichen mit kabelbasierten Verbindungen.

7 Freigabe der Anleitung

Die Dezernatsleitung zeichnet für die Übernahme der Anleitung an Endnutzer in der Verfahrensverantwortung.

Digital unterschrieben von Wächter Stefan
Datum: 2025.05.07 08:02:11 +02'00'

Unterschrift, DL 43 (ASDN)

Hannover, 07.05.2025
Ort, Datum