Konzept: kostenloses WLAN in der Stadt Diepholz

Erstellt von:

Stadt Diepholz
Team IT
Herr Berg
Rathausmarkt 1
49356 Diepholz
T 05441-205
it@stadt-diepholz.de
www.stadt-diepholz.de

Inhalt

1. Einleitung

Der Verwaltungsausschuss hat in der Sitzung vom 13.05.2024 beschlossen, die Verwaltung erarbeitet ein Konzept, wie das Angebot von kostenlosem WLAN in der Stadt ermöglicht werden kann.

Projektziel:

1. Bereitstellung eines flächendeckenden kostenfreien WLANs über eine ca. 700 Meter lange und ca. 10 Meter breite Fläche (Bremer Eck bis Einmündung Schloss)
2. Bereitstellung eines flächendeckenden kostenfreien WLANs auf einer ca. 40.000m² großen Fläche (Müntepark)
3. Bereitstellung eines flächendeckenden kostenfreien WLANs auf einer ca. 5.000m² großen Fläche (Bahnhofsvorplatz incl. ehem. Hotel Steuding und Bus Bahnhof)

In einer zunehmend vernetzten Welt spielt der drahtlose Zugang zum Internet eine entscheidende Rolle für die gesellschaftliche und wirtschaftliche Teilhabe. Öffentliche WLAN-Netzwerke, insbesondere in städtischen Gebieten, bieten nicht nur Touristen und Besuchern einen einfachen Zugang zu digitalen Informationen und Diensten, sondern sind auch für die lokale Bevölkerung von großem Nutzen. Sie ermöglichen eine kostengünstige und oft schnellere Alternative zu mobilen Datenverbindungen und fördern die Nutzung digitaler Angebote, von Navigation bis hin zu öffentlichen Dienstleistungen.

2. Planung

Performance, Stabilität, Technik

Wired Backhaul (LAN-Anbindung):

- Höhere Bandbreite und geringere Latenz: Eine kabelgebundene Verbindung bietet eine stabile und hohe Datenübertragungsrate ohne die Einschränkungen, die durch drahtlose Übertragungen entstehen.
- Skalierbarkeit: Bei 100 Nutzern, die möglicherweise gleichzeitig online sind, ist eine LAN-Anbindung pro Access Point empfehlenswert, um Engpässe zu vermeiden.
- Kosten: Deutlich höhere Kosten, da Erdarbeiten notwendig sind.
- Zuverlässigkeit: Kabelgebundene Verbindungen sind weniger anfällig für Störungen durch externe Faktoren wie Wetter oder Funkinterferenzen. Unanfälliger gegen technische Defekte.

Mesh-Netzwerk (Drahtloser Backhaul):

- Geteilte Bandbreite: Die Access Points teilen sich die verfügbare Bandbreite für Backhaul und Client-Verbindungen, was zu geringerer Performance führen kann.
- Höhere Latenz: Jeder zusätzliche Hop im Mesh-Netzwerk erhöht die Latenz und kann die Benutzererfahrung beeinträchtigen.
- Begrenzte Skalierbarkeit: Bei hoher Nutzerdichte kann ein Mesh-Netzwerk überlastet werden, was zu Verbindungsabbrüchen oder langsamen Geschwindigkeiten führt.
- Kosten: Geringere Kosten, da nur wenige Erdarbeiten notwendig.
- Zuverlässigkeit: Kabellose Verbindungen sind anfällig deutlich anfälliger gegenüber Störungen.

Aus technischer Sicht ist die Implementierung einer Wired-Backhaul-Lösung erforderlich, da die entstehenden Kosten nur durch die Gewährleistung eines stabil und zuverlässig funktionierenden W-LANs gerechtfertigt werden könnten.

Im Folgenden wird somit nur noch die kabelgebunden Variante analysiert.

Installationsaufwand

Der Installationsaufwand einer solchen Lösung lässt sich am besten zusammenfassen unter den folgenden Punkten:

Planung und Standortanalyse:

- Vermessung der Fläche und Identifikation der optimalen Positionen für Access Points (APs).
- Bewertung der Umgebungsbedingungen (z. B. Hindernisse, Signalinterferenzen, Nutzerdichte).
- Prüfung der notwendigen Genehmigungen für Bau- und Installationsarbeiten.

Kabelverlegung und Tiefbauarbeiten:

- Grabenarbeiten für die Verlegung von Glasfaserkabeln und Stromleitungen.
- Installationsaufwand für Leerrohre, Schächte und Kabelschutzsysteme.
- Oberflächenwiederherstellung nach Erdarbeiten (z. B. Asphalt, Pflastersteine, Grünflächen).

Netzwerkhardware-Installation:

- Montage und Befestigung der Access Points (z. B. an Masten, Wänden oder speziell errichteten Halterungen).
- Installation von Netzwerkswitches, PoE-Injektoren und anderen notwendigen Komponenten.
- Stromanschluss für die Geräte (ggf. in Zusammenarbeit mit Elektrikern).

Backhaul-Anbindung:

- Einrichtung und Verbindung der Glasfaserinfrastruktur zwischen den APs und dem zentralen Netzwerk.
- Installation von Netzwerk-Verteilerpunkten für den Backhaul.

Netzwerk-Konfiguration:

- Einrichtung der Access Points (SSID, Sicherheitsprotokolle, QoS).
- Konfiguration von Routern und Switches für optimale Leistung und Redundanz.
- Integration von Monitoring- und Management-Systemen für die Überwachung des Netzwerks.

Tests und Abnahme:

- Signaltests zur Überprüfung der Abdeckung und Signalqualität.
- Belastungstests zur Sicherstellung der Kapazität bei hoher Nutzerdichte.
- Fehlerbehebung und Feinjustierung.

Zusätzliche Herausforderungen:

- Arbeiten in belebten öffentlichen Bereichen mit minimaler Störung der Umgebung.
- Umgang mit unvorhergesehenen Hindernissen (z. B. unterirdische Leitungen, schwierige Bodenverhältnisse).
- Koordination mit Dritten

Kosten

Um eine konkrete Kostenplanung zu entwickeln müssen weitere Parameter zum Thema Verfügbarkeit, Accesspoint-Standorte, datenschutzrechtliche und allgemeinrechtliche Prüfung usw. gegeben sein.
Eine grobe Kostenschätzung kann nur aufgrund von Schätzungen und Erfahrungswerten gegeben werden.

1. Bremer Eck bis Einmündung Schloss (700m x 10m):

- Access Points: 12 APs
- Glasfaserverkabelung:
    - Länge der Straße: 700 Meter
    - Durchschnittliche Kosten pro Meter (inkl. Erdarbeiten): 80–120 EUR/m
    - Gesamtkosten Verkabelung: 56.000–84.000 EUR
- Kosten pro Access Point (Hardware, Installation, Verkabelung): 1.250 EUR
- Gesamtkosten APs: 15.000 EUR.

Gesamtkosten für diese Fläche: **71.000–99.000 EUR**
Laufende Kosten: **2.000–5.000 EUR/Jahr**

2. Müntepark (40.000m²):

- Access Points: 50 APs.
- Glasfaserverkabelung:
    - Geschätzte Gesamtlänge der Verkabelung (inkl. Leitungen zu allen APs): 1.500–2.500 Meter.
    - Durchschnittliche Kosten pro Meter (inkl. Erdarbeiten): 80–120 EUR/m
    - Gesamtkosten Verkabelung: 120.000–300.000 EUR
- Kosten pro Access Point (Hardware, Installation, Verkabelung): 1.250 EUR
- Gesamtkosten APs: 62.500 EUR

Gesamtkosten für diese Fläche: **182.500–362.500 EUR**
Laufende Kosten: **10.000–20.000 EUR/Jahr**

3. Bahnhofsvorplatz (5.000m²):

- Access Points: 8 APs
- Glasfaserverkabelung:
    - Geschätzte Gesamtlänge der Verkabelung (inkl. Leitungen zu allen APs): 300–500 Meter
    - Durchschnittliche Kosten pro Meter (inkl. Erdarbeiten): 80–120 EUR/m.
- Gesamtkosten Verkabelung: 24.000–60.000 EUR
- Kosten pro Access Point (Hardware, Installation, Verkabelung): 1.250 EUR
- Gesamtkosten APs: 10.000 EUR

Gesamtkosten für diese Fläche: **34.000–70.000 EUR**
Laufende Kosten: **1.500–3.000 EUR/Jahr**

Zusammenfassung der Gesamtkosten (Initial):

Lange Straße bis Einmündung Schloss (700m x 10m):	71.000–99.000 EUR
Müntepark (40.000m²):	182.500–362.500 EUR
Bahnhofsvorplatz (5.000m²):	34.000–70.000 EUR
Gesamtschätzung (Initial):	**287.500–531.500 EUR**

Zusammenfassung der laufenden Kosten (jährlich):

Lange Straße (700m x 10m):	2.000–5.000 EUR
Müntepark (40.000m²):	10.000–20.000 EUR
Bahnhofsvorplatz (5.000m²):	1.500–3.000 EUR
Gesamtschätzung (jährlich):	**13.500–28.000 EUR**

Wichtige Annahmen:

In dieser Schätzung enthalten sind die Kosten für die Schaffung eines neuen Netzwerks. Eventuelle vorhandene Strukturen sind nicht in die Planung eingerechnet.

Planung:
- Die Planung bezieht sich auf ein flächendeckendes WLAN, welches sich über die gewünschten Gebiete erstreckt.

Kosten für Erdarbeiten und Glasfaserkabel:
- Die Erdarbeiten (Graben, Kabelverlegung, Wiederherstellung der Oberfläche) sind für jede Fläche berücksichtigt.
- Tiefbaukosten variieren je nach Untergrund (Asphalt, Erde, Pflaster).

Access Point-Verteilung:
- APs sind strategisch verteilt, sodass die Abdeckung ohne übermäßige Überlappung gewährleistet ist.

Laufende Kosten:
- Beziehen sich auf Wartung, Stromversorgung und Internetanbindung.

5. Technische Risiken

5.1 Technische Risiken

Öffentliches WLAN in einer Fußgängerzone bietet zwar Bequemlichkeit, birgt aber auch erhebliche Risiken. Hier sind die wichtigsten Gefahren:

1. Datenabfang (Man-in-the-Middle-Angriffe): Hacker können den Datenverkehr zwischen Nutzer und WLAN abfangen. Dies ermöglicht es ihnen, sensible Informationen wie Passwörter, Bankdaten oder persönliche Nachrichten mitzulesen.
2. Unsichere Verschlüsselung: Viele öffentliche WLAN-Netzwerke verwenden schwache oder gar keine Verschlüsselung, was es Angreifern erleichtert, auf die Daten der Nutzer zuzugreifen.
3. Gefälschte WLAN-Hotspots: Angreifer können einen „Evil Twin“-Hotspot einrichten, der sich als legitimes WLAN ausgibt. Sobald sich Nutzer mit diesem verbinden, können Hacker leicht auf ihre Daten zugreifen.
4. Malware-Infektionen: Öffentliches WLAN kann genutzt werden, um Malware, Viren oder Trojaner auf das Gerät eines Nutzers zu übertragen, besonders wenn keine Sicherheitssoftware installiert ist.

5. Snooping und Sniffing: Hacker können spezielle Software verwenden, um den Datenverkehr im Netzwerk zu "schnüffeln" und persönliche Informationen wie E-Mails, Nachrichten oder Passwörter zu stehlen.
6. Automatische Verbindung zu unsicheren Netzwerken: Viele Geräte verbinden sich automatisch mit bekannten Netzwerken. Wenn ein Angreifer ein öffentliches WLAN nachahmt, könnten sich Nutzer unbewusst verbinden und so ihre Daten preisgeben.
7. Fehlende Sicherheitsupdates: Öffentliche WLANs können Geräte angreifbar machen, besonders, wenn diese nicht regelmäßig aktualisiert werden. Dies erhöht das Risiko, Opfer von Sicherheitslücken oder Angriffen zu werden.

Insgesamt ist die Nutzung von öffentlichem WLAN mit Vorsicht zu genießen. Um das Risiko zu minimieren, sollten Nutzer auf sichere Verbindungen achten, VPN-Dienste verwenden und sensiblen Datenverkehr vermeiden.

6. Datenschutzrechtliche Analyse

Die Bereitstellung und Nutzung öffentlicher WLAN-Netze in Deutschland ist datenschutzrechtlich streng reguliert, insbesondere im Hinblick auf die Datenschutz-Grundverordnung (DSGVO) und das Telekommunikationsgesetz (TKG). Hier sind die wichtigsten Punkte, die die datenschutzrechtliche Lage betreffen:

Erfassung und Speicherung personenbezogener Daten

Anbieter öffentlicher WLANs müssen sich an die DSGVO halten, wenn sie personenbezogene Daten ihrer Nutzer erheben, verarbeiten oder speichern. Zu den personenbezogenen Daten zählen u.a. die IP-Adressen, MAC-Adressen oder Nutzungsverhalten im Netzwerk.

- Einwilligungspflicht**:** Nutzer müssen transparent darüber informiert werden, welche Daten gesammelt werden und zu welchem Zweck. In der Regel geschieht dies durch eine Einwilligung, beispielsweise beim Login-Prozess über eine Login-Seite oder durch Akzeptieren der Nutzungsbedingungen.
- Datensparsamkeit**:** Nur die unbedingt notwendigen Daten dürfen erhoben werden. Das bedeutet, dass Anbieter keine unnötigen oder übermäßigen Daten speichern dürfen. Beispielsweise ist es unzulässig, umfangreiche Nutzungsprofile ohne klaren Zweck zu erstellen.

Verantwortung des WLAN-Anbieters

Anbieter öffentlicher WLANs sind datenschutzrechtlich für die Datenverarbeitung verantwortlich. Sie müssen sicherstellen, dass die erhobenen Daten sicher verarbeitet werden und nicht unbefugt in die Hände Dritter gelangen.

- Sicherheitsmaßnahmen**:** Es muss sichergestellt werden, dass geeignete technische und organisatorische Maßnahmen zum Schutz der Daten implementiert sind. Dazu gehört, dass der WLAN-Zugang mit modernen Verschlüsselungsverfahren gesichert wird.
- Informationspflicht**:** Anbieter sind verpflichtet, den Nutzern mitzuteilen, wie ihre Daten verwendet werden, und müssen eine Möglichkeit zur Kontaktaufnahme anbieten, falls ein Nutzer Fragen zum Datenschutz hat.

Störerhaftung

Die rechtliche Situation um die Störerhaftung hat sich seit dem Inkrafttreten des Telekommunikationsgesetzes (TKG) 2017 entspannt. Früher konnten WLAN-Anbieter für illegale Handlungen ihrer Nutzer haftbar gemacht werden (z.B. illegales Filesharing). Nach der Reform des TKG sind WLAN-Anbieter jedoch nicht mehr haftbar, wenn sie sich an bestimmte Bedingungen halten, wie z.B. Sicherungsmaßnahmen zur Verhinderung von Rechtsverletzungen durch ihre Nutzer.

Anonymität und Logging

Ein weiteres wichtiges Thema im Zusammenhang mit öffentlichem WLAN ist die Frage der Anonymität. Laut DSGVO dürfen Anbieter nur so viele Daten erfassen, wie unbedingt notwendig sind. Theoretisch ist es möglich, ein WLAN-Netzwerk ohne Registrierung anonym zu betreiben, jedoch verlangen viele Anbieter eine Anmeldung (z.B. mit E-Mail-Adresse oder Telefonnummer).

- Logging: Es ist umstritten, ob Anbieter öffentliche WLANs permanent Nutzeraktivitäten protokollieren dürfen. Nach DSGVO müssen solche Logs auf das Minimum beschränkt sein und dürfen nur bei konkretem Anlass oder einer gesetzlichen Verpflichtung gespeichert werden.

Richtlinie zur Speicherung von Verbindungsdaten

Die Speicherung von Verbindungsdaten ist datenschutzrechtlich besonders kritisch. Hier greifen die Regeln der Vorratsdatenspeicherung, die es verbieten, Daten ohne triftigen Grund langfristig zu speichern. WLAN-Anbieter dürfen also keine umfassenden Protokolle über die Internetaktivitäten der Nutzer führen, es sei denn, dies ist für die Bereitstellung des Dienstes unbedingt erforderlich oder gesetzlich vorgeschrieben.

Zustimmung und Informationspflichten

WLAN-Anbieter müssen ihre Nutzer über die Datenverarbeitung informieren. Dies umfasst in der Regel eine Datenschutzrichtlinie, die erklärt, welche Daten erfasst werden, wie lange sie gespeichert werden und welche Rechte die Nutzer haben (z.B. Auskunft, Löschung).

- Transparenz: Die Nutzer müssen klar und einfach verständlich darüber informiert werden, welche Daten gesammelt werden. Häufig geschieht dies durch Pop-ups oder Anmeldeseiten, die die Zustimmung der Nutzer einholen.

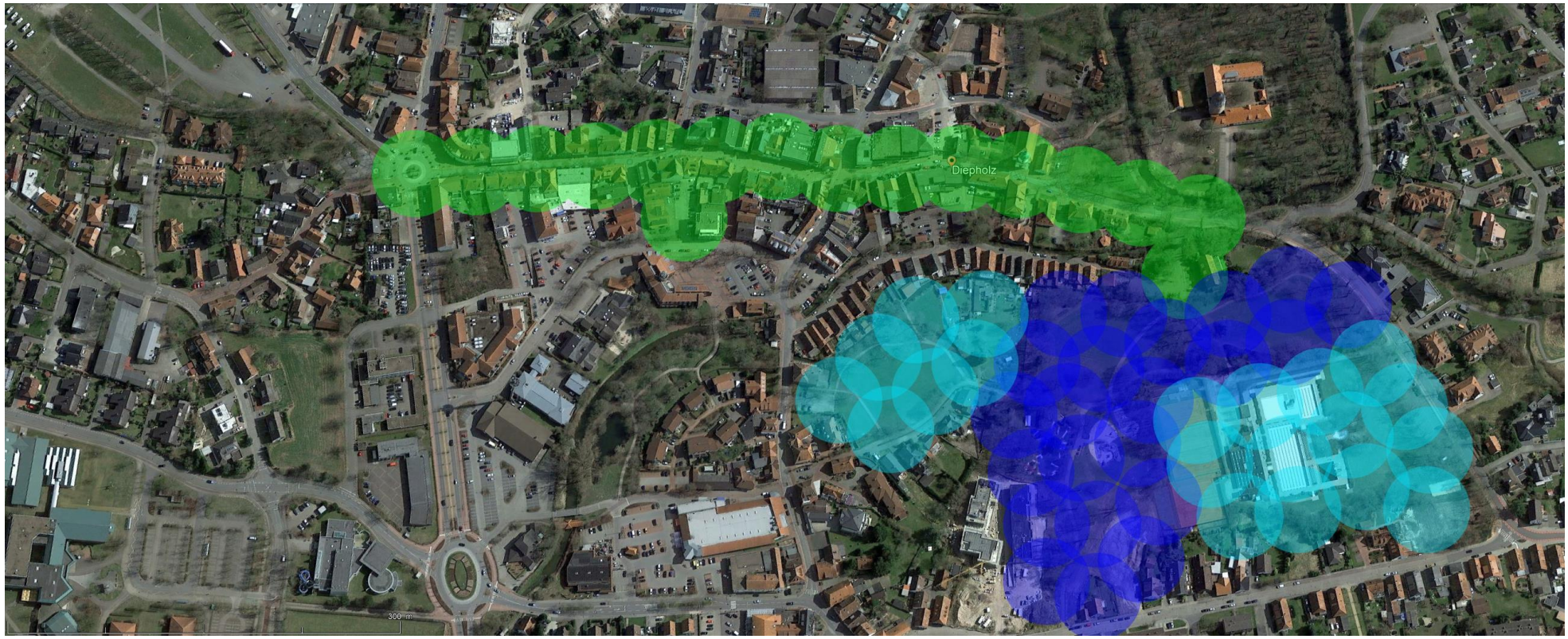
Fazit:

Aus Sicht der Stadt Diepholz ist ein solches WLAN nur Ganzheitlich zu erreichen, wenn man in einem großen Projekt entsprechende Bereiche modernisiert oder umbaut. Eine „Nebenbei“-Schaffung eines komplexen innenstadtumfassenden kabellosen Funknetzwerks ist nicht realistisch. Darüber hinaus verlieren öffentliche WLANs durch den Ausbau von 5G-Netzen zunehmend an Bedeutung – auch Aufgrund der Unsicherheiten, die ein solches Netz mit sich bringt.

Öffentliches WLAN in Deutschland unterliegt strengen Datenschutzanforderungen. Anbieter müssen sicherstellen, dass sie nur notwendige Daten erheben, diese sicher verwalten und die Nutzer transparent informieren. Die DSGVO bietet hierbei den rechtlichen Rahmen, um den Schutz der Privatsphäre zu gewährleisten. Nutzer sollten bei der Verwendung von öffentlichem WLAN ebenfalls Vorsicht walten lassen, da trotz der gesetzlichen Vorgaben die Sicherheit nicht immer gewährleistet ist. Dieses Verursacht bei dem Betreiber hohe laufende Kosten.

Final ist zu beachten, dass ein öffentliches WLAN nur dann erfolgreich realisiert werden kann, wenn die Anwohner und eventuell angrenzende Firmen oder Geschäfte dessen Einführung unterstützen und Gut heißen, da neben den Vorteilen auch potenzielle Risiken, wie Datenschutz- und Sicherheitsfragen, berücksichtigt werden müssen.

Anlage I: Plan Bremer Eck bis zum Schloss



Anlage II Plan Bahnhof