NOKIA

D211

DATENSICHERHEIT

NOKIA

Copyright © Nokia Corporation 2002. All rights reserved. | Ver. 1.0

Inhalt

Rechtliche Hinweise

Copyright © Nokia Corporation 2002. Alle Rechte vorbehalten.

Der Inhalt dieses Dokuments darf ohne vorherige schriftliche Genehmigung durch Nokia in keiner Form, weder ganz noch teilweise, vervielfältigt, weitergegeben, verbreitet oder gespeichert werden.

Nokia und Nokia Connecting People sind eingetragene Marken der Nokia Corporation. Andere in diesem Handbuch erwähnte Produkt- und Firmennamen können Marken oder Handelsnamen ihrer jeweiligen Eigentümer sein.

Nokia entwickelt entsprechend seiner Politik die Produkte ständig weiter. Nokia behält sich deshalb das Recht vor, ohne vorherige Ankündigung an jedem der in dieser Dokumentation beschriebenen Produkte Änderungen und Verbesserungen vorzunehmen.

Nokia ist unter keinen Umständen verantwortlich für den Verlust von Daten und Einkünften oder für jedwede besonderen, beiläufigen, mittelbaren oder unmittelbaren Schäden, wie immer diese auch zustande gekommen sind.

Der Inhalt dieses Dokuments wird so präsentiert, wie er aktuell vorliegt. Nokia übernimmt weder ausdrücklich noch stillschweigend irgendeine Gewährleistung für die Richtigkeit oder Vollständigkeit des Inhalts dieses Dokuments, einschließlich, aber nicht beschränkt auf die stillschweigende Garantie der Markttauglichkeit und der Eignung für einen bestimmten Zweck, es sei denn, anwendbare Gesetze oder Rechtsprechung schreiben zwingend eine Haftung vor. Nokia behält sich das Recht vor, jederzeit ohne vorherige Ankündigung Änderungen an diesem Dokument vorzunehmen oder das Dokument zurückzuziehen.

1. EINLEITUNG

Die neue Nokia D211 Multimodus-Funkkarte ist eine ideale Lösung für mobile Geschäftsleute, die von unterwegs den Zugriff auf das Unternehmensnetzwerk wünschen. Die übermittelten Informationen sind dabei häufig entscheidend für den Geschäftserfolg eines Unternehmens und dürfen nicht an Außenstehende gelangen. Daher nimmt die Sicherheit bei der Verwendung der Nokia D211 für Fernzugriffsdienste eine wichtige Rolle ein.

In diesem Dokument wird erläutert, was im Hinblick auf die Sicherheit bei der Verwendung der Nokia D211 zu beachten ist. Die Grundlagen der Internetsicherheit werden aufgezeigt und einige Referenzarchitekturen vorgestellt, die über GPRS-Netzwerke (General Packet Radio Service) und WLANs (Wireless Local Area Networks) einen sicheren Zugriff auf ein Unternehmensnetzwerk ermöglichen.

2. FERNZUGRIFFSARCHITEKTUREN

2.1 DFÜ-MODEMZUGRIFF

Bis vor kurzem wurden Fernzugriffsdienste meistens mit Hilfe von Standleitungen, DFÜ-Modems und Fernzugriffsservern implementiert. Die Verbindung wird unter Verwendung des öffentlichen Telefonnetzes sowie des bekannten Point-to-Point Protokolls (PPP) aufgebaut, das in nahezu jeder Terminalsoftware vorhanden ist. Die DFÜ-Verbindung wird über ein Festnetztelefon oder ein Funkterminal hergestellt. Der Fernzugriffsserver authentifiziert den Benutzer mit Hilfe eines Kennworts. Weitere spezielle Sicherheitsmechanismen kommen dabei normalerweise nicht zum Einsatz.

Die Nokia D211 bietet zwei Alternativen für die Anwahl: GSM-Daten und HSCSD (High Speed Circuit Switched Data). Bei dieser Einrichtung schützt das GSM-Netzwerk die Benutzerdaten über die Luftschnittstelle. Auf diese Weise erfordert der Funkzugriff keine zusätzlichen Sicherheitseinrichtungen, sondern kann genau wie ein DFÜ-Festnetzmodem verwendet werden. Die DFÜ-Verbindung wird gewöhnlich über die DFÜ-Funktion in Microsoft Windows aufgebaut.

2.2 SICHERER INTERNETZUGRIFF (GPRS, WLAN)

Die neuen kabellosen Internettechnologien, wie etwa GPRS und Funk-LAN, stellen eine schnellere und kostengünstigere Methode für den Zugriff auf Unternehmensdaten dar. Die neuen Zugriffsmechanismen erfordern einige Erweiterungen in der Unternehmensplattform für Fernzugriffsdienste, damit die Vertraulichkeit der Daten gewährleistet werden kann.

Abbildung 1 zeigt die Architekturen für DFÜ- und Internetfernzugriff. Der Hauptunterschied besteht darin, dass GPRS und Funk-LAN anstatt eines Telefonnetzes den Internet-Backbone als Gateway zum Unternehmensnetzwerk verwenden. Die Benutzerdaten werden unter Verwendung von Internetprotokollen aus dem Handynetz über das unsichere Internet an das Unternehmensnetzwerk übermittelt.

Das öffentliche Internet ist jedoch einer Vielzahl von Sicherheitsrisiken ausgesetzt. Eine große Sicherheitsschwäche besteht darin, dass, anders als bei einer Point-to-Point-DFÜ-

Verbindung, Internetpakete für jeden, der Zugriff zum Netzwerk hat, lesbar sind. Zudem folgen IP-Pakete häufig derselben Route, so dass ein potenzieller Angreifer sehr wahrscheinlich Zugriff auf alle IP-Pakete hat. Die Sicherheitsfunktionen von Funknetzwerken (GPRS und WLAN) reichen allein nicht aus, um die Vertraulichkeit zu gewährleisten. Durch Kombination von Funkzugriff mit einer End-to-End-Internetsicherheitslösung (IP) kann ein hoch zuverlässiges Fernzugriffssystem erstellt werden.

Hinweis: Für einen sicheren GPRS-/WLAN-Zugriff empfiehlt Nokia die Verwendung einer gebräuchlichen VPN-Sicherheitslösung (Virtual Private Network), die auf IP-Ebene arbeitet.

In den folgenden Abschnitten wird gezeigt, wie diese Technologie für GPRS-Zugriff, Funk-LAN-Unternehmenskonnektivität und private Vernetzung verwendet werden kann.

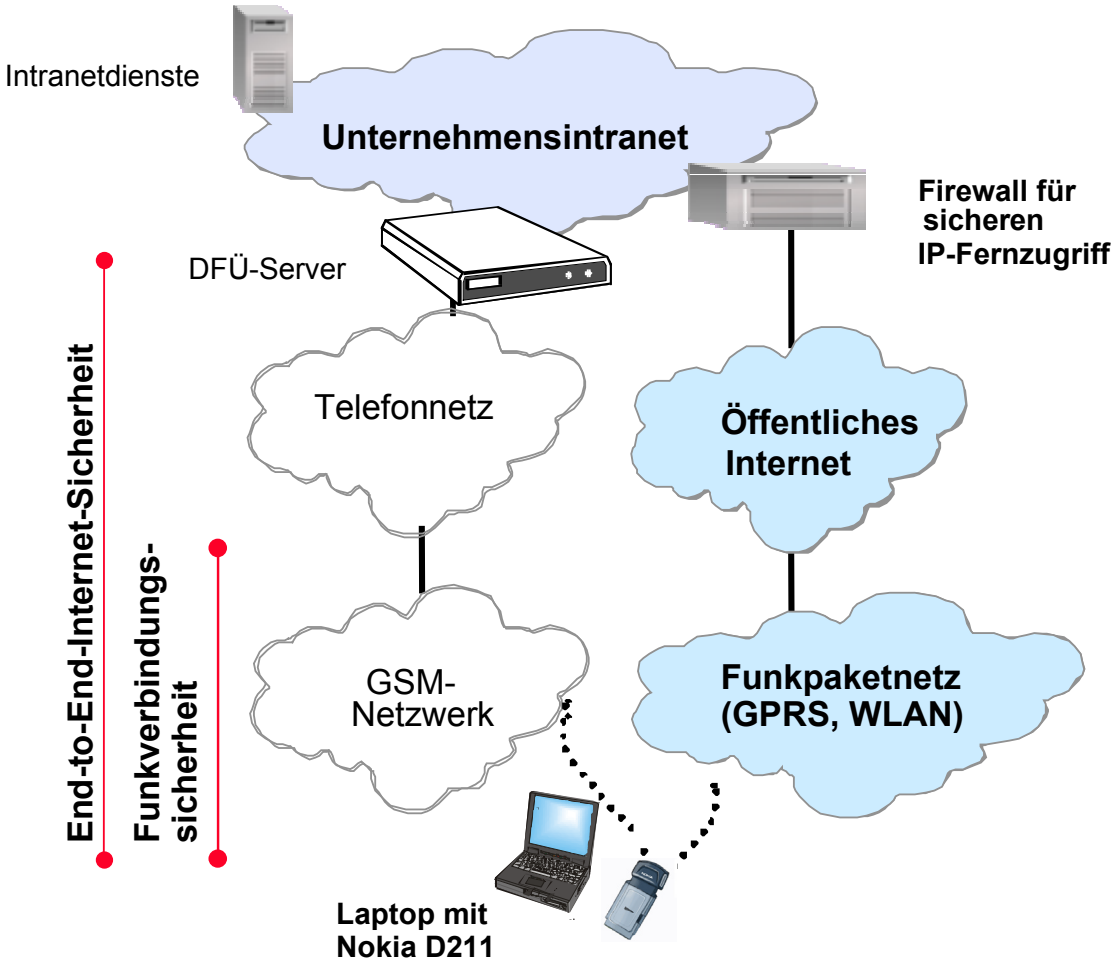

Abbildung 1: Alternative Fernzugriffsmechanismen: DFÜ- und Internetzugriff

2.2.1 Anforderungen an die Internetsicherheit

Eine Internetsicherheitslösung sollte folgende wichtige Funktionen bieten, um die Sicherheit von Daten und Unternehmensnetzwerk gewährleisten zu können:

- Eine Zugriffssteuerung, die den Zugriff auf das Unternehmensnetzwerk für nicht autorisierte Benutzer beschränkt.
- Eine Verschlüsselung, die verhindert, dass jeder die über das Internet transportierten Daten lesen oder kopieren kann. Die Datenverschlüsselung erfolgt zum Schutz der Daten vor nicht autorisierten Benutzern durch Kodierung des Inhalts. Es stehen sehr viele Verschlüsselungsmethoden zur Verfügung, die sich hauptsächlich durch ihren Verschlüsselungsalgorithmus unterscheiden.
- Eine Authentifizierung, die gewährleistet, dass die Daten aus der von ihnen angegebenen Quelle stammen.

Die VPN-Technologie (Virtual Private Network) wird häufig zur Verbindung von Unternehmens-LANs verschiedener Standorte oder externer Geschäftspartner mit dem Unternehmensnetzwerk eingesetzt.

2.2.2 Kurzbeschreibung der VPN-Technologie (Virtual Private Network)

Abbildung 2 zeigt eine typische VPN-Konfiguration. Dieselbe Technologie und Plattform kann auch zur Bereitstellung eines sicheren Fernzugriffs für Benutzer von GPRS und Funk-LAN verwendet werden.

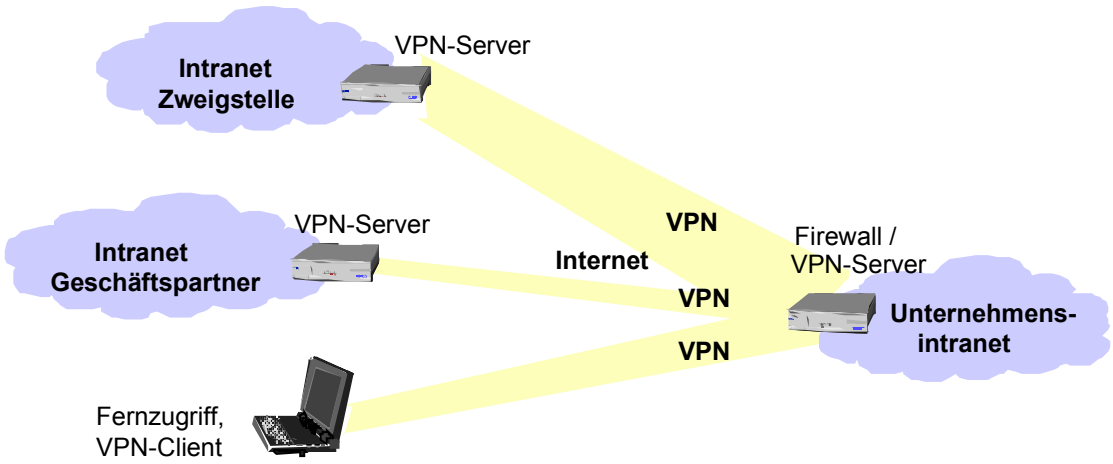

Abbildung 2: VPN (Virtual Private Network)

Die VPN-Lösung besteht aus einem Netzwerkserver und der Clientsoftware. Der VPN-Server schützt das Netzwerk sowohl vor eingehender als auch ausgehender unerwünschter oder nicht autorisierter Kommunikation. Der gesamte Datenverkehr zum privaten Netzwerk muss den VPN-Server passieren. Es wird ein Tunnel zwischen dem Terminal und dem VPN-Server erzeugt, und die Benutzerdaten werden in diesem Tunnel authentifiziert, verschlüsselt und an den Host übertragen.

Der Vorteil des VPN besteht darin, dass es die vom und zum Intranet übertragenen Informationen schützt und nicht autorisierten Zugriff verhindert. VPNs erhalten Verbindungen zwischen den Endpunkten nicht durchgehend aufrecht. Wenn eine Verbindung zwischen einem Terminal und dem Unternehmensnetzwerk benötigt wird, wird sie erstellt und nach Beenden der Sitzung geschlossen. Der Client initiiert den sicheren Tunnel, und der Remote-Benutzer wird vom Netzwerk authentifiziert. Durch die Benutzerauthentifizierung werden die Identitäten der Remote-Benutzer bestätigt. Der Zugriff auf das Unternehmensnetzwerk wird erst nach erfolgreicher Durchführung der Authentifizierung gewährt. Es gibt unterschiedliche alternative Authentifizierungsmechanismen, wie etwa Kennwörter, Sicherheitstoken (z.B. gespeichert auf einer Smart-Card) und Zertifikate.

Das End-to-End-Tunnelling schützt die Datenübertragung vor Sicherheitsangriffen. Häufig beinhalten die VPN-Clients und VPN-Server auch eine integrierte Firewall. Eine so genannte persönliche Firewall filtert die eingehenden Daten und lässt Internetverbindungen nur über vordefinierte Hosts zu. So wird verhindert, dass ein Angreifer auf das Fernterminal zugreifen kann.

Die integrierte Verschlüsselung gewährleistet, dass es für nicht autorisierte Parteien praktisch unmöglich ist, Daten zu lesen. Die meisten VPN-Geräte stellen zwischen den Kommunikationsparteien automatisch die leistungsfähigsten Algorithmen zur Verschlüsselung und Datenauthentifizierung ein. Die Verschlüsselung ist für alle Anwendungen, z.B. E-Mail und Webbrowser, die die IP-Protokolle verwenden, transparent. Die einzige bedeutende Auswirkung ist, dass durch die VPN-Einkapselung einige zusätzliche Daten beigefügt werden, die über die Funkverbindung übermittelt werden müssen.

2.2.3 Kommerzielle VPN-Anwendungen

Auf dem Markt ist ein breites Spektrum kommerzieller VPN-Lösungen erhältlich. Ein VPN-Sicherheitsgateway kann zu einer der folgenden Kategorien gehören: Hochleistungs-VPN-Router, Firewalls, integrierte VPN-Hardware und preiswerte VPN-Software. In Routern ist normalerweise Paketverschlüsselung integriert, entweder als Add-on-Software oder als zusätzliche Platine. Letztere Möglichkeit ist für Situationen, die einen höheren Durchsatz erfordern, am besten geeignet. Die Kombination aus Tunnelling und Verschlüsselung mit Firewalls eignet sich für kleine Netzwerke mit geringem Datenverkehr am besten.

In den meisten Fällen wird das VPN-System vom IT-Leiter des Unternehmens ausgewählt und verwaltet. Die erhältliche Produktpalette ist sehr umfangreich. Das Hauptkriterium für die Auswahl der geeigneten Lösung ist die erforderliche Kapazität, die sich in der Praxis aus der Anzahl von Fernzugriffsbenutzern ergibt. Gewöhnlich muss das VPN eine Umwandlung vom IP-Adress-Schema des Unternehmensnetzwerks in das des Betreibernetzwerks vornehmen. Daher ist es empfehlenswert, eine Lösung auszuwählen, die NAT (Network Address Translation) unterstützt.

Die standardisierte Kompatibilität von unterschiedlichen VPN-Geräten garantiert die Kompatibilität des VPN-Clients mit einer Vielzahl von VPN-Servern. Die Nokia D211 ist kompatibilitätsgeprüft mit führenden VPN-Client- und VPN-Server-Produkten. Eine ausführliche Liste der geprüften Produkte finden Sie unter www.nokia.com.

2.2.4 Persönliche Firewall

Eine persönliche Firewall ist eine Software mit einem Satz von Firewall-Regeln, mit deren Hilfe der Netzverkehr über einen Computer freigegeben oder abgeblockt wird. Darüber hinaus dient diese Software zur Überwachung und Steuerung von Anwendungen, um vor Trojanern und Keyloggern zu schützen. Sie dient in erster Linie zur Verbesserung der Sicherheit bei Verwendung eines VPN-Clients. Mit Hilfe einer persönlichen Firewall wird der Zugriff auf den PC eines Benutzers kontrolliert. Wenn Ihr Laptop in einem unsicheren Netzwerk verwendet wird, muss bei der Konfiguration eine sehr hohe Sicherheitsstufe gewählt werden. Tatsächlich müssen alle Versuche, eine Verbindung zu Ihrem Computer herzustellen, abgewiesen werden. Wenn die Firewall-Engine einen Eindringling entdeckt, gibt sie den Befehl an die Software aus, die IP-Adresse des Hackers zu blockieren. Da die Firewall die Datenübermittlung auf der TCP/IP Stack-Ebene kontrolliert, können Hacker die Blockade durch die Firewall nicht umgehen. Diese Art von Schutz muss, unabhängig vom Standort, immer aktiviert sein.

2.3 SICHERHEIT AUF ANWENDUNGSEBENE FÜR DAS BROWSEN IM INTERNET

Manche Internetanwendungen, wie z.B. Webbrowser, bieten eine zusätzliche Sicherheitsebene. Die aktuellen Versionen von Netscape und Internet Explorer verwenden Sicherheitsprotokolle auf Anwendungsebene, etwa Transport Layer Security und SSL (Secure Socket Layer), die dem Benutzer die Datensicherheit zwischen Clientanwendung und Server bieten. Diese Mechanismen sind z.B. beim Internetbanking und elektronischen Transaktionen weit verbreitet.

Durch die Sicherheit auf Anwendungsebene wird eine zusätzliche Sicherheitsstufe gewährleistet, die für den Internetzugriff genutzt werden kann, wenn keine vertraulichen Unternehmensdaten betroffen sind und auch das mobile Terminal keine vertraulichen Informationen enthält. In solchen Fällen kann der Benutzer die Nokia D211 ohne VPN-Dienste verwenden. Die Mechanismen für die Sicherheit auf Anwendungsebene schützen das mobile Terminal jedoch nicht vor externen Angriffen. Außerdem ist der Umfang der Verschlüsselung häufig geringer als bei der VPN-Verbindung.

Hinweis: Bei Anwendungen für Unternehmensdaten sollte der Benutzer stets End-to-End-VPN-Tunnelling einsetzen. Die Sicherheit auf Anwendungsebene bietet dann eine zusätzliche Sicherheitsebene, die auf dem VPN-Tunnelling aufsetzt.

3. SICHERER GPRS-ZUGRIFF AUF DAS UNTERNEHMENSNETZWERK

Das standardmäßige GPRS-Netzwerk bietet Datensicherung über die Luftschnittstelle, bietet jedoch keine End-to-End-Internetsicherheitslösung für den mobilen Zugriff auf ein Unternehmens-LAN. Das GPRS-Netzwerk bietet zwei Sicherheitsfunktionen: *Teilnehmerauthentifizierung* und *Datenverschlüsselung.* Die Vorgänge der Benutzerauthentifizierung in GPRS sind mit jenen im GSM-Netzwerk vergleichbar. Alle Sicherheitsfunktionen basieren auf dem Geheimschlüssel Ki, der sowohl auf der SIM-Karte

(Subscriber Identification Module) als auch in der Heimatdatenbank (HLR/Home Location Register) des Betreibers gespeichert ist. In GPRS werden Daten und Signale zwischen dem Terminal und dem Internet chiffriert.

Hinweis: Bei Verwendung einer GPRS-Verbindung mit der Nokia D211 zur Unternehmenskonnektivität ist der Einsatz einer VPN-Sicherheitslösung empfehlenswert, die End-to-End-Authentifizierung und Datenverschlüsselung bietet.

VPN ist nicht notwendig, wenn GPRS für nicht vertrauliche Anwendungen, z.B. zum Durchsuchen des Internets, verwendet wird. Gewöhnlich wird der VPN-Dienst vom IT-Management des Unternehmen oder durch den Mobilfunkbetreiber bereitgestellt. Das in Abbildung 3 dargestellte System funktioniert wie folgt:

1. Der Benutzer aktiviert die GPRS-Verbindung.
2. Das GPRS-Netzwerk authentifiziert das mobile Terminal mit der SIM-Karte und baut eine sichere Funk-GPRS-Verbindung zum Internet (GPRS-Verschlüsselung) auf.
3. Der Benutzer startet auf dem mobilen Terminal den VPN-Client, der einen verschlüsselten End-to-End-IP-Tunnel zum Unternehmensnetzwerk aufbaut (Internetdatenverschlüsselung).

Diese Lösung ist extrem zuverlässig und sicher, da der gesamte Datenverkehr auf der gesamten Strecke zwischen dem mobilen Terminal und dem VPN-Server im Unternehmen verschlüsselt ist und VPN ein hohes Maß an Sicherheit bietet. Der Benutzer kann über ein beliebiges GPRS-Betreibernetzwerk auf das Intranet zugreifen.

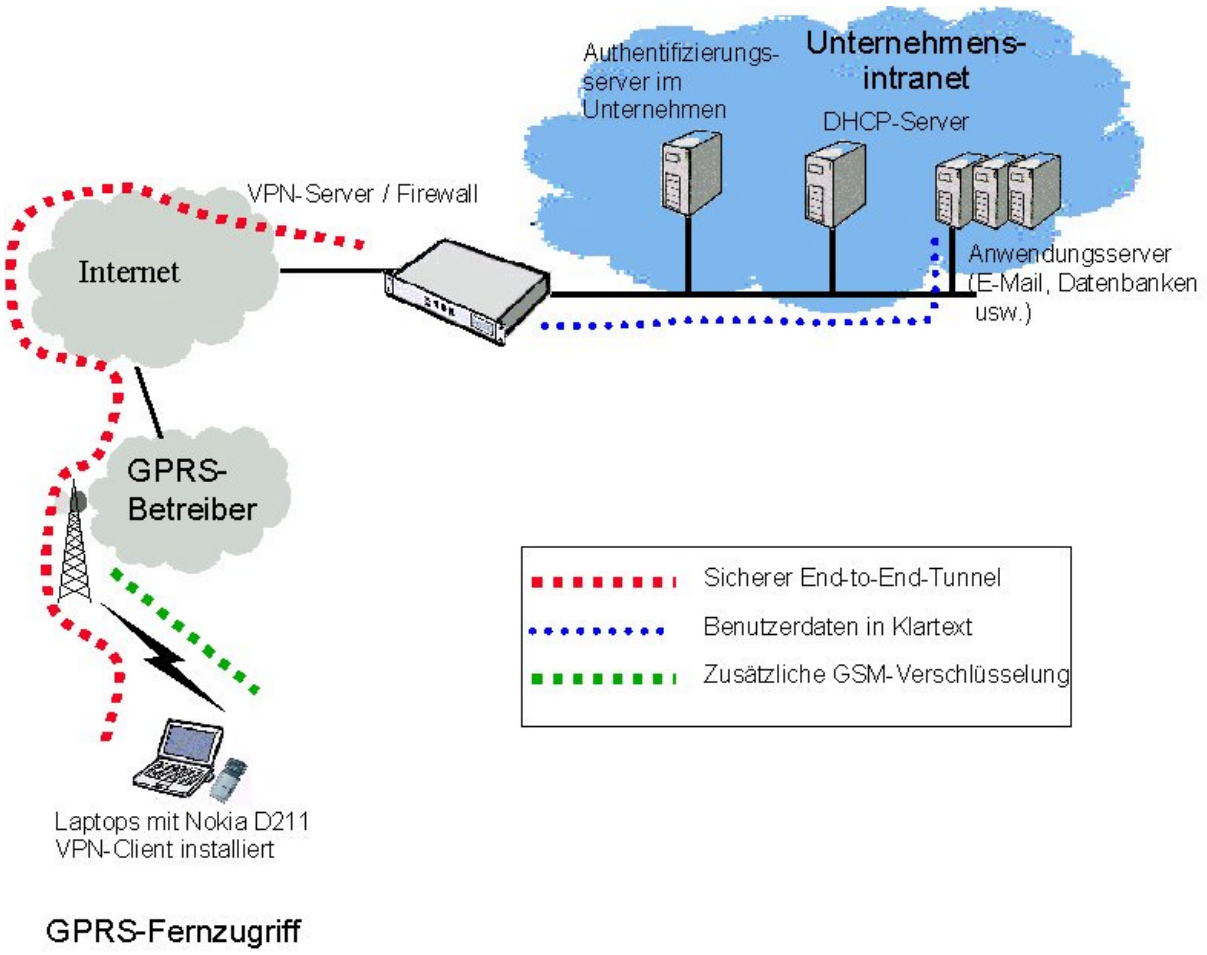

Abbildung 3: Sicherer GPRS-Zugriff auf das Unternehmensnetzwerk

Eine alternative Konfiguration ist die Verwendung einer Standverbindung vom GPRS-Netzwerk des Mobilfunkbetreibers zum Unternehmensintranet und damit die völlige Umgehung des öffentlichen Internets. In diesem Modell erfordert das mobile Terminal keinen VPN-Client. Die Sicherheitsfunktionen des GPRS-Netzwerks schützen die Daten zwischen dem Terminal und dem GPRS-Kern. Der Mobilfunkbetreiber baut dann einen sicheren Tunnel zwischen dem Betreibernetzwerk und dem Unternehmensnetzwerk auf. Bei diesem Ansatz muss der Unternehmenskunde dem Mobilfunkbetreiber, der das sichere Tunnelling anbietet, vertrauen. Einige Mobilfunkbetreiber bieten ihren Großkunden diese Art von Lösung an. Einzelheiten dazu erhalten Sie von Ihrem Mobilfunkbetreiber.

4. SICHERER FUNK-LAN-ZUGRIFF

Funk-LANs kommen gewöhnlich in Unternehmens-, privaten oder öffentlichen Zugangszonen, wie etwa Hotels, Flughäfen usw., zum Einsatz. Dank Funk-LANs können sämtliche Mitarbeiter sich frei im Büro und in Konferenzräumen bewegen oder zu Hause arbeiten und gleichzeitig immer auf die neuesten Informationen aus dem Unternehmensnetzwerk zugreifen. Wie GPRS nutzt auch das Funk-LAN den

Internetbackbone. Daher unterstützt dieselbe sichere VPN-Fernzugriffsplattform sowohl GPRS als auch Funk-LAN. Der Nokia D211-Benutzer kann zwischen einer GPRS- oder Funk-LAN-Verbindung wählen, und zur Verbindung mit dem Unternehmensnetzwerk dann dieselbe VPN-Konfiguration nutzen.

Das WLAN kann ein Sicherheitsrisiko darstellen, da die Funksignale aus dem Bürogebäude herausdringen. Durch angemessene Authentifizierung und Verschlüsselung können Sicherheitsrisiken in einem Funk-LAN vermieden werden.

Hinweis: Nokia empfiehlt den Einsatz einer End-to-End-VPN-Lösung, wenn über das Funk-LAN auf das Unternehmensnetzwerk zugegriffen wird.

Die Funk-LAN-Spezifizierung (IEEE 802.11b) beinhaltet den Sicherheitsalgorithmus Wired Equivalent Privacy (WEP), der zur Authentifizierung der Terminals im WLAN sowie zur Verschlüsselung der Daten an der Funkverbindung verwendet werden. Die Sicherheitsstufe von WEP ist verglichen mit IP-Sicherheit (VPN) niedrig. WEP kann als eine zusätzliche Sicherheitsebene aktiviert werden, die zur Steuerung des Zugriffs auf das Funk-LAN verwendet wird, z.B. zu Hause. Die richtige Wahl für die Steuerung des Zugriffs auf ein Unternehmensnetzwerk oder für die Sicherung vertraulicher Daten ist es nicht.

Einige Anbieter haben für die WEP-Sicherheit eigene Erweiterungen, wie z.B. 802.1x-Erweiterungen, implementiert und behaupten, dass diese ausreichen, um die Sicherheit des Unternehmensnetzwerks zu gewährleisten. Die Sicherheitsstufe dieser nicht standardisierten Lösungen ist im Vergleich zu einer End-to-End-VPN-Lösung jedoch erheblich niedriger. Die Kombination aus Funk-LAN und ordnungsgemäß konfiguriertem VPN ist äußerst sicher und stellt für alle WLAN-Umgebungen eine hervorragende Lösung dar.

4.1 FUNK-LAN-ZUGRIFF IM UNTERNEHMEN

Der häufigste Anwendungsbereich für ein Funk-LAN sind Unternehmensräume. Der Benutzer kann sich frei und unbeschwert in den Büroräumen bewegen, vom eigenen Schreibtisch zum Konferenzraum oder sogar zwischen zwei benachbarten Gebäuden, und dabei stets die Verbindung zum Netzwerk behalten. Abbildung 4 zeigt eine typische Unternehmenskonfiguration eines sicheren Funk-LANs.

Die Funk-LAN-Zugänge sind mit Hilfe eines VPN-Servers vom Unternehmensnetzwerk getrennt. Zwischen dem Funkterminal und dem VPN-Server wird ein VPN-Tunnel erstellt, der die vom und zum Intranet übermittelten Informationen schützt und nicht autorisierten Zugriff verhindert. Der Benutzer kann mit Hilfe von Kennwörtern, Einmalkennwörtern, z.B. Token, oder Zertifikaten authentifiziert werden.

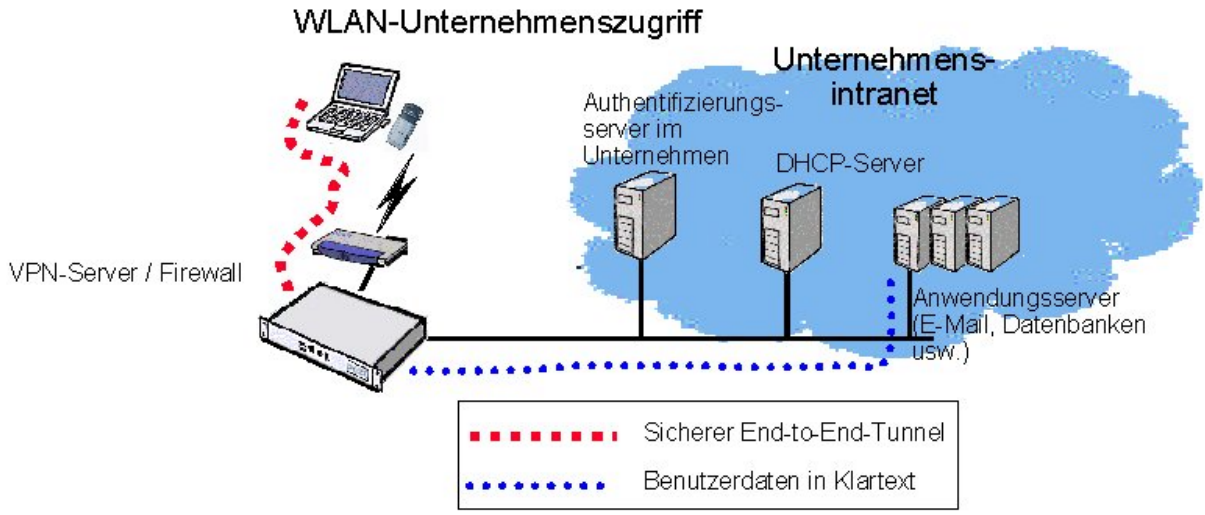

Abbildung 4: Ein sicheres Funk-LAN-Büro

4.2 FUNK-LAN-FERNZUGRIFF

Mobile Geschäftspersonen können Funk-LAN-Ausstattung auch unterwegs verwenden. Viele ISPs und Mobilfunkbetreiber haben öffentliche WLAN-Zugangsdienste an Flughäfen, in Hotels und an anderen öffentlichen Orten eingerichtet. Zudem haben einige Nutzer auch ein Funk-LAN zu Hause. Die Benutzer der Nokia D211 können von all diesen Orten aus eine sichere Funk-LAN-Fernverbindung zum Unternehmensnetzwerk unterhalten.

Die Architektur eines Fern-WLANs ähnelt jener des Unternehmens-WLANs. Der einzige bedeutende Unterschied besteht darin, dass im Unternehmen der Datenverkehr über ein privates Netzwerk direkt zum VPN-Server weitergeleitet wird. Im Fall einer öffentlichen Zugangszone oder eines privaten Funk-LANs werden die Daten über das öffentliche Internet weitergeleitet. Vom Standpunkt der Sicherheit erfordern beide den Gebrauch eines VPNs. Für Fernzugriff und Unternehmenszugriff kann dieselbe Terminalsicherheitskonfiguration genutzt werden. Abbildung 5 zeigt die Fernzugriffsarchitektur. Der Nokia D211-Benutzer wird zunächst durch das öffentliche Funk-LAN authentifiziert. Dann startet der Benutzer den VPN-Client, der automatisch einen sicheren Tunnel zum Unternehmensnetzwerk aufbaut.

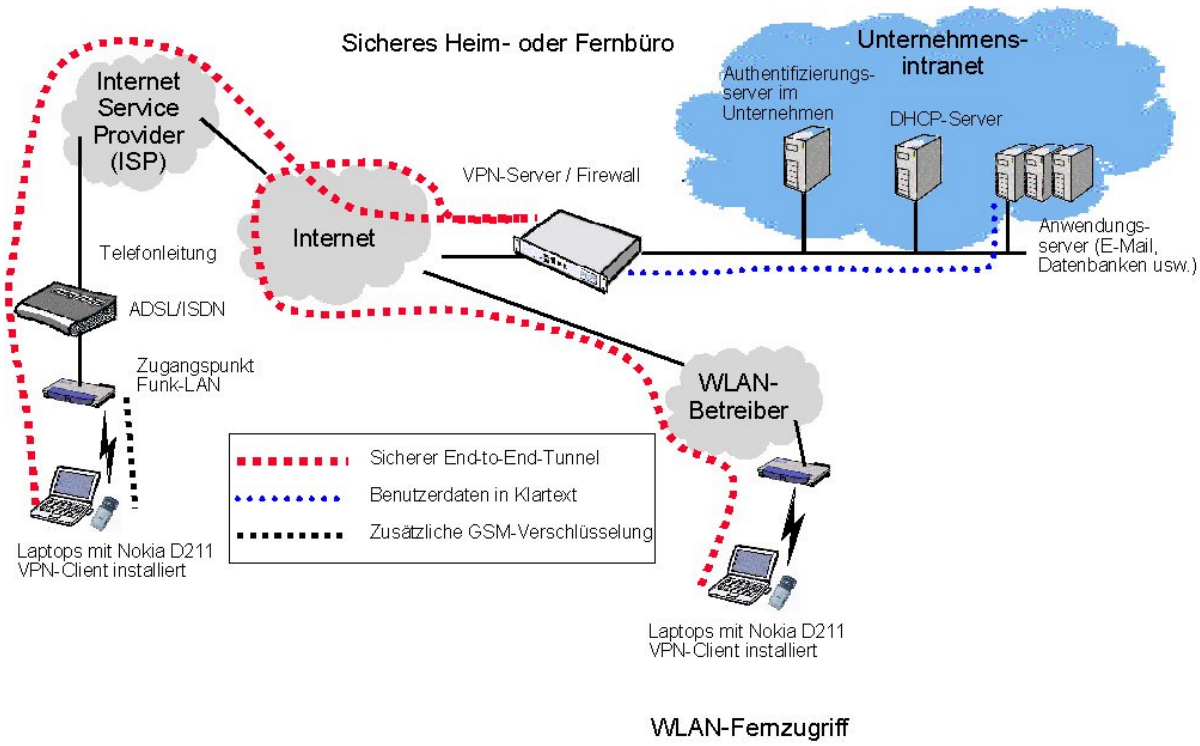

Abbildung 5: WLAN-Fernzugriff

5. ZUSAMMENFASSUNG – SICHERER UNTERNEHMESZUGRIFF MIT DER NOKIA D211

Die Nokia D211 ermöglicht dem Benutzer die Nutzung des konventionellen DFÜ-Netzwerks (Abbildung 1). In dieser Konfiguration ist der VPN-Client nicht erforderlich, sondern die Verbindung wird über die standardmäßigen DFÜ-Funktionen von Microsoft Windows aufgebaut.

Die vorgestellte Fernzugriffsarchitektur, zu sehen in Abbildung 6, setzt sich aus zwei Hauptbestandteilen zusammen: dem VPN-Server und dem VPN-Client. Der VPN-Server erweitert das Unternehmensnetzwerk um Internetzugang und bietet von allen alternativen Funknetzwerken aus einen sicheren Zugriff auf Ressourcen im Unternehmensnetzwerk: GPRS, HSCSD oder Funk-LAN. Ein und derselbe Server bietet Fernzugriffsdienste für alle Typen von Remote-Benutzern: Telearbeiter, Benutzer von GPRS-Roaming, Benutzer von öffentlichen Funk-LANs usw. Dadurch werden die Administrationskosten gesenkt, und die Netzwerkarchitektur wird weniger komplex. Normalerweise wird der VPN-Server von der IT-Abteilung eines Unternehmens verwaltet.

Die VPN-Clientsoftware wird auf dem PC des Benutzers installiert und setzt auf der Nokia D211-Software auf. Für GPRS und WLAN wird dieselbe Standardclientkonfiguration verwendet. Der Client baut automatisch einen sicheren Tunnel zum VPN-Server des Unternehmens auf. Zudem bietet er eventuell eine persönliche Firewall, die den PC vor

Angriffen schützt. Das Unternehmen kann den am besten geeigneten VPN-Client auswählen, da die Nokia D211 mit den führenden VPN-Clients kompatibel ist.

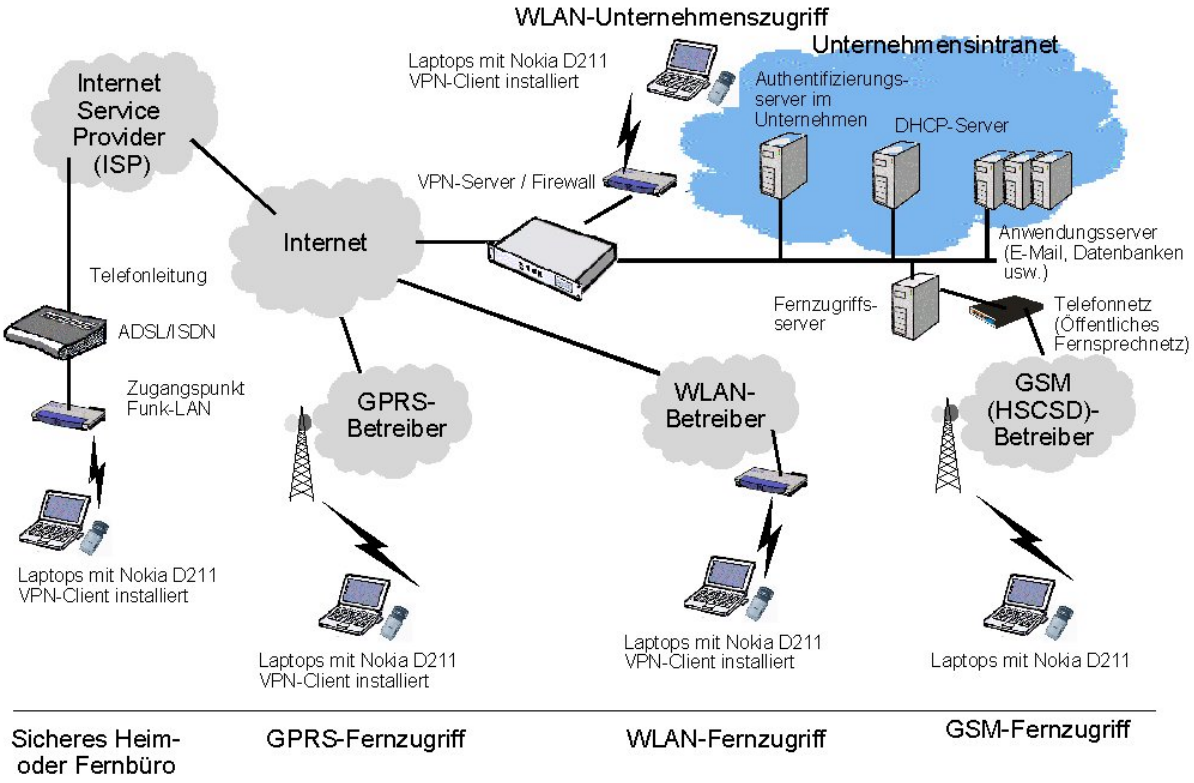

Abbildung 6: Zusammenfassung der sicheren Fernzugriffsarchitektur

VPN ist genau die richtige Methode für den Aufbau einer sicheren, privaten Kommunikationsinfrastruktur auf Basis des Internet. Es ergeben sich einige Vorteile, wenn Internetkonnektivität, GPRS und WLAN nach Möglichkeit immer verwendet werden:

- Der Benutzer muss keine Ferngespräche führen, um das Unternehmen direkt anzuwählen, sondern GPRS und Funk-LAN ermöglichen dem Benutzer die Verwendung der öffentlichen Internetverbindung.
- Die Berechnung basiert bei WLAN und GPRS gewöhnlich auf der übertragenen Datenmenge, nicht auf der Verbindungszeit. Daher können E-Mail und Surfen über diese Art von Verbindung erheblich kostengünstiger sein.
- Dank VPN können Unternehmen Modempools, teure Standleitungen und Fernzugriffsserver abschaffen.
- Weitere Einsparungen ergeben sich aus der Reduzierung der Betriebskosten in Bezug auf den Support von Remote-Benutzern.

Die Nokia D211 Multimodus-Funkkarte setzt einen neuen Maßstab für PC-Konnektivität, da sie sowohl DFÜ- als auch GPRS- und WLAN-Konnektivität in einem einzigen Gerät bietet.

Für das Produktdesign wurde der Sicherheitsaspekt berücksichtigt. Die Nokia D211 ist in den abgebildeten Referenzdesigns kompatibilitätsgeprüft mit Software führender VPN-Client-Hersteller und mit Microsofts eingebetteten Internetsicherheitslösungen (IPSEC). Ausführliche Informationen zum Thema Sicherheit finden Sie unter www.nokia.com.