von Rechtsanwalt **Max-Lion Keller**, LL.M. (IT-Recht)

Einsatz von WLAN bei Unternehmen; ein rechtlicher Erkundungsgang

So groß das technische Potenzial und der damit verbundene wirtschaftliche Nutzen des WLANs für Unternehmen auch sein mag, ist es doch, wie dieser Beitrag zeigt, unerlässlich, sich zumindest einmal im Groben mit der rechtlichen Seite der WLAN-Nutzung auseinandergesetzt zu haben. Denn in Zusammenhang mit der W-LAN-Nutzung stellen sich gerade für Unternehmen durchaus spannende rechtliche Fragen, etwa, ob es einer Lizenz für die firmeneigene WLAN-Nutzung bedarf oder ob datenschutzrechtliche Vorschriften zu beachten sind.

1. WLAN und der Access-Providing-Vertrag

Möchte ein Unternehmen seinen Angestellten die Anbindung an das World Wide Web mittels WLAN ermöglichen, ist es auf einen Dienstleister angewiesen, der in der Lage ist, einen entsprechenden Zugang ins Internet zu ermöglichen. Dies ist der so genannte Internet-Service Provider, kurz Provider. Er realisiert Internetzugänge mittels einer paketvermittelten Datenübertragung über seinen lokalen Einwahlknoten (sog. Point of Presence). Dieser ist wiederum mit einem Backbone-Netz verbunden ist. Der Vertrag mit dem Provider wird Access-Provider-Vertrag genant. Er wird oft als rahmenvertragsähnliches Dauerschuldverhältnis ausgestaltet und besteht vorwiegend aus werk-, miet- und dienstvertraglichen Elementen (sog. gemischttypologischer Vertrag).

Folgende wesentliche Vertragsinhalte sollte ein solcher Access-Provider-Vertrag typischerweise regeln:

- Leistungsumfang: Hier werden die vertraglichen Hauptpflichten geregelt, ggf. mit einer separaten Leistungsbeschreibung.
- Preise, Zahlungsbedingungen: Um Missverständnisse zu vermeiden, sollten die Vertragsparteien klare Preisregelungen bzw. Zahlbedingungen regeln.
- Vertragslaufzeit und Kündigung: Üblich sind hier Mindestvertragslaufzeiten. Es gilt eine ausgeglichene Balance zwischen der Planungssicherheit des Providers und einer zumutbaren Bindungsfrist des jeweiligen Unternehmens zu finden.
- Gewährleistung und Verzug: Hier hat man insbesondere zu beachten, dass entsprechende Klauseln der Kontrolle des AGB-Rechtes und der Telekommunikations-Kundenschutzverordnung (TKV) unterliegen.
- Vertraulichkeit, Datenschutz: Hier geht es um Regelungen zur Art der vertraulichen Informationen, die

Dauer der Vertraulichkeit, Weitergabe von sensiblen Informationen an Dritte etc.

2. WLAN - Gegenstand staatlicher Regulierung?

Bei der Nutzung von WLAN geht es um "Telekommunikation", da hierbei über Funkfrequenzen Daten mittels Telekommunikationsanlagen übermittelt werden. Dabei wird wohl jedem einsichtig sein, dass diese Form der Datenübermittlung der staatlichen Regulierung bzw. Steuerung unterliegt. Schließlich sind Frequenzen knappe Güter und es bedarf eines effektiven (hoheitlichen) "Frequenzmanagements", welches sicherstellt, dass die jeweiligen Funktechniken ausreichend gegen Störungen anderer Funkanwendungen geschützt sind. Dieses Frequenzmanagement ist in Deutschland in dem sog. Telekommunikationsgesetz ("TKG") abgebildet, welches die jeweiligen Frequenzbereiche den unterschiedlichsten Funkdiensten (z.B. Radio, TV, Handy) und anderen Anwendungen elektromagnetischer Wellen (z.B. Mirkowelle) zuweist. Für WLAN sind hierbei die Frequenzbereiche 2,4 GHz und 5 GHz vorgesehen.

Welche (greifbaren) Konsequenzen hat diese Erkenntnis aber nun für die firmeneigene Kommunikation über WLAN? Bedarf es zur Nutzung der WLAN-Frequenzbereiche der Abstimmung mit der deutschen Regulierungsbehörde, also der Bundesnetzagentur in Form von förmlichen Anträgen und Genehmigungen? Oder reicht möglicherweise bereits die bloße Anzeige des beabsichtigten WLAN-Betriebs aus?

Um es gleich vorwegzunehmen: Die firmeninterne Kommunikation über WLAN ist weder einer staatlichen Lizenz- noch einer Meldepflicht unterworfen:

- So wurde die noch vor wenigen Jahren bestehende Lizenzpflicht für bestimmte Arten von WLAN-Anwendungen im Zuge der europäischen Liberalisierung des telekommunikationsrechtlichen Lizenzrechtes mittlerweile komplett aus dem aktuellen TKG entfernt bzw. durch eine bloße "Meldepflicht" ersetzt.
- Aber selbst diese, in § 6 TKG normierte, Meldepflicht, spielt für reine Firmen-LANs keine Rolle, da § 6 TKG ausschließlich für gewerbliche Betreiber öffentlicher Telekommunikationsnetze gilt. Die bei Unternehmen eingesetzten kabellosen lokalen Netzwerke (WLAN) sind jedoch in aller Regel gerade nicht öffentlich, da hier nur geschlossenen Benutzergruppen, also den Angestellten, das Recht und die Möglichkeit eingeräumt wird, über das firmeneigene WLAN zu kommunizieren. Entsprechendes gilt natürlich auch für andere vergleichbare Benutzergruppen, wie etwa Krankenhäuser, Universitäten, Behördenstandorte etc. Zudem kann der unternehmenseigene Funkdienst auch nicht als gewerblich i.S.d. § 6 TKG verstanden werden, da das W-LAN weder mit Gewinnerzielungs- , noch mit Kostendeckungsabsicht. betrieben wird.

Fazit

Solange sich ein Firmen-LAN nicht gegen Entgelt Dritten öffnet, unterliegt das jeweilige Unternehmen keiner Meldepflicht i.S.d. des § 6 TKG.

3. Verpflichtungen datenschutzrechtlicher Art beim Einsatz von WLAN

Der Umfang der datenschutzrechtlichen Anforderungen betreffend der Nutzung von WLAN hängt ganz maßgeblich davon ab, ob dieses für die Öffentlichkeit oder nur für geschlossene Benutzerkreise bestimmt ist. Wie bereits ausgeführt, werden firmeneigene WLAN-Netze in aller Regel nur für geschlossene Benutzerkreise angeboten. Hierbei ist nun aus datenschutzrechtlicher Sicht zwischen zwei Varianten zu unterscheiden, aus denen sich wiederum unterschiedliche rechtliche Folgen ergeben können:

- Die Nutzung des firmeneigenen WLANs ist nur für betriebliche Zwecke erlaubt.
- Die Nutzung des firmeneigenen WLANs ist nur für private und betriebliche Zwecke erlaubt.

a. Nutzung für betriebliche Zwecke vorbehalten

Für den Fall, dass die Angestellten eines Unternehmens das firmeneigene WLAN ausschließlich für betriebliche Zwecke nutzen dürfen, ist das Unternehmen (als Betreiber des WLAN-Netzes) kein "Anbieter" im Sinne des Telekommunikations- oder Teledienstерechts. Schließlich stellt der Arbeitgeber seinen Arbeitnehmern lediglich ein weiteres Arbeitsmittel zur Verfügung. Beim Anbieter und Nutzer des WLANs handelt es sich damit rechtlich nicht um zwei verschiedene Rechtssubjekte. Diese "Personenidentität" hat nun für das Unternehmen die (sicherlich angenehme) rechtliche Konsequenz, dass es weder an die Vorschriften des TKG zum Fernmeldegeheimnis oder zum Datenschutz, noch an die datenschutzrechtlichen Vorschriften des Teledienstedatenschutzgesetzes ("TDDSG") gebunden ist. Das Unternehmen hat einzig und allein die jeweils einschlägigen landesrechtlichen Vorschriften für Personaldatenverarbeitung zu beachten.

b. Nutzung für betriebliche und private Zwecke gestattet

Wird dagegen den Angestellten erlaubt, das firmeneigene WLAN auch nachhaltig für private Zwecke zu nutzen, erbringt das jeweilige Unternehmen geschäftsmäßige Telekommunikationsdienste i. S. v. § 3 Nr. 10 TKG, da es in diesem Rahmen nicht auf eine irgendwie geartete Gewinnerzielungsabsicht ankommt. Eine "Personenidentität" ist nun nicht mehr annehmbar, vielmehr geht es nun um zwei verschiedene Rechtssubjekte, nämlich dem Arbeitgeber (Anbieter) und seinen Arbeitnehmer (Nutzer) ("sog. Anbieter-Nutzer-Verhältnis").

In datenschutzrechtlicher Hinsicht hat dies zur Folge, dass das betreffende Unternehmen sowohl das Fernmeldegeheimnis, als auch die datenschutzrechtlichen Vorschriften der §§ 88 ff. TKG und die Vorschriften des TDDSG zu beachten hat. Zwar enthält insoweit das TKG einige Erleichterungen für geschlossene Benutzergruppen. Diese sind jedoch für den Betrieb eines WLANs kaum von Bedeutung. In zweierlei Hinsicht sind jedoch betriebsinterne WLAN gegenüber denjenigen Anbieter, die Dienste für die Öffentlichkeit erbringen, privilegiert. So sind Anbieter betriebsinterner WLAN

- nicht verpflichtet, die erhöhten Anforderungen i.S.d. § 109 Abs. 2 und 3 TKG einzuhalten und
- nicht verpflichtet, auf eigene Kosten Vorkehrungen zur Überwachung der Kommunikation nach § 110 TKG zu treffen.

4. Wireless LAN - Strafbares Abhören ungesicherter Kommunikation

Ein für jedes Unternehmen besonders sensibles Thema stellt natürlich die Sicherheit der eigenen Datenströme dar, die es unter allen Umständen zu schützen gilt. Schließlich haben gerade Unternehmen ein ureigenes Interesse daran, Dritte nicht an Geschäftsinterna oder gar Betriebsgeheimnissen irgendeiner Art partizipieren zu lassen. Das WLAN ist jedoch bei einer Vielzahl von Unternehmen in technischer Hinsicht nur unzureichend geschützt und stellt eine sehr ernst zu nehmende Sicherheitslücke dar. Diese ist deswegen besonders gefährlich, da das sog. "war-driving" bereits seit Jahren eine Art Volkssport darstellt. Dabei versteht man unter dem Begriff "war-driving" das unerlaubte und in vielen Fällen auch unbemerkte Ausspähen fremder Daten, die über WLAN-Netze verarbeitet werden.

Vielen gilt diese Art der Datenspionage noch immer als eine Art Kavaliersdelikt. Dies ist ein gravierender Irrtum, da derjenige, der sich auf diese Art und Weise fremde Daten beschafft, sich strafrechtlich (vgl. nur § 202a StGB: Ausspähen von Daten) zu verantworten hat.. Dabei unterscheidet das Strafrecht übrigens nicht, ob die Bedeutung der Daten für Opfer und Täter wirtschaftlich erheblich sind oder nicht.

Insbesondere spielt auch keine Rolle, ob ein konkreter Vermögensschaden eintreten kann oder nicht. Entscheidend für eine strafrechtliche Sanktionierung ist nur, ob die Daten bei der Übertragung gegen unberechtigten Zugang gesichert sind. Damit möchte der Gesetzgeber insbesondere den Zugang zu den Originaldaten, d.h. den Inhalten sanktionieren. Folgerichtig ist das bloße Zugreifen auf verschlüsselte Daten wegen der fehlenden Möglichkeit, auf die Inhalte zugreifen zu können, nicht nach § 202a StGB strafbar: Erst eine Entschlüsselung dieser Daten würde die Strafbarkeit jedoch begründen.

Darüber hinaus können beim Hacken auch noch andere Straftatbestände verletzt werden, auf die im Rahmen dieses Artikels jedoch nur stichpunktartig eingegangen werden kann:

- § 44 Abs. 1 BDSG: Schützt alle Informationen über persönliche oder sachliche Verhältnisse, die man einer natürlichen Person zuordnen kann (Name, Alter, Beruf etc.).
- § 17 Abs. 2 Nr. 1 UWG: Diese Norm regelt die Betriebsspionage, wonach bestraft wird, wer sich zu Zwecken des Wettbewerbs, aus Eigennutz, zu Gunsten eines Dritten oder um das betroffene Unternehmen zu schädigen ein Geschäfts- oder Betriebsgeheimnis verschafft oder sichert - bloße Neugier als Motiv scheidet dabei jedoch aus.
- § 86 Satz 1 TKG: Enthält das Verbot des Abhörens von Nachrichten mit einer Funkanlage, wenn diese für die Funkanlage nicht bestimmt sind. Geschützt sind dabei jede Art von "Nachrichten", also etwa das gesprochene Wort, schriftliche Übermittlungen, Bilder, Musik etc..

Fazit

Es zeigt sich also, dass der Gesetzgeber das Ausspähen fremder Daten umfänglich sanktioniert hat und damit die Opfer entsprechender Angriffe keinesfalls schutzlos lässt. Vor diesem Hintergrund sollten Hacker ihre Meinung überdenken, dass über das Wireless LAN übertragene Daten stets gefahrlos abgegriffen werden könnten. Unabhängig von der Strafbarkeit des Datensausspähens ist aber jedem Nutzer von WLAN, insbesondere aber Unternehmen, dringend anzuraten, ihr Netz optimal zu schützen. Dies wird in der Regel nur durch vollständige Verschlüsselung aller Daten gelingen.

Autor:
RA Max-Lion Keller, LL.M. (IT-Recht)
Rechtsanwalt