Sicherheit im zweiten Anlauf

Immer mehr Banken wollen ihren Kunden in der Filiale einen freien WLAN-Zugang anbieten. Der Wegfall rechtlicher Hürden erleichtert das. Doch es gibt noch immer einiges zu beachten.

Der erste Versuch des deutschen Gesetzgebers, freies WLAN zu fördern, war eher gut gemeint als gut gemacht (siehe „Profil“ 2/2017, Seite 40). Denn mit der Novelle des Telemediengesetzes im Jahr 2016 wurden WLAN-Anbieter zwar von Schadensersatzansprüchen für den illegalen Download von Dateien durch Nutzer freigestellt. Für etwaige Abmahnkosten und Unterlassungsansprüche unterblieb jedoch eine ausdrückliche Freistellung. Letztlich blieb also alles beim Alten. WLAN-Anbieter mussten weiterhin im eigenen Interesse ihren Internetzugang per Passwort schützen.

Gesetzgeber bessert nach

Der Gesetzgeber hat nun nachgebessert und klargestellt: Bei einer rechtswidrigen Handlung eines Nutzers hat der Geschädigte gegenüber dem WLAN-Anbieter keinen Anspruch auf Schadensersatz, Beseitigung oder Unterlassung einer Rechtsverletzung.

Rechteinhaber geistigen Eigentums, also zum Beispiel Musikunternehmen, können allenfalls verlangen, dass ein Zugang für bestimmte Personen gesperrt wird. Dies ist aber auch nur dann möglich, wenn etwa das Musikunternehmen keine andere Möglichkeit hat, der Verletzung seines Rechts abzuhelfen. Selbst in diesem Fall besteht jedoch kein Anspruch gegen den WLAN-Anbieter auf Erstattung der vor- und außergerichtlichen Kosten für die Geltendmachung und Durchsetzung der WLAN-Sperre.

WLAN-Hotspots dürfen weiterhin durch ein Passwort geschützt werden. Damit ist jedoch die Entscheidung verbunden, ob etwa eine Bank WLAN nur ihren Kunden anbieten will – zum Beispiel, damit diese die mobilen Dienstleistungen des Instituts besser kennenlernen können – oder ob sie einen öffentlichen Internetzugang anbieten möchte. Da die Funkwellen nicht an Gebäudegrenzen Halt machen, kann ein rund um die Uhr frei zugängliches WLAN auch von Personen genutzt werden, die nichts mit der Bank zu tun haben. Ob diese im Umfeld des Bankgebäudes oder der SB-Geschäftsstelle willkommen sind, muss jedes Kreditinstitut für sich entscheiden.

Privatsphäre schützen

In jedem Fall sollten die bayerischen Volksbanken und Raiffeisenbanken – aber auch jede andere Genossenschaft – schon wegen der allgemeinen Sorgfaltspflichten sowie aus Imagegründen auf ein professionelles WLAN-Angebot Wert legen. Dazu sind einige Punkte zu beachten. So sollte überall dort, wo WLAN angeboten wird, auf eine ausreichende Sendestärke geachtet werden. Gegebenenfalls können dafür Repeater eingesetzt werden. Die Sendestärke sollte dennoch so eingestellt sein, dass außerhalb der Grundstücksgrenze der Bank keine Kommunikation möglich ist.

Darüber hinaus sollten die Vertraulichkeit und die Privatsphäre der einzelnen Nutzer beachtet werden. Deshalb sollte die Kommunikation der einzelnen im Netzwerk angemeldeten Geräte untereinander ausgeschlossen werden. So kann das Risiko, dass Kriminelle Daten abgreifen oder Schadsoftware in die verbundenen Geräte einschleusen, deutlich reduziert werden.

Zusätzlich sollte das Kreditinstitut Filterfunktionen für das WLAN nutzen. Damit kann sie zulässige („Whitelist“) oder unzulässige („Blacklist“) Internetseiten definieren. Wenn dies auch keinen zuverlässigen Schutz vor unerwünschtem Surf-Verhalten bietet, mag die Einrichtung einer Filterfunktion doch im Einzelfall helfen, Ärger zu vermeiden.

Es ist nicht zu empfehlen, das von den Kunden genutzte WLAN auch für die eigene geschäftliche Kommunikation einzusetzen. Die Systeme sollten strikt getrennt werden. Zudem sollte die IT der Bank regelmäßig auf ihre Sicherheit überprüft werden. Mit solchen Checks lassen sich das vorhandene Schutzniveau überprüfen und Verbesserungsmöglichkeiten aufzeigen. In diesem Zusammenhang weist der Bereich Bankenprüfung des GVB darauf hin, dass die WLAN-Infrastruktur der bayerischen Volksbanken und Raiffeisenbanken ein zentraler Bestandteil im Rahmen der IT-IKS-Schwerpunktprüfung 2017/2018 des Verbands sein wird.

In jedem Fall sollte neben dem IT- beziehungsweise Informationssicherheitsbeauftragten auch der Datenschutzbeauftragte der Bank in die Planung für ein Kunden-WLAN einbezogen werden, damit alle Datenschutzvorgaben eingehalten werden. *Oliver Schießer, Bereich Rechtsberatung/Thomas Goldbrunner, Prüfungsbereich Banken*