ITDSC UG
Data-Security-Consulting
www.itdsc.de

CHECKLISTE: Sicheres WLAN im Unternehmen

Frage	Erläuterungen	Kontrolle
Sind die Hardware, Firmware und Software der WLAN- Komponenten aktuell?	Denken Sie stets daran: Ein wichtiger Aspekt des Art. 32 DSGVO ist, dass eingesetzte Gerätschaften und Software dem Stand der Technik entsprechen. Veraltete Geräte mit veralteter Firmware, Betriebssystem oder Software sind generell ein erhebliches Risiko. Dabei sollten Sie nicht nur an den Router denken. Denken Sie auch an andere Komponenten wie Accesspoints, Verstärker oder Repeater. Ob etwa ein Router aktuell ist, lässt sich leicht im Internet recherchieren. Ebenso, welche Firmwareversion aktuell ist bzw. welche Softwareversion installiert sein sollte. Auch lässt sich im Internet leicht recherchieren, ob es generelle Probleme oder Sicherheitsrisiken mit einem Produkt oder Gerät gibt. Werfen Sie einfach die Suchmaschine an.	❑ Ja ❑ Nein
Ist der WLAN-Router sicher vor dem Zugriff Unbefugter untergebracht?	Der Router muss vor dem Zugriff Unbefugter geschützt sein. Idealerweise ist der Router in einem abschließbaren Raum untergebracht. Um das Risiko so gering wie möglich zu halten, sind Berechtigungen nur auf den unbedingt erforderlichen Personenkreis zu beschränken. Die Zugriffsregelung ist zu dokumentieren.	❑ Ja ❑ Nein
Sind Accesspoints vor Manipulationen sicher?	Das Netz wird über Accesspoints aufgebaut, meist als Antennen oder kleine Kästen an Decke bzw. Wand erkennbar. Diese sollten außer Griffreichweite fest verankert und ggf. angeschlossen oder nur mit Spezialwerkzeug zu öffnen sein.	❑ Ja ❑ Nein
Sind Standard- bzw. Werkseinstellungen bezüglich sicherheitsrelevanter Aspekte verändert worden?	Werden Geräte eingerichtet, sind werksseitig unter Umständen Sicherheitsfunktionen deaktiviert oder auf einem niedrigen Niveau. Auch Standardpasswörter können zum Problem werden. Suchen Sie gezielt danach, etwa in Betriebs- oder Installationsanleitungen des betreffenden Herstellers, oder recherchieren Sie im Internet.	❑ Ja ❑ Nein
Wird das WLAN vor Angriffen ausreichend geschützt?	Um zu verhindern, dass sich beispielsweise Hacker Zugang zum WLAN Ihres Unternehmens verschaffen, ist die Verschlüsselung des Netzwerks absoluter Standard. Dabei sollten Sie ein Auge auf das Verschlüsselungsverfahren haben. WPA ist veraltet und gilt als unsicher. Standard ist aktuell noch WPA2. Moderner und unter Sicherheitsaspekten besser wäre jedoch der Einsatz von WPA3.	❑ Ja ❑ Nein
Kommt eine Gerätefilterung zum Einsatz?	Im Einzelfall kann es sinnvoll sein, dass Restriktionen bezüglich berechtigter Geräte vergeben werden. So kann etwa über die MAC-Adresse gefiltert werden, welches Gerät sich am WLAN überhaupt anmelden kann.	❑ Ja ❑ Nein
Wird auf ein starkes WLAN- Passwort gesetzt?	Das WLAN ist mit einem starken Passwort zu schützen. Hier gilt das Übliche: je länger und komplexer das Passwort, desto besser. Raten Sie daher zu mindestens 20 Stellen. Groß- und Kleinbuchstaben sollten genauso enthalten sein wie Ziffern und Sonder- zeichen.	❑ Ja ❑ Nein

ITDSC UG
Data-Security-Consulting
www.itdsc.de

Wie werden Geräte am WLAN angemeldet?	Idealerweise gibt es für Nutzer bzw. Geräte individuelle Anmeldeinformationen. Das hat den Vorteil, dass die Zugangsdaten jedes einzelnen Nutzers zentral gesteuert wer- den und jederzeit aktiviert und deaktiviert werden können. Gibt es nur ein Passwort für die Anmeldung am WLAN, sollte dieses Passwort idealer- weise nur den Administratoren zur Verfügung stehen. Diese können Geräte einrichten bzw. anmelden. Ansonsten besteht das Risiko, dass früher oder später das Passwort in falsche Hände gerät.	❑ Ja ❑ Nein
Besteht ein Konzept für die Verwaltung verschiedener Nutzergruppen?	Sollen verschiedene Nutzergruppen (z. B. Mitarbeiter, Gäste) das WLAN verwenden, müssen die Berechtigungen entsprechend zugeschnitten werden. Mitarbeiter benöti- gen zum Arbeiten Zugriff auf unternehmensinterne Laufwerke und Dateien. Idealer- weise erhalten Gäste nur einen „Gastzugang“, der von vielen Routern standardmäßig unterstützt wird. Oder es gibt ein zweites WLAN für Gäste mit entsprechend einge- schränkten Berechtigungen.	❑ Ja ❑ Nein
Wie erkennt man Unregelmäßigkeiten?	Hinterfragen Sie, ob man überhaupt mitbekommt, dass Unbefugte sich am WLAN zu schaffen machen. Hier kann das Auswerten von Protokollen sinnvoll sein, etwa un- berechtigte Anmeldeversuche. Allerdings bringt das nur etwas, wenn das regelmäßig passiert und nicht nur einmal im Jahr.	❑ Ja ❑ Nein
Sind die Beschäftigten sensibilisiert?	Bei all den technischen Sicherheitsmaßnahmen darf man den Nutzer nicht vergessen. Das heißt, die Beschäftigten müssen Bescheid wissen, worauf es bei der Nutzung ankommt. So sollte etwa bekannt sein, in welchen Fällen eine VPN-Verschlüsselung einzusetzen ist, damit der Datenverkehr nicht von Unbefugten „mitgelesen“ werden kann.	❑ Ja ❑ Nein

Bitte sprechen Sie dazu mit Ihrem IT-Dienstleister.

Bemerkungen:

_____ _____

Datum Bearbeiter

Scannen Sie diese Dokumente ebenfalls und legen Sie diese im DSMS entsprechend ab.
Somit können Sie die Unterlagen immer wieder nutzen.

Bei Fragen zur Umsetzung kommen Sie gern auf mich zu.

Detlef Riese
Datenschutzbeauftragter