Sehr geehrte Damen und Herren,

der sichere und gefahrlose Umgang mit unseren Produkten hat oberste Priorität in unserem Unternehmen. Dies gilt sowohl in Bezug auf Personenschäden als auch für den Schutz privater Nutzerdaten.

Kürzlich wurden in einigen Medien Berichte veröffentlicht, die auf eine sogenannte Sicherheitslücke bei unserer Küchenmaschine mit WLAN-Funktion – KM 2017Wi – hinweisen. Diesen Meldungen liegt ein Bericht der Fachhochschule Oberösterreich zugrunde, der beschreibt, dass es Studenten in Zusammenarbeit mit Professoren gelungen sein soll das Gerät zu hacken, also die WLAN-Verbindung zu übernehmen. Die durch die Fachhochschule vorgenommenen Bewertungen über mögliche Manipulationen und daraus entstehenden Gefahren entsprechen jedoch nicht der Realität und suggerieren Gefährdungen, die aufgrund der Geräteausführung inkl. der Auslegung des WLAN-Netzes, nicht in dieser Art vorhanden sind.

Die öffentlichen Berichterstattungen, die sich daraus ergeben und entsprechend öffentlichkeitswirksam formuliert sind enthalten zudem teils unwahre Aussagen, die möglicherweise verunsichernd auf Nutzer der Küchenmaschine wirken können. Wir möchten Ihnen daher mit diesem Schreiben darlegen wie die WLAN-Verbindung ausgelegt ist, mit welchen physischen Sicherheitseinrichtungen das Gerät ausgestattet ist und warum wir weiterhin ohne Einschränkung von der Sicherheit unseres Gerätes überzeugt sind und keinerlei Gefahren für Sie als Nutzer des Gerätes sehen.

Da es aus unserer Sicht (wie auch durch zahlreiche diesbezügliche Meldungen bestätigt wird) keinen vollumfänglichen Schutz gegen kriminelle Hackerangriffe gibt, haben wir schon während der Entwicklungsphase des Gerätes den Fokus auf den größtmöglichen Schutz für den Nutzer gelegt und daher entschieden, dass für die Bedienung per App ausschließlich eine WLAN-Direktverbindung in Betracht kommt. Das Gerät ist also direkt mit Ihrem Mobilgerät (Smartphone/Tablet) verbunden und nicht mit dem Internet gekoppelt. Eine Verbindung ist daher nur in einem begrenzten Abstand (einige Meter) von Küchenmaschine und Mobilgerät möglich.

Ferner haben wir die WLAN-Funktion so gestaltet, dass sich nur ein Nutzer mit dem Gerät verbinden kann, die Funktion ausschließlich an der Küchenmaschine über einen Tastendruck aktiviert werden kann und sich bei jedem Ausschalten des Gerätes und bei jedem Wechsel in den Standby-Modus deaktiviert. Die Funktion kann nur per Tastendruck an der Küchenmaschine, nicht aber über das Mobilgerät (re-)aktiviert werden. Zur Aktivierung muss der Nutzer also das Gerät bedienen und daher in unmittelbarer Nähe sein.

Für einen Angriff auf das WLAN muss…

- der Nutzer/Besitzer des Gerätes die WLAN Funktion am Gerät aktiviert haben
- der Angreifer in physikalischer Nähe des Gerätes sein
- der Angreifer über die nötigen Kenntnisse verfügen
- der Angreifer über das für einen Angriff erforderliche Equipment/Ausrüstung verfügen

Schon das geringe Zeitfenster, das sich aus der Auslegung ergibt, sorgt für eine extrem geringe Wahrscheinlichkeit für eine Übernahme des WLANs. In Kombination mit den weiteren, für einen Angriff nötigen Bedingungen, die alle gleichzeitig erfüllt sein müssen, ist ein Angriff unter reellen Bedingungen praktisch nicht möglich.

Zudem ergibt sich für einen potentiellen Angreifer keinerlei Nutzen und damit keinerlei Motivation, da weder private Daten noch sonstige Informationen erfasst oder verarbeitet werden und aufgrund der fehlenden Internetverbindung auch kein Netzwerk gebildet werden kann. Das Gerät wurde daher im Rahmen einer umfangreichen Prüfung durch den TÜV Rheinland als „Protected Privacy IoT Product“ zertifiziert und hat in diesem Zuge das nachfolgende Qualitätssiegel erhalten.

Sollte es dennoch zu einer, aus unserer Sicht unter reellen Bedingungen nicht möglichen, Übernahme des WLAN kommen, so ist das Gerät nach den Vorgaben der Niederspannungsrichtlinie konzipiert und darüber hinaus mit einer GS-Zertifizierung versehen. Es ist daher mit einer Vielzahl an physikalischen Schutzmechanismen ausgestattet, die unabhängig von der WLAN-Funktion in jedem Fall greifen. Hierzu nachfolgend nur einige, wenige Beispiele

- Überhitzungsschutz – Schaltet das Gerät bei zu hoher Temperatur ab-
- Temperatursicherung – Schaltet die Heizfunktion bei einer Temperatur von 135°C ab
- Sicherheitsverriegelungen – Betrieb ohne Sicherheitsdeckel ist **nicht** möglich → Klingen/Messer sind während des Betriebes **nicht** berührbar
- Begrenzte maximale Drehzahl des Motors/Klingeneinsatzes

Nachdem wir über die Ergebnisse der Fachhochschule informiert wurden, haben wir umgehend den TÜV Rheinland mit einer entsprechenden Risikoanalyse beauftragt. Hierbei haben Spezialisten des Bereiches „Cyber Security“ in Zusammenarbeit mit den professionellen Prüfern aus dem Bereich Sicherheit für elektrische Geräte die Küchenmaschine in Verbindung mit der WLAN Funktion hinsichtlich der Aussagen der Fachhochschule und damit zusammenhängenden Gefahren umfangreich untersucht.

Im Ergebnis bescheinigt der TÜV Rheinland in dem in diesem Zuge erstellten Bericht, dass die Risiken basierend auf dem offenen WLAN im Rahmen der Analyse als „**extrem gering**“ einzustufen sind.

Wir hoffen, dass wir mit unseren Erklärungen dazu beitragen konnten, die Sicherheit der Küchenmaschine nochmals klar darzulegen und dass entgegen einiger Meldungen keinerlei Gefahren von der Nutzung des Gerätes ausgehen.

Aufgrund unserer vollen Überzeugung hinsichtlich der umfassenden Sicherheit des Gerätes, die auch durch den TÜV Rheinland nochmals bestätigt wurde, wünschen wir Ihnen weiterhin viel Spaß bei der Zubereitung Ihrer Gerichte mit der Küchenmaschine.

Ihr HUP-Team