DAS INTERNET DER DINGE

Big Brother kommt zu uns nach Hause

In beliebten Hollywood-Filmen rauben Ganoven mit raffinierten Methoden Spielcasinos aus. Kürzlich fand ein Gangster aber einen besonders originellen Weg, illegal in ein amerikanisches Casino einzudringen. Das Internet der Dinge machte es ihm möglich.

Der Ganove wählte den Weg in das Casino über das Aquarium des Hauses. Der Fischbehälter war mit dem Casinorechner vernetzt, um automatisch den pH-Wert stabil zu halten und die Fische zu füttern. Durch eine Sicherheitslücke gelangte der Hacker über das ungeschützte Interface des Aquariums in das gesamte Netzwerk und konnte noch etliche Datenpakete nach Finnland schicken, bevor der Einbruch entdeckt wurde.

SCHÖNE NEUE WELT?

Derart offene Einfallstore finden die Hacker bald in jedem Haushalt: Das Internet der Dinge macht es möglich. Videorekorder, Fernsehgeräte, Heizungssteuerungen, Überwachungskameras, Putzroboter, Kaffeemaschinen, Kühlschränke – die digitale Vernetzung im Heim 4.0 schreitet unaufhaltsam voran. Kürzlich untersagte die Bundesnetzagentur Verkauf und Nutzung der Spielzeugpuppe Cayla und Kinderuhren, die mit ferngesteuerten Abhörfunktionen ein unbemerktes Ausspionieren im Haus und in der Schule ermöglichten.

Besorgten Helikopter-Eltern wird im Onlinehandel die totale Überwachung ihrer Sprösslinge angeboten: Mit einem Kids-Tracker auf der Smartwatch können sie jederzeit den Standort ihrer Kinder auf 5 m genau orten. Sollte ihr Kind eine vorab definierte „sichere Zone“ überschreiten, erhalten sie sofort eine Warnmeldung und können sich per Direktanruf einschalten. Auch die Babybetreuung wird erheblich erleichtert. Suzy Snooze und Snoo fungieren als smartes Nachtlicht, Audio-Babymonitor und Schaukelrobotor. Mit gedimmtem Licht, zarten Klängen und leichtem Schaukeln wird das Kind schläfrig gemacht. Sanftes Regenplätschern oder Mutterleibsgeräusche schalten sich beim nächtlichen Weinen ein. Auf der App können die Eltern das Schlafverhalten des Babys ständig überwachen und sich notfalls per Lautsprecher beruhigend einschalten.

BIG BROTHER FÜR JEDERMANN

Einen erstaunlichen Boom erlebt gerade auch die smarte Zahnpflege. Während des Putzens erfasst die Genius 9000 per Positionserkennung, wie gründlich jeder Zahn geputzt wird. Durch Punktesammeln lässt Benjamin Brush die Familienmitglieder spielerisch miteinander konkurrieren. Oclean One liefert einen ausführlichen Report über die persönliche Performance durch Messung von Bewegung, Winkel und Druck beim Putzvorgang. Und die Zahnbürste Ara verbindet den Nutzer zur Ermittlung eines Scores mit der künstlichen Intelligenz, die einen wöchentlichen Bericht über Putzerfolge und -misserfolge erstellt.

Direkt aus dem Schneewittchen-Märchen scheint MirroCool zu stammen. Der Spiegel der Zukunft nutzt Facial-Gesture-Recognition und erkennt dadurch das Gesicht jedes einzelnen Nutzers. Er wird mit seinem Namen begrüßt, hat direkten Zugriff auf seine Daten und kann durch Zwinkern zwischen E-Mails, Wetterprognose und Kalender hin und her „klicken“. Die Hände bleiben dabei frei zum Zähneputzen oder Schminken. Auf Wunsch löst ein Lächeln ein Selfie mit der integrierten HD-Kamera aus. In der Nähe der Haustür kann MiroCool als Bewegungsmelder eingesetzt werden, der seine abwesenden Bewohner bei einem Einbruch alarmiert. Big Brother kommt zu uns nach Hause.

Manfred Kindler, KKC-Vorsitzender,
Kontakt: m.kindler@kkc.info

DAS INTERNET DER DINGE ...

... und seine dunkle Seite

Alle Apps für das Internet of Things (IoT) haben eines gemein: Sie sind über WLAN an externe Server angeschlossen und übermitteln permanent Daten, um per Data-Mining angeschlossene AI-Systeme mit Weltwissen zu versorgen. Damit sie in der realen Umgebung der Nutzer kommunizieren können, sammeln „persönliche Assistenten“ wie Alexa, Cortana, Siri und Google Home unentwegt persönliche Daten.
Die mangelhafte Absicherung der Zugänge hat in den letzten Jahren schon enorme Schäden angerichtet. Ein 29-jähriger Brite koppelte beispielsweise im November 2016 fast 600.000 IoT-Geräte mittels dem Botnet Mirai und legte bei einem Angriff 1,2 Millionen Kunden der Deutschen Telekom lahm. Ein Test ergab kürzlich, dass weltweit noch 34 Millionen vernetzte Geräte diese offene Schnittstelle aufweisen. Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) und Europol veranstalteten im Oktober 2017 ihre erste IoT-Sicherheitskonferenz.

Logo: KKC