Datensicherheit und -sparsamkeit

Newsletter Nr. 4/2018

Köln, 1. Oktober 2018

Ob Smartphone, Smartwatch, Smart TV oder Smart Home: Der Begriff „smart“ steht vor allem für eine intelligente Technik, die „mitdenkt“ und so den persönlichen Lebensalltag im Idealfall erleichtert. Immer wichtiger wird dabei der Aspekt der Datensicherheit. Denn mit jedem technischen Fortschritt steigt auch die Gefahr des Missbrauchs persönlicher Daten.

Ständige Begleiter und „Digitale Helferlein“

Beim Smartphone handelt es sich um ein leistungsfähiges Multitalent, das neben der reinen Kommunikation und Information unter anderem auch navigieren, dokumentieren und bezahlen kann, manchmal sogar als Schlüsselersatz fungiert. Wichtige Daten sind auf einem Gerät dauerhaft gespeichert (u.a. Zugangspasswörter, biometrische Werte, Standortdaten, Kontakte, Fotos und Dokumente).
Sprachassistenten unterstützen uns bei der Organisation des Alltags, managen Termine, schalten die Kaffeemaschine, das Radio oder den Fernseher ein und aus, wenn es erwünscht ist, sie passen Licht und Temperatur im Eigenheim an, servieren uns die neusten Meldungen und schaffen es immer mehr, uns sogar zum Lachen zu bringen. Sie sind immer erreichbar und damit „always on“, also im ständigen Datenaustausch mit dem Besitzer, den Geräteherstellern und den Software- sowie App-Programmierern. Aber weiß man, mit wem darüber hinaus auch noch? Das „Internet der Dinge“ (Internet of Things, IoT) wächst täglich und schnell. Daher gilt: Mit dem Fortschritt gehen, das eigene Verhalten überdenken und angleichen.
Straftäter nutzen die intelligente Technik ebenso selbstverständlich und innovativ für ihre kriminellen Handlungen. Beispielsweise verwenden sie aufmerksamkeitserregende Formulierungen im Betreff einer E-Mail oder einer Chat-App, die zum Öffnen der Nachricht animieren. Beim Öffnen werden Schadprogramme/Trojaner freigesetzt. Dadurch holen sich die Täter die erforderlichen sensiblen Daten in Kopie oder verschlüsseln sogar die Originale auf den Geräten und erpressen damit anschließend die Besitzer (sowohl Privatpersonen sowie ganze Unternehmen). Häufig wird die Gerätesoftware (Firmware/Betriebssystem), beispielsweise von Überwachungskameras, Babyphonen oder Kühlschränken angegriffen: In einem Fall wurde beispielsweise das Mirabotnetz (Vernetzung von gekarperten Computern) genutzt, um die Internetgiganten Amazon, Netflix und Twitter erheblich zu stören.

Die Polizei Köln rät:

1. Geräte auswählen, die von autorisierten Stellen geprüft und zertifiziert sind. Wichtiges Kriterium für Kaufentscheidung: Gerätesoftware erhält dauerhaft Aktualisierungen, sodass Straftäter es schwerer haben, die Geräte zu beherrschen.
2. Antivirenprogramme verbessern den Sicherheitsstatus, deshalb überall installieren, wo es möglich ist.

Das Kriminalkommissariat Kriminalprävention/Opferschutz der Polizei Köln informiert dazu kostenlos. Lassen Sie sich beraten.

Ihre Polizei Köln

Polizeipräsidium Köln - Kriminalkommissariat Kriminalprävention/Opferschutz
Walter-Pauli-Ring 2-6, 51103 Köln, Tel.: 0221 229-8655, E-Mail: kriminalpraevention.koeln@polizei.nrw.de
Stand: 09/2018 - KW