Information des DIN-Verbraucherrates

DIGITALE SICHERHEIT – Internet of Things

Das Dokument gibt einen Einblick in die immer weiter zunehmende Vernetzung von Geräten bis hin zum Internet der Dinge, auch Internet of Things (IoT) genannt. Es wird erläutert, welche Geräte dazu zählen und gibt einen kurzen Einblick in die Problemstellungen vernetzter Geräte.

Was ist das Internet of Things (IoT)?

„Internet of Things“ (kurz IoT) oder auch „Internet der Dinge“ steht für keine einzelne Technologie. Es ist vielmehr ein Sammelbegriff für die Vernetzung und Interaktion von Sensorik und intelligenten Geräten untereinander sowie mit dem Menschen.
Das Internet der Dinge umfasst Geräte, die über zusätzliche Funktionen zur Vernetzung *(siehe auch VR Information – digitale Sicherheit – vernetzte Produkte)* und zum Datenaustausch verfügen. Diese werden in der Regel drahtlos an Datennetze angeschlossen. Häufig können sie auf das Internet zugreifen und auch darüber erreicht werden. Im Zuge dessen werden Daten meist an eine Cloud gesendet und dort aufbereitet und zugänglich gemacht *(siehe auch VR Information – digitale Sicherheit – Cloud Computing)*. Dabei können die Daten auch als Grundlage für weitere Dienstleistungen dienen.

Welche Geräte betrifft das?

Die Anzahl an vernetzten Geräten steigt rasant. Dafür gibt es viele Gründe. Unter anderem wächst das Breitbandinternet und die Kosten für Sensorik, Speicher, Recheneinheiten und Kommunikationsmodule fallen stark. Dadurch werden immer mehr Geräte, bis hin zum untersten Preissegment, mit diesen Merkmalen ausgestattet. „Alles was mit einem Netzwerk verbunden werden kann, wird es auch“, umschreibt das Wirtschaftsmagazin Forbes den Einfluss von IoT. Das Marktforschungsinstitut Gartner errechnete, dass bis 2020 mehr als 26 Milliarden IoT-Geräte mit dem Internet verbunden sein werden.
Zu den vernetzten IoT-Geräten zählt mittlerweile fast alles: vom Auto über digitale Assistenten und das smart Home bis hin zu smartem Spielzeug und Wearables (kleine Computersysteme, die direkt am Körper getragen werden).
Verbraucher kommen daher immer häufiger, und durchaus auch ungewollt, mit IoT-Geräten in Kontakt.

Problemstellung vernetzter Geräte

Durch „intelligente“, d. h. vernetzte und mit Sensoren ausgestattete, Geräte entstehen neue Risiken auf verschiedenen Ebenen. Dazu gehören:

Hardware-Ebene

- hier interagiert das IoT-Gerät meist über Sensoren mit seiner Umgebung
- Signalarten können manipuliert werden, so dass Sensoren gestört werden und es zu Fehlfunktionen kommt

Netzwerkebene

- betrifft den Informationsaustausch zwischen Komponenten
- Angreifer können durch ungewollten Zugriff die verwendete Software dazu bringen, ungewollte Aktionen auszulösen

- unzureichende Sicherung des Back-End oder der verwendeten Cloudlösung führen zu Schwachstellen (z. B. veraltete Software), die Angreifer ausnutzen und für bösartige Aktionen missbrauchen können

Applikationsebene

- umfasst Schwachstellen in der Bedienung einer Webanwendung oder eines mobilen Geräts

Zusammenfassend kann gesagt werden, dass unzureichend geschützte IoT-Geräte ein Risiko für die Informationssicherheit und Privatsphäre von Verbrauchern darstellen. Sie sind ein beliebtes Ziel von Cyber-Angreifern. Kompromittierte Geräte können missbraucht werden, um an persönliche Daten der Besitzer zu gelangen oder um großflächige Cyber-Angriffe auf Infrastrukturen Dritter durchzuführen.

Welche Rolle spielt die Normung?

In der Normung werden viele Aspekte des Internet of Things bearbeitet. Hierzu zählen derzeit schwerpunktmäßig industrielle Anwendung sowie Anforderungen an einzelne Komponenten (u.a. Sensoren), Kommunikation sowie Interoperabilität.
Zunehmend werden jedoch auch direkt verbraucherrelevante Themen adressiert und entsprechende normative Dokumente erarbeitet. Hierzu zählen zum Beispiel die 2019 veröffentlichte DIN SPEC 27072 *„Informationstechnik - IoT-fähige Geräte – Mindestanforderungen zur Informationssicherheit“* sowie die Mitte 2020 erschienene horizontale Norm ETSI EN 303 645 *„Cyber Security for Consumer Internet of Things: Baseline Requirements“*. Horizontale Normen, mit ihren allgemein formulierten Anforderungen, bilden die Grundlage für präzise, auf das jeweilige Gerät bzw. die Anwendung zugeschnittene Anforderungen. Diese Anforderungen werden zukünftig immer mehr Einzug in Produktnormen finden (müssen).

Welche verbraucherrelevanten Aspekte sind in der Normung adressiert?

Die deutsche Spezifikation DIN SPEC 27072 aus dem Jahr 2019 enthält IT-Sicherheitsanforderungen und Empfehlungen für internetfähige Geräte im privaten oder kleingewerblichen Endkundenbereich wie z. B. IP-Kameras, Smart-TVs oder Smart Speaker. Die DIN SPEC 27072 beschränkt sich dabei auf Anforderungen an das jeweilige IoT-Gerät und lässt Anforderungen an das IoT-Ökosystem (zugehörige Dienstleistungen, Apps oder Desktop Software zum IoT-Gerät) außen vor.

Die Norm fordert u. a.

- sichere Update-Funktionalität;
- eine im Initialzustand nach Inbetriebnahme verpflichtende Authentisierung vor Zugriffen über eine IP-Schnittstelle und verbietet die Nutzung von Standardpassworten im Netzwerkbetrieb;
- verpflichtende Nutzung kryptographischer Verfahren nach dem Stand der Technik.

Das Dokument gibt Herstellern konkrete Anhaltspunkte für die Umsetzung von Security-by-Design und Security-by-Default. Diese Prinzipien sollten generell bei der Konzeption und Entwicklung von IT-Produkten eingehalten werden. Dabei wird der komplette Produktlebenszyklus inklusive Auslieferung, Inbetriebnahme, Individualisierung und Außerbetriebnahme berücksichtigt.

Die 2020 veröffentlichte Europäische Norm ETSI EN 303 645 baut unter anderem auf der zuvor beschriebenen DIN SPEC 27072 auf und geht in ihren Anforderungen darüber hinaus. Die ETSI EN 303 645 hat zudem einen breiteren Anwendungsbereich. Während die DIN SPEC 27072 IP-fähige an das Stromnetz angeschlossene Geräte adressiert, beschreibt

die ETSI EN Empfehlungen und Anforderungen an die sichere Entwicklung (Security by Design) von IoT-Geräten die von Verbrauchern genutzt werden.
In der Norm sind unter anderem die folgenden verbraucherrelevanten Themen in Bezug auf IoT-Geräte adressiert:

- voreingestellte Passwörter;
- Updateprozess und Berichte über Sicherheitslücken;
- Integrität der verwendeten Gerätesoftware;
- sichere Kommunikation;
- Minimierung der möglichen Angriffsflächen des Systems;
- Speicherung sensitiver Informationen;
- Sicherheit persönlicher Daten sowie Umgang mit persönlichen Daten (Erstellen und Löschen von Benutzerdaten);
- Validierung von Eingabedaten;
- Installation und Wartung.

Auf Basis der ETSI EN 303 645 wird an einer neuen Prüfnorm gearbeitet, in der festgelegt sein wird, wie die zuvor aufgelisteten Empfehlungen und Anforderungen strukturiert und umfassend getestet werden können.

Was muss bei der Normung von Produkten mit Vernetzung beachtet werden?

Die in der ETSI EN 303 645 sowie DIN SPEC 27072 enthaltenen verbraucherrelevanten Themen sind auch in anderen Normen für geräte- und produktspezifische Anforderungen relevant. Sofern ein Gerät in den Bereich „Internet der Dinge“ fällt, also über Sensoren verfügt und/oder vernetzt ist, sollten die genannten Themen berücksichtigt und die entsprechenden Anforderungen an das jeweilige Gerät angepasst werden. Als erster Schritt kann auch in einer Produktnorm auf die ETSI EN 303 645 bzw. die DIN SPEC 27072 normativ verwiesen werden, ohne direkte Anpassungen der Anforderungen in Hinblick auf das zu normende Gerät vorzunehmen.

Welche Lücken gibt es noch in der Normung?

Bei der DIN SPEC muss beachtet werden, dass sich – wie schon zuvor beschrieben – die Anforderungen auf das IoT-Gerät an sich beschränken und weitergehende Anforderungen an das IoT-Ökosystem nicht Teil der Spezifikation sind.

Die ETSI EN 303 645 ist ein weiterer Schritt in die richtige Richtung. Es sind viele verbraucherrelevante Aspekte adressiert. Anzumerken ist allerdings, dass viele Festlegungen nicht in Form normativer Anforderungen, sondern als Empfehlung formuliert sind. Hier muss bei der nächsten Überarbeitung nachgesteuert werden, damit mehr verbraucherrelevante Festlegungen als Anforderung formuliert sind.

Darüber hinaus müssen noch weitere relevante Festlegungen aufgenommen werden. Hierzu zählen u.a.:

- Aufnahme per Mikrophon oder Kamera darf nur nach bewusstem Befehl durch die Nutzerinnen und Nutzer erfolgen;
- aktive Aufnahme muss immer deutlich erkennbar sein;
- Bei von Kindern genutzten IoT-Geräten wie „smarten“ Spielzeugen ist sicherzustellen, dass die Datenschutzeinstellungen nur von den Eltern und nicht von den Kindern geändert werden können;
- Neben einer ausreichenden Sicherung der Daten auf dem IoT-Gerät müssen auch externe Server, auf denen Daten gespeichert oder verarbeitet werden, adäquat gegen Cyberangriffe und Datendiebstahl geschützt sein;
- Produkt-Updates sollten optional angeboten werden, falls sie nicht sicherheitsrelevant sind *(siehe auch VR Information – digitale Sicherheit – Updates)*;

- Bereitstellung maschinenauslesbare Datenschutzerklärungen würde die Vergleichbarkeit für die Verbraucherinnen und Verbraucher erhöhen;
- Die Anbieter von IoT-Geräten sollten verpflichtend kennzeichnen müssen, wenn sie algorithmische Systeme nutzen und über deren Funktionsweise aufklären.

Diese noch aufzunehmenden Festlegungen wurden der Studie des DIN-Verbraucherrates zu smartem Spielzeug entnommen.