INTERNET OF THINGS – WENN SICH DINGE VERSELBSTSTÄNDIGEN

Wieder schlägt ein neuer Ausdruck hohe Wellen: Internet of Things, kurz „IoT“. Diesmal ist die Veränderung so tief im Dickicht der Technik versteckt, dass die damit verbundene Revolution von der Öffentlichkeit kaum wahrgenommen wird. Ganz neue Objekte mit elektronischer Steuerung werden sich in Kürze selbstständig mit anderen vernetzen können. Das hat weitreichende Konsequenzen, die künftig durch eine neuartige Adressierung sogar noch verschärft werden.

Die Erfahrung lehrt, dass fundamentale Technologien in der Wahrnehmung scheinbar verschwinden. Sie verweben sich so tief mit dem täglichen Leben, dass sie selbst gar nicht mehr bemerkt werden. Das ist keine grundlegende Konsequenz der Technologie, sondern eine Folge der menschlichen Psychologie. Sobald Menschen etwas ausreichend kennen und immer wieder erleben, verschwindet es aus ihrem Bewusstsein. Jeder Autofahrer kennt dieses Phänomen, wenn Verkehrzeichen oder Plakatwerbung, an denen man täglich vorbeifährt, nicht mehr wahrgenommen werden.

Das Gleiche passiert gegenwärtig in der Informationstechnologie. So werden in viele neue Geräte immer kleinere, vernetzte und sich selbst organisierende winzige „Computerchen“ eingebaut. Sie sollen Menschen und ihre Arbeit unterstützen, ohne selbst abzulenken oder überhaupt aufzufallen. So werden die heutigen Rechner zunehmend durch winzige „intelligente Gegenstände“ ergänzt.

Für dieses Phänomen wurde der Begriff „Internet of Things“ geprägt. Damit bezeichnet man die Verknüpfung eindeutig identifizierbarer physischer Objekte (also „Things“) mit ihren elektronischen Repräsentationen und digitalen Nachrichten in einem weltweit immer dichter werdenden Datennetz. Diesmal sind es die Dinge selbst und nicht mehr die Menschen, die aktiv werden.

Das echte IoT ist also ein Netzwerk, in dem nicht nur die menschlichen Benutzer einzelne Gerätezustände abfragen und verwalten können, sondern in dem auch kleinste Geräte über standardisierte Kanäle direkt selbsttätig untereinander kommunizieren. Diese vernetzten Geräte werden so preiswert und leistungsfähig, dass sie überall Einzug halten und menschliche Intervention gezielt unterstützen oder gar ersetzen können.

Zauberwort Selbstvernetzung

Beispiele kennt man schon aus dem Fernsehen, wenn etwa „intelligente“ Heizungsregler und Steuerungssysteme beworben werden. Oder aus der Medizin, wo beispielsweise ganz neue Bewegungs- und Atemsensoren zur Alarmierung erster Vorzeichen eines plötzlichen Kindstodes zum Einsatz kommen. In Medizinerkreisen bescheinigt man IoT bereits ein großes Potenzial zur flexiblen Patientenüberwachung, zum Beispiel mittels aufklebbarer Temperatursensoren oder EKG-Monitoren auf der Haut. Und so funktioniert es: Das EKG-Pflaster sendet seine Daten an den Monitor, der Glukosesensor am Oberarm wird vom Computer abgefragt, die neue Infusionspumpe stimmt sich mit der Steuereinheit ab. Ähnliches gilt für die Medikationsplanung einer sensorgestützten Apothekenverwaltung oder deren Ausgabe auf Basis von Funketiketten. Durch Selbstvernetzung entstehen damit ganz neue Produkte oder Leistungen – scheinbar ganz von selbst und genau so, wie es sich die Benutzer wünschen.

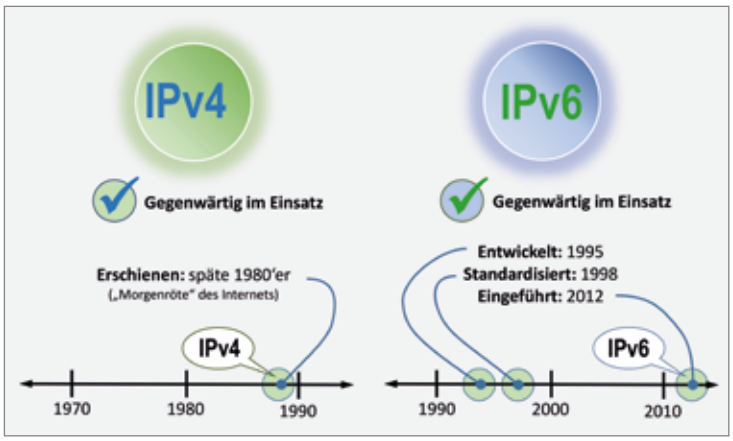
Möglich wird dies durch eine zweite, nicht minder gravierende Neuerung, die sich ganz still im Untergrund der heutigen Computertechnologie vollzieht. Zur Erklärung: Im Internet, wie in jedem Netz, muss jeder einzelne Knotenpunkt direkt adressierbar sein, damit Nachrichten von A nach B geleitet werden können. Das bisherige Internet mit seinem Kommunikationsprotokoll der vierten Generation (IPv4) kannte maximal 4,2 Milliarden Adressen. Das galt in den 1960er Jahren als unvorstellbar viel, ist aber heute längst bis auf die letzte Adresse ausgebucht. Als Hilfskrücke wird daher jede freiwerdende IPv4-Adresse sofort woanders weitergenutzt. Das geschieht flächende-

ckend, zum Beispiel jede Nacht, wenn dem eigenen sogenannten „Router“, wie der „Fritz!Box“ oder dem „SpeedPort“, vom Provider eine neue Adresse für die nächsten 24 Stunden zugewiesen wird.

Umstellung auf IPv6-Standard

Zur Auflösung dieses längst bekannten Flaschenhalses wurde schon 1995 das Internetprotokoll der sechsten Generation (IPv6) entwickelt und zwei Jahre später verabschiedet, das jetzt mehr als 340 Sextillionen (10^{36}) Adressen kennt. Rein theoretisch könnte man damit jedem Sandkorn auf der Erde mehrere Internetadressen zuweisen. Damit wird eine ganz neue Vergabestrategie für Adressen möglich. Mit IPv6 erhält jeder Nutzer nicht mehr nur eine der wertvollen Internetadressen für 24 Stunden, sondern dauerhaft ein ganzes sogenanntes „64er“-Netz, mit dem er eigenen Geräten in seinem Einflussbereich theoretisch mehr als 18 Trillionen (10^{18}) IP-Adressen zuordnen kann. Die Umstellung des Internets auf IPv6 erfolgt bereits seit 2012 und wird von den Internetanbietern angestoßen. Inzwischen unterstützen fast alle Anbieter und fast alle Endgeräte dieses neue weltweite Netz parallel zum alten IPv4.

Mit dem neuen Adressraum gibt es aber keine der bislang strukturell bedingten „schwarzen Flecken“ mehr im weltweiten Netz. Die bisher „hinter“ einer gemeinsamen IPv4-Adresse automatisch geschützten lokalen Netzwerkendgeräte stehen durch die neuen, individuellen IPv6-Adressen plötzlich im Rampenlicht der Öffentlichkeit – wenn man nicht selbst eingreift und den Zugriff von außen unterbindet. Die bisher unbeachteten Brandschutzmauern, die „Firewalls“, müssen deshalb neu aufgestellt und neu ausgerichtet werden. Wer IPv6 ohne Spezialvorkehrungen unbedacht aktiviert lässt, wenn die großen Provider damit beginnen, das neue Protokoll anzubieten, der riskiert, dass alle angeschlossenen Geräte und Daten aus dem Internet unter Beschuss geraten.



Quelle: nach TraceMyIP.org

Eigene wirksame Vorkehrungen treffen

Die gute Nachricht ist, dass die Netzanbieter die Umstellung von IPv4 auf IPv6 nicht ungefragt vornehmen – wenn alles richtig läuft. Die schlechte Nachricht ist, dass viele Hersteller von Routern die Option „IPv6 benutzen, wenn verfügbar“ automatisch aktiviert lassen. Dies stellt ein gefährliches Einfallstor dar. Im Endeffekt sollte IPv6 und dessen automatische Nutzung aus Sicherheitsgründen so lange ausgeschaltet bleiben, bis eine interne Umstellung gewünscht ist und eigene wirksame Vorkehrungen getroffen sind. Diese Überprüfung sollte heute und nicht erst morgen erfolgen. Sie sollte so schnell wie möglich durch einen Fachmann des Vertrauens vorgenommen werden.

Dass das Ganze kein Kindergeburtstag wird, zeigt die Suchmaschine „Shodan“. Sie wurde speziell dafür entwickelt, alle mit dem Internet verbundenen Geräte zu identifizieren. Es gibt also jetzt schon funktionierende Suchmaschinen oder Netzwerk- und Schwachstellenscanner wie „Nessus“, die IPV6 bis ins hinterste Eck ausleuchten und bei der Suche nach Schwachstellen helfen – im Guten wie im Schlechten. Das trifft natürlich auch die winzigen Knechte des IoT.

Verantwortung übernehmen

In der Gesamtschau vereinigen sich gegenwärtig zwei wichtige Veränderungen, deren praktische Tragweite für die Gesundheitsversorgung noch schwer zu beurteilen ist. Immer mehr kleinste Objekte senden beziehungsweise empfangen selbstständig Daten. Gleichzeitig wird die Zahl der verfügbaren Internetadressen in ungeahnte Dimensionen gehoben.

Der Endanwender wird aller Voraussicht nach von diesen Neuerungen nur wenig mitbekommen. Aber so bequem und nützlich IoT werden könnte, so sehr verlagert die IP-Umstellung die Aufgabe der Prüfung und des sinnvollen Einsatzes auf den verantwortlichen Anwender. Dieser sollte sich auskennen und vorbereiten.

Dr. med. Christoph Goetz,
Leiter Gesundheitstelematik (KVB)

Die Umstellung von IPv4 auf IPv6 sollte seitens der Netzanbieter gegenüber den Kunden kommuniziert werden. Wer auf Nummer Sicher gehen will, sollte IPv6 und dessen automatische Nutzung unbedingt so lange ausgeschaltet lassen, bis eigene Schutzvorkehrungen getroffen wurden.