Information des DIN-Verbraucherrates

DIGITALE SICHERHEIT – VERNETZTE PRODUKTE

In diesem Papier soll aufgezeigt werden, durch welche Eigenschaften sich vernetzte Produkte auszeichnen. Damit werden Hinweise gegeben, ob ein bestimmtes Produkt als ein vernetztes Produkt betrachtet werden kann. In der Gremienarbeit kann das für die Verbrauchervertretung wichtig werden, da bei vernetzten Produkten zusätzliche Anforderungen in die Normungsarbeit eingebracht werden müssen.

Verbindungen

Für die Verbindung von Produkten werden seit langem elektrische Leitungen verwendet. Eine elektrische Verbindung ist gegeben, wenn ein elektrisch leitender mechanischer Kontakt zwischen zwei Punkten vorhanden ist, über den die elektrischen Ladungsträger (Elektronen) in einem Leiter (zum Beispiel ein Kabel) fließen können. Mehrere solcher Verbindungen bilden einen Stromkreis beziehungsweise eine elektrische Schaltung.

Durch den analogen Rundfunk wurde es möglich, Information mit Hilfe von elektromagnetischen Wellen von einem Sender gleichzeitig und drahtlos an mehrere Empfänger zu senden. Heute werden solche Verbindungen häufig als Übertragungen mit digitalem Funk realisiert.

Kommunikation

Für die Kommunikation ist jedoch ein Informationsaustauch erforderlich, bei dem auf gegenseitige Anforderungen oder Fragen Antworten erfolgen. Dieser Informationsaustauch erfolgt zwischen den beteiligten Knoten in der Regel paarweise und bidirektional. Wenn zwei oder mehr Teilnehmer kommunizieren, entsteht ein Netzwerk. Damit Sender und Empfänger wirksam kommunizieren können, sind Übertragungsstandards und Spezifikationen – sogenannte Datenprotokolle – sinnvoll beziehungsweise erforderlich. In der Digitaltechnik werden für die Kommunikation viele verschiedene Datenprotokolle eingesetzt.

Wenn ein Kommunikationspartner permanent Video- oder Audiodaten an einen oder mehrere Empfänger sendet, wird dieser Vorgang „Live-Streaming“ genannt. Auf eine entsprechende individuelle Anfrage kann ein „On-Demand-Streaming“ erfolgen. Wenn ein Kommunikationspartner Daten sendet, die gleichzeitig von allen Empfängern eines Teilnetzes weiterverarbeitet werden können, wird vom „Broadcasting“ oder „Multicasting“ gesprochen.

Bei der digitalen Kommunikation ist es möglich, dass auch Daten übertragen werden, die Informationen über Merkmale anderer Daten enthalten (Metadaten) und die für die vom Benutzer gewünschte Funktion ggf. vollkommen überflüssig sind (zum Beispiel bei der Nutzerverfolgung durch Web-Tracking beziehungsweise durch „Web Analytics“).

Lokale Netzwerke

Persönliche Netzwerke (Personal Area Networks (PAN)) werden heutzutage sowohl kabelgebunden als auch kabellos über standardisierte digitale Schnittstellen aufgebaut. Zu den kabelgebundenen Schnittstellen gehören zum Beispiel das Ethernet (LAN = „Local Area Network“), USB- (Universal Serial Bus), DVI- (Digital Visual Interface) oder HDMI-Verbindungen (High Definition Multimedia Interface) oder TOSLINK (TOShiba-LINK mit Lichtwellenleiter). Diese sind immer unmittelbar sichtbar, weil für die Herstellung von Netzwerkverbindungen immer elektrische Kabelverbindungen erforderlich sind.

Zu den kabellosen Schnittstellen gehören digitale Technologien wie zum Beispiel WLAN (Wireless Local Area Network, im Englischen „Wi-Fi“), Bluetooth, Near Field Communication (NFC), Zigbee oder RFID (Radio Frequency Identification). Mit Infrarotlicht arbeiten die Standards RC-5 oder Consumer IR (Infra Red) für Fernbedienungen RC (Remote Control), die im Gegensatz zum Standard der Infrared Data Association (IrDA) oder dem Standard Infrared Mobile Communications (IrMC) jedoch in der Regel nur unidirektional verwendet werden.

Clouds / Internet

Immer häufiger werden Produkte heute in Datenwolken („in die Cloud“) eingebettet, indem sie wie häufig üblich zum Beispiel mit dem Internet verbunden werden. Auch hierfür werden standardisierte Schnittstellen eingesetzt, wie zum Beispiel ein heimischer Router, der per Kabel angeschlossen wird und über das Transmission Control Protocol / Internet Protocol (TCP/IP) arbeitet. Ferner sind Anbieter („Provider“) erforderlich, die die Infrastruktur der kabelgebundenen Netzwerke zur Verfügung stellen.

Die Anbindung in Datenwolken kann ebenfalls drahtlos erfolgen, und auch hier ist ein Dienstleister erforderlich, die für die entsprechenden Mobilfunkstandards die Infrastruktur der Netzwerke zur Verfügung stellen. Als Beispiele sind hier Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE = 4G) oder Fifth Generation (5G) zu nennen.

Software

Vernetzte Produkte zeichnen sich durch eine automatisierte Kommunikation aus. Diese kann zum Beispiel durch in die Produkte eingebaute Mikrocontroller (eingebettete Systeme) erfolgen. Die Kommunikation wird über die Software in den Geräten (Firmware) gesteuert und erfolgt über sogenannte „Ports“ (Tore), über die Datenströme ausgetauscht werden können. Diese sind potentielle Einfallstore („offene Ports“) für Cyber-Attacken. Schalten sich Angreifer zwischen das Gerät und die Cloud, kann ein unverschlüsselter Datenstrom von diesen mitgelesen und ausgewertet werden.

Auch Benutzer können über Software in die Kommunikation von vernetzten Produkten einbezogen werden, indem beispielsweise Vorgaben gemacht werden sollen, wann welche Information ausgetauscht werden soll, oder indem es eine aktive Beteiligung an der Kommunikation gibt. Die Einbeziehung von Benutzern erfolgt

- über Desktop-Anwendungen, die auf persönlichen Computern (PC) installiert werden,
- über mobile Apps, die in App-Stores verfügbar sind und auf mobilen Endgeräten wie Tablet-PCs oder Smartphones installiert werden, oder
- über Web-Anwendungen. Hier kann unterschieden werden,
    - ob die Software auf einem im kommunizierenden Gerät integrierten Web-Server abläuft und eine entsprechende, über einen Web-Browser aufruf- und anzeigbare Benutzerschnittstelle zur Verfügung stellt oder
    - ob die Software durch den Aufruf einer speziellen Web-Adresse automatisch heruntergeladen wird und somit direkt in Web-Browsern lauffähig ist (wie zum Beispiel Extensible Application Markup Language (XAML), Google Native Client oder WebAssembly).

Software kommuniziert mit anderen Programmen und Geräten über sogenannte „Doors“ (Türen). Diese sind potentielle „Backdoors“ (Hintertüren), die geheime, nur den Angreifern bekannte Möglichkeiten bieten, mit der Software zu kommunizieren und sie zu ändern. Auch können hierüber die Daten beispielweise mit Schadprogrammen wie Viren und Trojanern angegriffen oder ausspioniert werden.

Persönliche vernetzte Produkte

Zu den persönlichen vernetzten Produkten gehören zum Beispiel Smartwatches oder intelligente Zahnbürsten, die in der Nähe der betreffenden Personen benutzt und eingesetzt werden. Diese Produkte verbinden sich häufig mit Hilfe einer mobilen App im persönlichen Smartphone über einen Router oder über einen Mobilfunkanbieter mit dem Internet. Es ist wichtig festzuhalten, dass viele solcher Anwendungen auch ohne eine permanente Verbindung in eine Cloud oder ins Internet funktionieren können.

Heimische vernetzte Produkte

Zu den heimischen vernetzten Produkten gehören zum Beispiel intelligente Leuchtmittel, Heizungsthermostate oder Bewässerungsanlagen. Diese Geräte können permanent, temporär oder optional direkt untereinander und über einen Router mit dem Internet verbunden sein. Eine Smart-Home-Zentrale oder ein zentraler „Hub“ können hierbei über sternförmig angeordnete Netzknoten zwischengeschaltet werden. Sogenannte „Gateways“ können zwischen verschiedenen standardisierten Datenwelten vermitteln.

Permanent vernetzte Produkte

Bei Produkten, die regelmäßig oder überall mit dem Internet verbunden sein können („Ubiquitous computing“), wird auch von einem sogenannten Cloud Connected Device gesprochen. Stationär kann dies ein Smart Home oder ein Smart Office sein, mobil kann dies ein Smartphone oder ein selbstfahrendes Auto sein.

In einer vernetzten digitalen Welt können alle persönlichen, heimischen und mit dem Internet verbundenen Geräte miteinander kommunizieren.

Datensparsamkeit und Datenschutz

Viele Anbieter werben damit, dass die Daten von vernetzten Geräten in einer Cloud automatisch gesichert und effizienter verarbeitet werden können als auf lokalen Systemen. Da dies keineswegs zwingend zutreffen muss, gilt es hierbei immer abzuwägen, inwieweit der Schutz der Privatsphäre dadurch betroffen sein kann oder gar eingeschränkt ist. Ferner sollte immer geprüft werden, ob es datensparsame Lösungen gibt, die nur die tatsächlich erforderlichen Daten übertragen oder diese zumindest nicht dauerhaft speichern beziehungsweise an Dritte weiterleiten.

Oft sind ohne Einschränkung der Funktionalität sogar Lösungen möglich, bei denen gar keine Daten in die Cloud (ins Internet) übertragen werden müssen. Dennoch werden insbesondere durch mobile Apps und Web-Tracker viele Geräte und Anwendungen in einer Weise vernetzt, bei denen vielfältige Daten in großer Menge weltweit an zahlreiche Adressaten versendet werden, ohne dass dies einen positiven Einfluss auf die Funktionalität hat.

DIN-Verbraucherrat, Juni 2019

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages