POLIZEI
Nordrhein-Westfalen
Dortmund

Internet of Things

Quelle: adobe stocks (Polizei NRW)

Das „Internet der Dinge“

POLIZEI
Nordrhein-Westfalen
Dortmund

Der Begriff „Internet der Dinge“ oder auch „Internet of Things“ (IoT) steht für eine vernetzte Welt aus smarten Geräten, Sensoren und weiteren Technologien. Das Internet der Dinge ist ein Sammelbegriff für Technologien der globalen Infrastruktur der Informationsgesellschaften, wodurch physische und virtuelle Gegenstände miteinander vernetzt werden und mittels Informations- und Kommunikations-techniken zusammenarbeiten.

IoT-Geräte sind also lokal oder über das Internet mit anderen Geräten vernetzt. Dadurch wird eine Interaktion zwischen Mensch und den vernetzten Systemen, sowie zwischen diesen selbst ermöglicht.

So können wir beispielsweise von überall aus unsere Heizung zu Hause steuern, dass Licht einschalten oder viele weitere Vorgänge automatisieren. Häufig sendet das Gerät dabei Informationen an eine Cloud. Dort werden die Daten aufbereitet, zugänglich gemacht oder dienen als Grundlage für weitere Dienstleistungen.

Quelle: adobe stock (Polizei NRW)

Smarthome

POLIZEI Nordrhein-Westfalen Dortmund

Einsatzgebiete IoT
Beispiele für IoT-Geräte und ihre Einsatzgebiete sind Smarthome, Smart Toys, Wearables, digitale Assistenten, Smart-TVs, sowie die Industrie 4.0 und der Bereich Smart City.

Das **Smarthome** umfasst dabei alle Geräte, deren Einsatzgebiet sich in Ihrem Wohnraum befindet. Viele der sich darin befindlichen IoT-Geräte sind mit dem Internet verbunden und erlauben so die Kommunikation von Mensch zu Maschine oder auch Maschine zu Maschine. Hierzu zählt die sogenannte Hausautomatisierungstechnik, bei der zum Beispiel Fenster, Rollläden oder Türen gesteuert werden können, sowie auch weitere Haushaltsgeräte wie Kühlschränke, Smart-TVs, Kameras, digitale Sprachassistenten oder Unterhaltungselektronik. Diese Systeme lassen sich je nach Konfiguration von überall aus steuern und erlauben so eine permanente und komfortable Kontrolle über die eingesetzte IoT-Infrastruktur. Der Einsatz von IoT kann hier einerseits helfen, Kosten und Zeit zu sparen, birgt aber andererseits auch dieselben Risiken/Gefahren wie andere internetfähige Geräte.

Für einen sicheren Einstieg ins Smarthome sollten Sie folgende Hinweise beachten:

- Ihr Router, als zentraler Zugangspunkt zum Internet, sollte eine integrierte Firewall besitzen
- Voreingestelltes Routerpasswort durch ein eigenes, starkes Passwort schützen
- Firmware Updates regelmäßig einspielen
- Software- und Sicherheitsupdates für alle Geräte und Applikationen einspielen und aktuell halten
- Verwenden Sie keine Standardpasswörter
- Keine bereits zuvor benutzen Passwörter wiederverwenden
- Achten Sie auf eine verschlüsselte Kommunikation der Endgeräte
- Verwenden Sie ein virtuelles privates Netzwerk (VPN)
- Richten Sie ein separates Heimnetzwerk ein (Netzwerksegmentierung/Gäste-WLAN)
- Achten Sie auf physikalische Sicherheit (USB- oder LAN-Ports sollten nicht frei zugänglich sein)

Smart Toys

Smart Toys werden auch bei uns immer beliebter und so erhalten die „intelligenten Spielzeuge“ Einzug in die Kinderzimmer. Dabei zeichnen sich smarte Spielzeuge dadurch aus, dass sie lernfähig sind, ihre Umgebung erkunden können und mit ihrer Umwelt interagieren. Zu unterscheiden sind Spielzeuge, die sich mit dem Internet oder anderen Geräten verbinden können, und denen, die offline betrieben werden. Smart Toys können dabei als interaktives Spielzeug Kindern Hilfestellungen bei Lernprozessen bieten, sowie Spaß am Lernen fördern. So eröffnen smarte Spielzeuge ein großes Potential an neuen Möglichkeiten, Wissen spielerisch zu vermitteln und gleichzeitig, durch Vernetzung Zugriff auf die große Wissensdatenbank Internet zu erlangen.

Doch auch Smart Toys sollten kritisch hinterfragt werden. So können intelligente Spielzeuge nicht nur Wissen fördern, sondern auch eine große Gefahr darstellen, beispielsweise durch Ausspähen des privaten Lebensraumes, durch abgegriffene GEO-Informationen oder Gesprächsaufzeichnungen.

Smart Toys sollten daher sicher und verantwortungsbewusst unter Beachtung folgender Maßnahmen verwendet werden:

- Wenn das Spielzeug keinen Internetzugang benötigt, nutzen Sie es nur offline; andernfalls verwenden Sie nur ein passwortgeschütztes WLAN
- Wird das Spielzeug in Verwendung mit einer App genutzt, achten Sie auf die freigegebenen Rechte für das Smart Toy; z.B. Zugriff auf Kontaktdaten
- Inbetriebnahme in vertrauenswürdiger Umgebung
- Updates und Aktualisierungen vornehmen
- Voreingestellte PINs/Passwörter durch neue, starke Passwörter ersetzen
- Schnittstellen, z.B. zum Smartphone nur bei Verwendung aktivieren; danach deaktivieren
- Zugriffsschutz für den Verlustfall einrichten
- Bereits vor dem Kauf prüfen, ob Verschlüsselungsmechanismen zum Schutz der eigenen Daten existieren

Wearables

Wearables (Tragbar) existieren in verschiedenen Arten und Formen und sind kleine Computer in Form einer Hardwarekomponente, wie zum Beispiel Fitness-, Activity-Tracker oder Smartwatches und enthalten eine Vielzahl an Sensoren. So können sie beispielsweise Anrufe entgegennehmen, die Herzfrequenz und den Blutdruck messen, den Schlaf- und Kalorienverbrauch berechnen und Termine anzeigen und verwalten.
Darüber hinaus gibt es noch viele weitere Arten von Wearables wie smarte Kopfhörer mit Übersetzungsfunktion, smarte Kleidung zur Überwachung der Körperwerte oder Datenbrillen mit digitaler und virtueller Sichtfeldanreicherung im Bereich der Augmented Reality.
Diese Unterstützungsfunktionen tragen je nach Bedarf zur Performanceverbesserung bei und geben Feedback um individuelle Ziele leichter zu erreichen.

Durch die Tatsache, dass Wearables immer kleiner werden und eine immer größere Anzahl an Funktionen und Möglichkeiten zur Verfügung stellen, steigen auch hier die Risiken bei der Verwendung von Wearables, da persönliche Daten gespeichert und ausgewertet werden (z.B. Standortdaten, Gesundheitsdaten). Potentielle Käufer sollten also auch bei Wearables viel Wert auf IT-Sicherheit legen, um sich vor Cyberkriminellen, Identitätsdiebstahl und potentiellen Sicherheitslücken zu schützen. Bitte beachten Sie hierzu folgende Hinweise:

- Machen Sie sich mit der Funktionsweise ihres Wearables vertraut; Wie funktioniert es? Welche Daten werden erzeugt und wohin abgespeichert?
- Sicherheitseinstellungen prüfen und Updates einspielen
- Zugriffsrechte auf Wearable und dem damit verbundenen Gerät (z.B. Smartphone) einstellen
- Starke Passwörter oder PINs verwenden
- Erstkopplung von Wearables in vertrauenswürdiger Umgebung
- Eindeutige Identifizierung des Wearable muss möglich sein
- Daten sollten mit einer Transport- und Speicherverschlüsselung geschützt sein

Digitale Assistenten

Digitale Assistenten sind Geräte, welche uns im Alltag unterstützen sollen, zum Beispiel mit Hilfe von Erinnerungen, digitalen Einkaufslisten, Verwaltung von Terminen oder zur Steuerung anderer Smart Home-Systeme.
Viele Assistenten können per Sprachsteuerung verwendet werden, wie beispielsweise Alexa, Siri oder Google Assistent.
Bei der Verwendung digitaler Assistenten sollte jedem bewusst sein, dass hier private Informationen generiert und in die Cloud des jeweiligen Dienste Anbieters gesendet werden.
Die Risiken liegen hier bei unverschlüsselter Kommunikation, bei ungesicherten Servern oder beim verantwortungslosen Umgang mit personalisierten Nutzerinformationen.

Bei der Benutzung digitaler Assistenten sollten folgende Maßnahmen beachtet werden:

- Machen Sie sich mit dem Gerät und den Datenschutzeinstellungen vertraut; Datenschutzeinstellungen anpassen; die meisten Geräte sind standardmäßig auf volle Informationsweitergabe eingestellt
- Verwenden Sie starke Passwörter für kritische Sprachbefehle und Bestellungen
- Deaktivierung digitaler Assistenten bei Abwesenheit; bei nicht Nutzung
- Richten Sie ein separates Heimnetzwerk ein (Netzwerksegmentierung / Gäste-WLAN)
- Achten Sie auf eine geeignete Platzierung der Geräte in ihrem Umfeld (z.B. nicht am Fenster)
- Beschränken sie notwendige Schnittstellen zu anderen Geräten auf das Notwendigste
- Prüfen sie die gespeicherten Daten in ihrem Account; die Speicherung kann bei einigen Geräten deaktiviert werden

Smart-TV

Internetfähige **Smart-TV**-Geräte erlauben das Streamen von Filmen aus Online-Videotheken sowie das surfen im Internet, Unterstützung von Sprachsteuerung und Hybrid Broadcast Broadband TV (HbbTV), wobei Webinhalte des jeweiligen Senders in das Programm integriert werden. Viele Hersteller bieten ihren Kunden auch einen interaktiven Applikations-Store an, bei dem Inhalte kostenlos oder gegen Gebühr erworben werden können. Mittlerweile verfügen einige Smart-TVs schon über integrierte Webcams mit Mikrofon und erlauben so die Kommunikation über das Endgerät.

Mit diesen Möglichkeiten steigen auch hier die Risiken für den Nutzer von Smart-TVs. Potentielle Sicherheitslücken durch fehlende Softwareupdates oder Schwachstellen im System können zu einem ausspähen oder infizieren mit Schadsoftware führen. Ist ein Smart-TV erst einmal mit Malware infiziert, können Cyberkriminelle großen Schaden anrichten, zum Beispiel durch stehlen der digitalen Identität des Nutzers oder dem Einbinden des TVs in ein Botnetz mit dem Zweck, weitere Straftaten zu begehen.

<u>Allgemeine Sicherheitsempfehlungen bei Smart-TV:</u>

- Beachten Sie vor dem Kauf die notwendigen Leistungsmerkmale und Hardwareanforderungen
- Bereitstellung von Betriebssoftwareupdates und Updates im App-Store von Seiten des Herstellers/ Anbieters prüfen
- Applikationen und Herausgeber auf Vertrauenswürdigkeit prüfen
- Prüfen Sie die Verschlüsselung der zu übertragenen Daten
- Sicherheits- und Datenschutzeinstellungen des Smart-TV prüfen & anpassen (Webcam, Mikrofon)
- Zugriffsschutz des TVs prüfen (Passwort/PIN)
- Verwenden Sie keine kritischen Anwendungen wie Online-Banking über den Smart-TV
- Deaktivieren Sie Dienste, die nicht standardmäßig verwendet werden
- Bei der Entsorgung alter Geräte, müssen unbedingt alle Nutzerkonten, Passwörter und WLAN-Freigaben gelöscht werden

Industrie 4.0 & Smart City

Der Kerngedanke von **Industrie 4.0** besteht in der intelligenten Vernetzung von Menschen, Maschinen, Produkten, Logistik und ihren Abläufen mittels der Informations- und Kommunikationstechnik.
Durch das „Internet der Dinge“ können einzelne Produktionsschritte durch digitale Vernetzung und Kommunikation in Echtzeit optimal geplant und aufeinander abgestimmt werden, um so Effizienz und Produktivität weiter zu steigern.
Die Kommunikation von Mensch zu Maschine aber auch Maschine zu Maschine verläuft durchweg digital und bietet auch hier viele Angriffspunkte für Cyberkriminelle. Aus diesem Grund müssen hier ebenfalls grundlegende Sicherheitsvorkehrungen und Mechanismen geschaffen und beachtet werden, um Kommunikationswege und Infrastrukturen zu sichern.

Der Sammelbegriff **Smart City** steht für gesamtheitliche Entwicklungskonzepte, um Städte effizienter, sicherer, technologisch fortschrittlicher und sozial inklusiver zu gestalten. Hierzu gehören Beleuchtung, Verkehrsinfrastruktur, Energie- und Wasserversorgung, sowie städtisches Datenmanagement. Und auch diese vernetzten, zum Teil kritischen Strukturen, gilt es zu schützen.

Wo gibt es Hilfe?

POLIZEI Nordrhein-Westfalen Dortmund

Wenn Sie Opfer von Cybercrime geworden sind, stehen Ihnen die gleichen umfangreichen Hilfs- und Unterstützungsangebote zur Verfügung, wie den Opfern von Straftaten in der realen Welt.

Bei akuter Bedrohung, wählen Sie 110! Die Polizei wird alles Erforderliche tun, um Sie zu schützen.

- Zeigen Sie die Straftat bei der Polizei an (Strafanzeige ist bei jeder Polizeidienststelle möglich)
- Existierendes Datenmaterial, wie z. B. E-Mails, digitale Fotos oder Videos sind wichtige Beweismittel, die Sie bis zum ersten Kontakt mit der Polizei bestenfalls komplett unverändert lassen.
- Bringen Sie das gesicherte Beweismaterial am besten gleich zur Anzeigenerstattung mit. Das ist wichtig für die weiteren Ermittlungen, um den Verlust von Spuren im Netz zu vermeiden.