Eine Kaffeemaschine, die über WLAN und Sprachsteuerung bedient werden kann, könnte Gespräche aufzeichnen.

Kaffeemaschine hört mit

Die Vernetzung „intelligenter" Geräte bringt neben Vorteilen auch eine Reihe von Gefahren mit sich, die von Lauschangriffen bis Sabotage reichen.

Digitale Assistenten, verbunden mit dem Internet, erzeugen zugleich Begeisterung und Angst. Unweigerlich denken viele an HAL aus dem Film „2001, Odyssee im Weltraum" von Stanley Kubrick oder an „Terminator" mit Arnold Schwarzenegger als „Cyborg".

„Intelligente" Geräte, die im Internet of Things – IoT („Internet der Dinge") untereinander verbunden sind, bringen nicht nur Vorteile sondern bergen auch Gefahren, die von Lauschangriffen bis Sabotage reichen. Das „Internet der Dinge", die „Blockchain" und „künstliche Intelligenz" sind Schlüssel zur Dezentralisierung und Automatisierung in einer zunehmend digitalisierten Welt.

Das Internet der Dinge. Wir haben uns an Echtzeitinformationen über öffentliche Verkehrsmittel, Verfügbarkeit von Leihautos oder den Zustellstatus von Paketen gewöhnt. Wir können Heizung und Licht steuern und die Routenplanung vom Wohnzimmer aus ins Auto überspielen. IoT ist zu einer allgegenwärtigen Unterstützung geworden. In den letzten Jahren haben sich einige Bereiche des Lebens tiefgreifend verändert: Heute werden Musik oder Filme ganz anders konsumiert, als noch vor fünf oder zehn Jahren. Einkaufen, Urlauben, Planen oder Kommunizieren funktionieren für eine immer größere Zahl von Menschen nur mehr über unsere kleinen digitalen Helfer und den dahinter liegenden weltumspannenden Netzwerken. In ihrer Begeisterung sind Benutzer und Anbieter nicht immer auf die Sicherheit bedacht, die notwendig wäre. Spektakuläre Berichte von der Fernbeeinflussung von Autos, die beliebig gestartet oder gestoppt werden können, oder der Manipulation von ferngesteuerten Leuchtkörpern, die massive flächendeckende Blackouts erzeugen könnten, machen Angst. Woran liegt es, dass das passieren kann, und kann man etwas dagegen tun? Die Gründe, warum IoT oft mit mangelnder Sicherheit zu kämpfen hat, sind vielfältig. Das erklärt sich großteils damit, dass IoT besondere Bedingungen hat, wie sie an Schnittpunkten sehr unterschiedlicher Welten üblicherweise auftreten.

Drei Welten. IoT bringt Mechanik, Elektronik und IT zusammen. Diese drei Domänen funktionieren nach unterschiedlichen Spielregeln. Lösungen im Maschinenbau sind für Jahrzehnte ausgelegt, Veränderungen sind langsam, überprüft, erfordern hohen Änderungsaufwand in der Herstellung. Auch klassische elektroni-

FOTO: PROXIMA STUDIO/STOCK.ADOBE.COM

sche Systeme sind auf Dauer, Modularisierung, Optimierung und Kostenminimierung ausgelegt. Im Gegensatz dazu stehen IT-Lösungen: Sobald Hardware und Software zusammenwirken, gibt es neue Optimierungsmöglichkeiten, die meist in die Richtung laufen, dass Hardware zunehmend allgemein und wenig spezialisiert ist und erst die Software die konkrete Anpassung an die Anforderungen des Anwendungsfalles abdeckt. Rasche Anpassungen sind möglich, durch den Marktdruck sogar nötig. Damit sind regelmäßige Updates die Regel.

Es kann vorkommen, dass eine bestimmtes Gerät oder eine Anlage sich seit der Inbetriebnahme mechanisch nur minimal verändert hat, die Elektronik vielleicht zwei oder drei Generationswechsel in den letzten 40 Jahren erfahren hat, aber die digitale Steuerung, die in den Neunzigern hinzugekommen ist, alle fünf Jahre komplett erneuert wurde und mehrmals jährlich ein Update erhält – oder hätte erhalten sollen.

Beispiele für diese Mischwesen dreier Welten gibt es viele: Flugzeuge, die seit über 50 Jahren in Betrieb sind (die *Boeing 747* feierte 2019 ihren Fünfziger), Kraftwerke, die seit sechzig und mehr Jahren Energie liefern, öffentliche Verkehrssysteme, Wasser- und Energieversorgungen, Spitäler, Waffensysteme.

Jede Änderung dieser Systeme erfordert Spezialisten aus drei Welten, denn es gibt kaum Experten, die sich in mehr als einem dieser Felder bewegen können. Jede Änderung ist dadurch umso fehleranfälliger, da Auswirkungen auch über die Grenzen der Domäne hinaus passieren können (und müssen).

IoT-Geräte wie Webcams oder Router können ein Einfallstor in das Netzwerk bieten, in das das Gerät eingebunden ist.

Ebenen der Programmierung. Ein weiteres Thema, das IoT besonders betrifft, sind die unterschiedlichen Ebenen der Programmierung. Traditionelle Software besteht aus verschiedenen Schichten: Vereinfacht gibt es die Schicht, die mit den Anwendern in Verbindung tritt, die Schicht, die die Anwendungslogik handhabt, und die Schicht, die die Daten verwaltet. Dazu kommen besondere Funktionen, die sich durch eine mögliche Vernetzung ergeben, sowie besondere Schnittstellen, etwa zu Sensoren und Aktoren (Stellmotoren, Ventile, Schalter).

Im klassischen Anlagen- und Gerätebereich treten die einzelnen Schichten gemeinhin direkt miteinander in Verbindung. In der modernen IT gibt es in jedem System ein vielschichtiges Betriebssystem, das aus hierarchischen Modulen aufgebaut ist, in die sich die einzelnen Komponenten auf standardisierte Weise einklinken. Darauf bauen Frameworks („Baukastensysteme“) auf, die Funktionen in standardisierter Weise bereitstellen. Die eigentliche Anwendungsentwicklung findet meist mithilfe dieser Frameworks statt. Erst durch diese Architektur, modularisiert und standardisiert, kann eine zuverlässige Sicherheit, Überprüfbarkeit und Wartbarkeit erreicht werden. Aber immer noch sind typische „Anlagen“ wie Autos oft als nicht standardisierte Ad-hoc-Architekturen oder bestenfalls mittels standardisierter Bussysteme[1] aufgebaut. Firewalls, Sicherheitsfilter oder komplexe Plausibilitätsüberprüfungen (auf Basis von künstlicher Intelligenz) haben es in solchen Architekturen schwer. Ohne die Architektur komplett zu verändern, kann in einem solchen System nur unter unwirtschaftlich hohem Aufwand ein komplexes Sicherheitssystem eingebaut werden.

Abgesehen von den systembedingten Schwächen, die diese Ad-hoc-Lösungen bergen, kommt oft erschwerend der Zeitdruck hinzu, unter dem Entwickler von IoT-Lösungen stehen: Um rasch am Markt präsent zu sein, wird der Aufwand in der zeitraubenden Softwareentwicklung gering gehalten und oft unzureichend getestet. Anders, als beispielsweise bei einer Anwendungssoftware, die regelmäßig Updates erhält, fällt diese Möglichkeit bei IoT-Geräten meistens aus.

Dennoch gibt es Lösungen, die für IoT eine systematische, nachvollziehbare und testbare Sicherheit ermöglichen. Es handelt sich dabei um standardisierte Frameworks, die auf IoT-Anwendungsfälle spezialisiert sind. Eines der führenden Frameworks stammt von einem österreichischen Anbieter, dessen Know-how weltweit gefragt ist. *Applied Informatics Software Engineering GmbH*, eine Firma aus Kärnten, bietet für industrielle IoT, Automotive und Netzwerke von Sensoren Lösungen an, die weltweit gefragt sind.

Potenzielle trojanische Pferde. Moderne IoT-Lösungen für den Consumer-Bereich verwenden oft aus Kostengründen vorhandene Komponenten, die eine Vielzahl an Funktionen abdecken können. Je nach Konfiguration und Software werden bestimmte Funktionen eingesetzt. Es könnte beispielsweise eine Steuerung für eine Heizung, die Schnittstellen für entfernte Temperatursensoren und eine WLAN-Schnittstelle bietet, genauso in einem Babyfon verwendet werden, mit Mikrofon und einer Zweiwegkommunikation über einen eingebauten Lautsprecher. Durch Weglassen oder Hinzufügen von Teilen und durch Software entstehen verschiedene Geräte. Da die Komponenten immer kleiner und immer integrierter werden, kann es dazu kommen, dass das Mikrofon immer eingebaut bleibt, und in den meisten Anwendungsfällen einfach deaktiviert ist. Wer weiß, vielleicht ist die Kaffeemaschine, die über WLAN angeschaltet werden kann, bereits vorgesehen als ein System, das Wasserstand, Temperatur und Kaffeemenge überprüfen könnte und auf Zuruf reagieren könnte – irgendeinmal? Auf der Platine sind die nötigen Elemente bereits vorhanden, fehlen nur noch die entsprechenden Funktionen in der Software und die Sensoren.

FOTOS: VIPERAGP/STOCK.ADOBE.COM

IoT bringt Mechanik, Elektronik und IT zusammen. Diese drei Domänen funktionieren nach unterschiedlichen Spielregeln.

Vergleichbares gilt beispielsweise für WLAN-Router. Diese können durchwegs schlummernde Technologien enthalten, die nicht dokumentiert sind und für gezielte Angriffe nutzbar sind.

IoT und Wartbarkeit. Doch das augenscheinlichste Problem der derzeit üblichen IoT-Geräte ist banaler. Es entsteht aus einer Mischung aus Kostenoptimierung und oft gedankenloser Vereinfachung: Geräte sind über unveränderbare Passwörter abgesichert, die weltweit gleich sind; alte, unsichere Netzwerkprotokolle werden verwendet und so manches IoT-Gerät bietet ein Einfallstor in das Netzwerk, in dem das Gerät eingebunden ist. Viele dieser Geräte können nicht einmal durch ein Software-Update sicherer gemacht werden und sind in diesem Zustand von ihren Nutzern kaum beachtet über Jahre in Einsatz. Beispiele für solche problematischen Geräte sind manche fernsteuerbaren Lampen, WLAN-Router oder Webcams. Es gibt aber noch weitere Einfallstore, bei weit kritischeren Geräten, von denen Leben abhängen können: Im medizinischen Bereich werden Geräte oft über PC-Software gesteuert, die entweder im Gerät eingebaut oder über einen externen PC betrieben wird.

Da diese Geräte oft Verwendungszeiten von weit mehr als zehn Jahren haben, kommt es öfter vor, dass Systeme beispielsweise mit *Windows 2000* betrieben werden (müssen), das nicht den aktuellen Sicherheitsanforderungen entspricht – um Diagnose- oder Wartungsdaten einfach weiterzuleiten, hängen diese Systeme im Netzwerk, zusammen mit PCs, mit Zugang zum Internet. Muss ich mich vor meiner Kaffeemaschine schützen? Die einfache Antwort: Wenn Sie eine klassische Siebträgermaschine verwenden, sind Sie auf der sicheren Seite. Und beim Kaffeetratsch können unbedachte Worte auch ohne mithörende Kaffeemaschine gefährlich sein.

Internet. Was in den Sechzigern des vorigen Jahrhunderts als dezentrales Netzwerkprojekt von Militär und Universitäten in den USA begann, wurde in den 1980ern zu einem Rückgrat der Kommunikation zwischen Forschungszentren und Bildungseinrichtungen und drang in den Neunzigern in die kommerzielle Welt ein: 1995 gab es rund 16 Millionen Internetnutzer weltweit *(IDC)*, 2019 sind es bereits rund 4,4 Milliarden Nutzer *(www.internetworldstats.com/stats.htm)*. Einstmals ein Netz von Großrechnern, umfasst das Internet nun nicht nur Personal-Computer und Laptops, sondern auch Mobiltelefone und eine ständig steigende Zahl von Geräten, beispielsweise Kameras, Wetterstationen, Heizungssysteme oder Zimmerlampen – und die digitalen Assistenten. 2017 gab es weltweit rund 21 Milliarden vernetzte Geräte, 2022 werden es etwa 28 Milliarden sein – davon 24 Prozent Smartphones und 51 Prozent IoT-Geräte *(Cisco Visual Networking Index)*[2]. Das bringt eine Reihe technologischer Herausforderungen mit sich, ändert aber auch unser Leben in vieler Hinsicht. *Michael Werzowa*

Der Autor ist Experte für Netzwerk- und Datensicherheit, Vorstand der IoT Austria – The Austrian Internet of Things Network (www.iot-austria.at)

Anmerkungen:
[1]Bussysteme sind Austauschkanäle, an denen verschiedene Teilnehmer parallel angeschlossen sind, die ihre Kommunikation über dieses System abwickeln. In Autos gibt es den CANbus, über den sämtliche Sensor- und Steuersysteme der Fahrzeuge kommunizieren.
[2]www.cisco.com/c/en/us.