EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

FACHBERICHT

Internet of Things

Wie weit ist die Vision in der Realität angekommen?

Autor: Mihael Zadro, Business Consultant, IPG GmbH Deutschland

EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Inhaltsverzeichnis

1 Einleitung

Das Internet of Things (IoT) ist seit geraumer Zeit ein prominentes Gesprächsthema in den Medien. Eine allgemeingültige Definition des Begriffes sucht man jedoch vergebens. So unterschiedlich wie die Ansichten zu diesem Thema sind, präsentieren sich auch die Erklärungen dafür. Möchte man IoT in einem Unternehmen einsetzen, stellt man fest, dass es keine Standards gibt, die einem den Einstieg dazu erleichtern. Hohe Hürden hinsichtlich Sicherheit sind die Folge. Es gilt, die Risiken so weit wie möglich zu reduzieren und Fehlmanipulationen vorzubeugen. Dieser Fachbericht bietet eine Orientierungshilfe dazu.

2 Definition

Dieses Kapitel behandelt die geradezu inflationäre Verwendung des Begriffs IoT [1].

Google präsentiert für den Suchbegriff "Definition Internet der Dinge" (auf Deutsch) rund zwei Millionen Ergebnisse. Erstaunlicherweise wird keine konkrete Definition oder Erklärung eingeblendet. Es werden nur direkt wissenschaftliche Artikel in der Suche aufgelistet (Stand Dezember 2017).

Was diverse andere große Informationsanbieter über das "Internet der Dinge" sagen, wird nachfolgend erläutert.

Wikipedia [2] legt als Definition eine Vision dar, in der Computer die Aufmerksamkeit seitens der Menschen verlieren und ihre Dienste unbemerkt weiter verrichten. Im IoT werden physische Objekte (Dinge) der realen Welt mit einer virtuellen Repräsentation verknüpft. So werden laut Wikipedia diese physischen Dinge selbst zu Teilnehmern der virtuellen Welt. Dieser Zustand wird dadurch erreicht, indem Computer in (zum Teil alltägliche) Gegenstände eingebettet werden. Der Wikipedia-Artikel benennt auch mehrere verwandte Begriffe, die Überschneidungen mit dem IoT haben, geht aber nicht weiter darauf ein. Beispiele und Anwendungsgebiete für IoT sind überwiegend in der Logistik-Branche zu finden.

Der Deutsche Bundestag [3], genauer genommen der wissenschaftliche Dienst des Deutschen Bundestages spricht ähnlich wie Wikipedia von einer "technischen Vision, Objekte jeder Art in ein universales digitales Netz zu integrieren". Der Bundestag stellt sich so die Verknüpfung der Welt der Dinge (unsere reale Welt) mit der Welt der Daten (virtuelle Welt) vor. Alltagsgegenstände erhalten eine eindeutige Identität, mit der sie im Internet repräsentiert und angesteuert werden können. Das IoT hat laut dem wissenschaftlichen Dienst des Deutschen Bundestages dabei drei Eigenschaften:

- es ist allgegenwärtig
- die darin befindlichen Objekte sind weitgehend unsichtbar
- handeln aber autonom

Beispiele werden auch hier überwiegend aus der Logistik-Branche genannt. Interessant ist dabei, dass Begriffe, wie zum Beispiel: «Maschine-zu-Maschine-Kommunikation», «Smart Factory» und «Smart Grid» eindeutig dem IoT zugeordnet werden. Dies ist bei Wikipedia nicht so direkt der Fall.

Das Gabler Wirtschaftslexikon [4] präsentiert das IoT als "Vernetzung von Gegenständen mit dem Internet, damit diese Gegenstände selbstständig über das Internet kommunizieren und so verschiedene Aufgaben für den Besitzer erledigen können". Im Grunde sehr ähnlich der ersten beiden Erklärungen, wobei hier eher der Einsatzzweck hervorgehoben wird und nicht die Verbindung von realer und virtueller Welt. Beispiele finden sich bei Gabler aus der Welt der allgemeinen Informationsversorgung und dem E-Commerce (automatische Bestellungen). Als weiteres Einsatzgebiet für IoT werden Warn- und Notfallfunktionen genannt. Wie beim Bundestag werden hier auch die Begriffe: Digitalisierung, Industrie 4.0, Smart Home und Soziale Medien in Verbindung mit IoT gebracht.

Die FAZ [5] bietet bei der Suche nach IoT nur Beispiele für IoT an und bleibt eine Definition schuldig. Die einzige Aussage ist, dass der Mensch nicht in die Kommunikation, die zwischen den Dingen des IoT stattfindet, eingebunden ist. Weiter trifft die FAZ folgende Annahme: Alle Dinge sind mit einem Server oder einem Anbieter verbunden, der die Daten, welche die Dinge erheben, verarbeitet. Beispiele oder Anwendungen für IoT werden bei der FAZ nur aus der Logistik-Branche genannt.

ITWissen.info [6] bietet interessanterweise das erste Mal eine Unterscheidung von IoT: Es gibt Konzepte für die Industrie und Konzepte für Consumer/Endverbraucher. ITWissen.info bestätigt auch, dass Dinge des IoT eine eindeutig zugeordnete Identität oder ID erhalten. Man geht sogar einen Schritt weiter und behauptet, dass Dinge so zu "Smart Objects" oder «IEDs» (Intelligent Electronic Devices) werden. Genannt werden hier auch die selbstständige Kommunikation zwischen Dingen des IoT. Der Artikel geht auch etwas auf die Geschichte um IoT ein und besagt, dass es Geräte die miteinander kommunizieren bereits gab, bevor es den Begriff IoT gab. Im Prinzip nichts Neues. Beispiele und Anwendungsbereiche werden hier weit mehr genannt als in den vorhergehenden Artikeln. Es finden sich Beispiele aus den Bereichen: Auto, Medizin, Gebäudeautomatisierung, Wearables (Smarte Kleidung) und natürlich auch Logistik. Interessant ist, dass am Ende die erste Erwähnung des Begriffes "Internet of Everything" als Weiterentwicklung des IoT folgt.

Das Portal **"Mittelstand: Die Macher"** [7] erwähnt zum ersten Mal, dass es eigentlich keine einheitliche Definition für IoT gibt. Jeder hat seine eigene Definition. Und das führt der Artikel auch aus und bezeichnet IoT als Thema im dem es um die "Kommunikation zwischen Geräten geht, die mit Mikroprozessoren und jeweils mit einem RFID-Funk-Chip oder QR-Code ausgestattet sind". Dinge sammeln Informationen über sich und die Umgebung in der sie sich befinden und senden diese an andere (vernetzte) Dinge. Gesammelte Daten werden dabei ausgewertet. Als Beispiele und Anwendungsgebiete werden das Gesundheitswesen (eHealth), Smart Home, Auto und Industrie genannt.

Alle vorgestellten Definitionen für das IoT zeigen, wie unterschiedlich ein an sich einfacher Sachverhalt verstanden werden kann. Klar wird auch, dass es aktuell an einer allgemein gültigen Beschreibung oder Definition von höherer Stelle, wie einer Regierung oder einem Board, die sich um Standards kümmert, mangelt. Man stolpert bei der Recherche von einem Schlagwort zum anderen. Alle haben jedoch irgendwie etwas mit IoT zu tun.

2.1 Weiterführende Gedanken zur Definition IoT

Der Grundgedanke von IoT ist: Jedes in der realen Welt "smarte" Objekt oder auch Ding "transportiert" Informationen, die es unter Umständen selbst erheben kann, aus der realen Welt in die virtuelle Welt. Diese Informationen stellt es anderen Objekten in der virtuellen Welt zur Verfügung. Das Internet der Dinge ist somit ein Netz von Dingen über welches Informationen ausgetauscht werden. Diese «Kommunikation» läuft dabei ohne menschlichen Eingriff ab.

Auf welcher technischen Ebene oder wie genau die Kommunikation zwischen zwei Dingen abläuft, spielt für die übertragenen Informationen im Wesentlichen keine große Rolle. Also hat die technische Ebene für die Definition auch keine Relevanz. Die Kommunikation kann sich nach Einsatzzweck und davon abhängigen technischen Möglichkeiten (siehe dazu die Kapitel Standards und Protokolle) unterscheiden.

Was sich im Wesentlichen nicht unterscheidet, sind die Objekte in der virtuellen Welt selbst. Man kann dazu folgende These aufstellen: Jedes smarte Objekt, welches in der realen Welt existiert, stellt in der virtuellen Welt eine eindeutige Identität dar. Mit dieser Identität kann ein virtuelles Objekt einem realen Objekt zugeordnet werden. Das Kapitel IoT & IDM geht weiter auf diese These ein.

Bis heute begegnet man vielen Ideen rund um den Einsatz für Dinge des IoT. Die Definition darf aber keinen Bezug zu einem Einsatzzweck oder einer Idee, deren Realisierung ein Objekt im IoT ist, nehmen. Das ist wichtig, da wir heute nicht erahnen können, welche Ideen zukünftig aufkommen werden. An sich ist die Liste der Einsatzmöglichkeiten von IoT unbegrenzt. Genauso unbegrenzt, wie die Anzahl der Ideen, die mit Geräten realisiert werden können (Siehe dazu Kapitel Anwendungsgebiete /-Ideen).

Ein weiterer zu betrachtender Aspekt ist das Thema Sicherheit. Auch dieser Aspekt ist für Dinge im IoT sehr wichtig. Für die Definition hat Sicherheit aber keine Relevanz. Sicherheit ist stark mit dem Einsatzzweck verbunden. Da der Einsatzzweck auch die erforderliche Sicherheitsstufe bestimmt und der Einsatzzweck keinen Bezug zur Definition hat, hat auch die Sicherheit keine Berechtigung in der Definition genannt zu werden.

Neben dem Begriff Sicherheit gibt es noch einen weiteren Begriff, der sehr eng mit IoT verknüpft ist: "Industrie 4.0". Kaum ein anderer Begriff wird so stark mit dem IoT in Verbindung gebracht wie Industrie 4.0. Industrie 4.0 beherbergt ein sehr weites Feld an Themen und beinhaltet das Thema IoT lediglich. Aus diesem Grund ist es für die Definition auch nicht relevant. Welche Themen genau und was Industrie 4.0 genau ist, ist im Kapitel IoT und Industrie 4.0? zu finden.

2.2 Eigene Definition

Nach der Betrachtung fremder Definitionen, Ausführungen und den oben aufgeführten weiterführenden Gedanken ergibt sich folgende Definition für das IoT:

Das IoT besteht aus Dingen, die durch eingebaute Computer in die Lage versetzt werden, direkt und / oder über das Internet mit anderen Dingen oder Computern zu kommunizieren. Diese Kommunikation kann autonom, ohne menschlichen Eingriff stattfinden.

Diese Definition unterscheidet sich nicht grundlegend von anderen Definitionen, bildet aber die Basis für die in diesem Bericht verarbeiteten Informationen.

3 IoT und Industrie 4.0?

Der Begriff "Industrie 4.0" ist zurzeit allgegenwärtig. Doch woher kommt der Begriff und was bedeutet er? Kurz: Der Begriff steht für die vierte industrielle Revolution.

3.1 Die industriellen Revolutionen im kurzen Überblick

Als industrielle Revolution wird in der Regel eine tiefgreifende und dauerhafte Veränderung von gewerblichen Produktionsformen und damit einhergehenden Änderungen von Arbeitsbedingungen bezeichnet. Mit den Arbeitsbedingungen ändern sich aber auch die wirtschaftlichen und sozialen Verhältnisse in der Welt.

Die erste industrielle Revolution fand Ende des 18. Jahrhunderts statt und breitete sich von England über Westeuropa, die USA und etwas später auch über den Rest der Welt aus. Unter dieser ersten industriellen Revolution versteht man die Einführung von mechanischen Produktionsanlagen. Damit gemeint sind Dampfmaschinen, der Webstuhl oder auch Erfindungen wie die Gasbeleuchtung, mit der Anfang des 19. Jahrhunderts viele Straßen europäischer Großstädte erhellt wurden.

Die zweite industrielle Revolution begann im deutsch- und französischsprachigen Raum, ungefähr Ende des 19. Jahrhunderts und wird allgemein mit dem Beginn der Massenproduktion mit Hilfe von Elektrifizierung gleichgesetzt. So auch in den USA: Dort wird mit der zweiten industriellen Revolution der Übergang zur Massenproduktion aber auch der Übergang zu industriellen Organisationsformen wie dem Fordismus (in den 1920er Jahren) bezeichnet.

Die dritte industrielle Revolution ist im Grundgedanken mit der digitalen Revolution gleichzusetzen. Diese basiert auf der Entwicklung und Einführung von Mikrochips und ist etwa in der Mitte der 1970er Jahre anzusiedeln. Aus der Zeit der dritten industriellen Revolution stammt auch das Moore'sche Gesetz. Im Rahmen dieser Revolution wurden die Informations- und Kommunikationsprozesse digitalisiert und somit endgültig das digitale Zeitalter eingeführt. In der Industrie wurden und werden Produktionsprozesse mit Hilfe von Elektronik und Informationstechnologien mehr und mehr automatisiert.

3.2 Industrie 4.0 ist die vierte industrielle Revolution

Ursprünglich wurde die Verwendung des Begriffes Industrie 4.0 in Deutschland mit der Acatech-Studie "agendaCPS" (Agenda Cyber-Physical Systems) im Jahr 2011 ausgelöst. In dieser Studie wird der Weg von "Embedded Systems" hin zu "Cyber-Physical Systems" beschrieben. Neben den Entwicklungsmethoden werden auch einige Anwendungsbereiche benannt. Darunter finden sich auch Begriffe wie Smart Mobility, Smart Grid und Smart Factory. Insbesondere der Begriff Smart Factory sorgte über die Studie hinaus für viele Diskussionen. Eine Forschungsunion widmete sich der Frage, wie eine vernetzte, echtzeitfähige und adaptive Produktion (Fabrik) aussehen könnte. Weitere Informationen hierzu finden sich im nächsten Unterkaptiel unter dem Schlagwort «Smart Factory».

3.3 Zukunftsprojekt Industrie 4.0

Aufbauend auf der agendaCPS-Studie arbeitete ein "Arbeitskreis Industrie 4.0", der Ende 2011 von der Promotorengruppe Kommunikation der Forschungsunion Wirtschaft-Wissenschaft initiiert wurde, an den weiterführenden strategischen Umsetzungsempfehlungen für das "Zukunftsprojekt Industrie 4.0". In den Ausführungen zu den Umsetzungsempfehlungen werden die Voraussetzungen für das vierte industrielle Zeitalter ebenso behandelt, wie die Auswirkungen auf Wirtschaft, Wissenschaft und Gesellschaft. Der Abschlussbericht des Arbeitskreises und die Umsetzungsempfehlungen wurden der Bundesregierung auf der Hannover-Messe 2013 übergeben. Im Zuge dessen hat der Bund im Rahmen seiner High-Tech-Strategie einige Projekte angeregt. Darunter befindet sich auch das ressortübergreifende "Zukunftsprojekt Industrie 4.0". Mit diesem Projekt werden Forschung und Entwicklung in verschiedenen Bereichen gefördert. Dies sind unter anderem die Integration heterogener IT-Systeme in der Produktion sowie die Standardisierung von Soft- und Hardware-Schnittstellen zur Realisierung der Interoperabilität zwischen Produktionssystemen. Damit soll ein möglicher künftiger Standard gefunden werden.

Gleichzeitig mit der Übergabe der Umsetzungsempfehlungen fiel auch der Startschuss für die von den Verbänden VDMA, ZVEI und Bitkom getragene "Plattform Industrie 4.0". Ihr Ziel: Das im Abschlussbericht beschriebene Innovationspotenzial zu konkretisieren und ein Konzept zur Umsetzung zu erarbeiten. Darunter fällt auch die Smart Factory.

Smart Factory

Eine "smarte" Fabrik könnte sich in etwa so präsentieren: Produkte werden in Echtzeit und nur nach Bestellung hergestellt. Sobald eine Bestellung für ein Produkt eingeht, wird ein individueller Auftrag erstellt, der neben technischen Informationen weitere Daten (z.B. Auftraggeber, Lieferadresse etc.) enthält. Dieser Auftrag wird mit dem Produkt, beispielsweise mittels eines Barcodes, verknüpft. Die Fertigungsstraße kann anhand des Barcodes am Rohling feststellen, für welchen Auftrag der Rohling vorgesehen ist und diesen nach dem jeweiligen Wunsch bearbeiten. Sollte etwas für einen späteren Produktionsschritt fehlen, so wird die gewünschte Teilkomponente (auch extern) bestellt. Ein großer Vorteil des Systems: Das Produkt lässt sich über die gesamte Wertschöpfungskette hinweg verfolgen. Alles kann Just-in-Time erfolgen. Soweit die Theorie.

3.4 Projekte zeigen: Es geht - aber es fehlt ein Standard

Verschiedene Projekte in der Industrie zeigen, dass schon mit den heute verfügbaren Mitteln vieles davon umsetzbar ist. Die Technik für die Vernetzung von Produkten, Lieferketten und Lieferanten ist vorhanden. Vielen Unternehmen bereitet es aber Schwierigkeiten, die entsprechenden Prozesse zu gestalten. Dies weil neue Abläufe häufig Abteilungs- und Unternehmensgrenzen überschreiten und unterschiedliche Datenquellen anzapfen. Noch schwieriger wird es, wenn sich unterschiedliche Branchen auf Schnittstellen für den Informationsaustausch einigen müssen. Wie aufwändig ein solches Unterfangen werden kann, zeigen gerade die Energieversorgungs- und Automobilindustrie. Bislang ist es ihnen nicht gelungen, die Elektromobilität und die erneuerbare und dezentrale Energiegewinnung zusammenzuführen.

Industrie 4.0 umfasst also nicht nur eine intelligente Produktion, sondern auch die Expansion der Fertigungsunternehmen in den Servicemarkt. Grundsätzlich sieht die Industrie in der Vernetzung einzelner Komponenten den Mehrwert, physikalische Produkte mit Dienstleistungen so zu ummanteln, dass neue Geschäftsmodelle entstehen.

3.5 Wie hängen IoT und Industrie 4.0 nun zusammen?

Industrie 4.0 ist ohne IoT nicht möglich! Die Industrie möchte in ihrem vierten Zeitalter die Produktion, Produktionsschritte und im Endeffekt den Kunden verbinden. Dazu bedarf es Technologie, die einen Zustand über die virtuelle Welt transportieren kann. Damit braucht Industrie 4.0 das Internet der Dinge. Das IoT gab es technisch gesehen bereits vor Industrie 4.0. Durch Industrie 4.0 bekommt die Vernetzung von Dingen allerdings eine neue Bedeutung. Objekte müssen Informationen transportieren. Damit das aber auch Branchenübergreifend funktioniert, muss eine gemeinsame Sprache gefunden werden.

4 Standards

Nach einer langen Recherche zu einem eventuell vorhandenen einheitlichen Standard im Bereich IoT gibt es nur festzuhalten, dass es keinen Standard gibt.

Eigentlich müsste mit dem Internet-Protokoll auch im IoT eine globale Ende-zu-Ende-Kommunikation möglich sein. Auf der Netzwerkebene trifft das auch weitgehend zu. Geräte hören sich gegenseitig. "Das ist aber nur so hilfreich wie ein Telefonanruf in China, wenn man kein Chinesisch spricht", sagte Professor Axel Sikora, wissenschaftlicher Direktor des Instituts für verlässliche Embedded Systems und Kommunikationselektronik (ivESK) an der Hochschule Offenburg. "Solange die Maschinen auf der Anwendungsebene unterschiedliche Sprachen sprechen, verstehen sie sich trotz bestehender Verbindung nicht."

Diesen Umstand müssen Entwickler von Geräten für das IoT berücksichtigen und das Problem der Verständigung lösen. Dabei helfen vor allem Protokolle wie MQTT, LWM2M und OPC-UA für die Anbindung von Geräten auf Anwendungsebene. Aber einen wirklichen Standard gibt es nicht. Ganz im Gegenteil. Die offiziellen Standardisierungsgremien, die Standards eigentlich verabschieden müssten, verlieren Stück für Stück ihre Vorreiterrolle. Immer häufiger werden in der Industrie selbst und in anderen Organisationen Beschlüsse gefasst, die dann vom Standardisierungsgremium einfach übernommen werden.

Daraus ergeben sich zwei Entwicklungen:

- Sehr große Unternehmen wie zum Beispiel Amazon, Google oder Samsung bringen ihre Lösungen ohne vorherige Abstimmung unmittelbar in den Markt. Damit versuchen sie einen Quasi-Standard einzuführen. Standardisierungsgremien werden somit «vor vollendete Tatsachen» gestellt. Die schiere Größe der Unternehmen und die Reichweite ihrer Produkte definieren das Produkt dann als Standard.
- Kleinere Unternehmen, denen die Produkte der großen Unternehmen entweder zu teuer sind oder den Anforderungen nicht entsprechen, folgen in diesem Sinne dem Ansatz der Großen und

etablieren ihren eigenen «kleinen Standard». Sie kochen umgangssprachlich ihr eigenes Süppchen.

Diese beiden Entwicklungen wirken im Grundsatz gemeinsam einem Standard entgegen. Ursache dafür ist das Ziel eines jeden Unternehmens, schnell im Markt zu sein und schnell Geld mit seinen Produkten zu verdienen und eine Abhängigkeit der Kunden zu schaffen. Kleinere Unternehmen werden dadurch von großen Unternehmen aus dem Markt gedrängt.

4.1 Zusammenfassung

Abschließend kann festgehalten werden, dass ein branchenübergreifender und damit in gewisser Weise verbindender IoT-Standard noch nicht gefunden worden ist. Dieser Umstand stellt für viele Unternehmen eine hohe Hürde dar. Das Ergebnis ist, dass viele Unternehmen ihre eigenen Lösungen kreieren und sich in der Regel nicht miteinander abstimmen. Das steht wiederum einem gemeinsamen Standard im Weg. So lange dieser Kreis nicht durchbrochen wird, wird die Idee eines IoT-Standards nur bedingt funktionieren und die Entwicklung aufgrund ausbleibender Erfolge nur langsam und unkontrolliert fortschreiten.

5 Protokolle

Es gibt sehr viele Protokolle und Transportwege auf allen Ebenen der elektronischen Kommunikation. Die einen nutzen dafür einen komplexen CAN-Bus, andere nur einen Draht.

Maschinen werden für die verschiedensten Anwendungen eingesetzt und kommunizieren dementsprechend miteinander. Beispielsweise muss die eine Maschine lediglich wissen, ob die anderen betriebsbereit sind, eine andere Maschine hat die Aufgabe eine Temperaturangabe zu übermitteln und wieder andere übermitteln/empfangen komplexe Befehle mit Abhängigkeiten. Weiter gibt es Maschinen, die hochsensible Daten übermitteln, die im Extremfall sogar über Leben und Tod entscheiden können.

Dies zeigt, dass sich auch die «Datentransportwege» unterschiedlich gestalten. Während manche Maschinen per Kabel miteinander verbunden sind, sind andere über einen drahtlosen Zugang verbunden. In Anbetracht der enormen Vernetzung, die heute herrscht, sind viele Maschinen und Dinge über das Internet (TCP/IP) verbunden.

Grob können von IoT verwendete Protokolle in folgende Kategorien eingeordnet werden:

- Infrastruktur (Bsp: IPv4/IPv6, ROLL/RPL, UDP, 6LowPAN)
- Identifikation / Authentifizierung (Bsp: IPv6, QUIC, NanoIP, TSMP)
- Kommunikation / Transportmedium (Bsp: Wifi, Bluetooth, LPWAN, u.a.)
- Identifikation / Präsenz (Bsp: PhysicalWeb, mDNS, DNS-SD, UPnP)
- Datentransport (Bsp: MQTT, CoAP, XMPP, AMQP, Websocket, Node)
- Management (Bsp: TR-069, OMA-DM)
- Sicherheit (OTrP, X.509)

Diese Liste ist nicht abschliessend.

6 Sicherheit

Befürworter predigen, dass IoT-Business-Möglichkeiten enorme Erfolgspotentiale mit sich bringen. Gleichzeitig wird das IoT Probleme hinsichtlich der Privatsphäre und Sicherheit mit sich bringen.

6.1 Sicherheit

Über Sicherheit in Bezug auf das IoT zu diskutieren ist schwierig, weil dieses Konzept gewaltige Ausmasse hat, wenn „alles“ miteinander verbunden ist. Die Schwierigkeit dabei ist es, den Überblick zu behalten, wenn Autos, Kühe, Bohrinseln, Kühlschränke usw. miteinander verbunden sind.

6.2 Privatsphäre

Alle werden feststellen, dass die Selbstkontrolle über (ihre) Daten komplett verloren ist. Keiner weiß wirklich mehr, wo sich seine Daten und Informationen befinden und wohin sie verschoben werden / wurden. Die Kontrolle über Daten verschiebt sich vom Anwender zu den Maschinen. Wenn ein Mensch einem anderen nicht sagen möchte, wie viel Grad es in seiner Wohnung hat oder ob er zu Hause ist, dann schweigt er einfach. Ein Gerät welches dazu entwickelt wurde, die Temperatur oder die Anwesenheit zu melden, wird dies immer tun.

In diesem Zusammenhang bedeutet Sicherheit auch Rechenleistung. „Dinge“ (z.B. Sensoren) sind aber nur mit einem absoluten Minimum ausgestattet, wenn überhaupt.

Es gibt meist ein (wenn auch kleines) Betriebssystem, das die smarten Dinge betreibt und steuert. Die Verwendung dieser Betriebssysteme folgt aktuell keinem Standard und keiner Empfehlung. Geräte werden entwickelt und gebaut, um möglichst schnell im Markt präsent zu sein. Verwendete Softwarekomponenten werden so zusammengesetzt, dass sie funktionieren. Meist wird ausser Acht gelassen, dass die eingesetzte Software das Tor für den (Daten-)Missbrauch ist. Verwendete Betriebssysteme und Komponenten müssen aktualisiert werden können, um Schwachstellen auszumerzen. Nur so haben unberechtigte Zugriffe und böswillige Veränderungsabsichten keinen Zugang (mehr).

6.3 Haftung

Nicht sehr hilfreich in diesem Zusammenhang ist auch die unklare Gesetzeslage über die Haftbarkeit. Wer haftet, wenn beispielsweise jemand das Bremssystem eines Autos verändert? Verletzungen, Sachschäden oder sogar Tod können die Folge eines manipulierten Bremssystems sein. Ist der Autohersteller für die Sicherheitslücke oder der «Einbrecher», welcher die Sicherheitslücke ausnutzt, verantwortlich? Im Moment bewegen wir uns hier noch in einer Grauzone.

In den meisten Fällen werden die Hardware-Hersteller der „Dinge“ nicht für die Sicherheit verantwortlich sein wollen. An dieser Stelle wird man die Software-Hersteller in die Pflicht nehmen, welche die Anwendung für die Verbindungen der „Dinge“ bereitstellen.. Eine klare Definition zur Haftung hilft auch den Betreibern von IoT-Geräten, die meist der erste Ansprechpartner von Betroffenen sind.

6.4 Auswirkungen und Gefahren

Immer mehr, mehr oder weniger intelligente, Geräte werden ans Internet angeschlossen. Dadurch steigt nicht nur die Anzahl der Kommunikationsteilnehmer im Internet, sondern auch die Anzahl verwundbarer Geräte, welche missbraucht werden können. Kriminelle Energie treibt wundersame Blüten. Bevor es nicht passiert ist, konnte sich kein Hersteller ausmalen, dass sein Raumthermometer dazu verwendet wird, um beispielsweise Spam-E-Mails zu versenden oder an Angriffen auf andere Internet-Teilnehmer beteiligt zu sein (DDoS-Attacken). Anders als beim Desktop-Computer oder Smartphone denkt aber beim intelligenten Lichtschalter oder Kühlschrank noch kaum jemand daran, dass auch diese Geräte Software- und Sicherheit-Updates brauchen.

Sind die Geräte und Dinge über das Internet zu erreichen, ist das Gefahrenpotenzial noch höher. Grundsätzlich können solche Geräte über einen Portscan oder eine Suchmaschine wie Shodan, von jedem gefunden werden. Sind sie dann lediglich mit Standard-Zugangsdaten (Benutzername und Passwort) geschützt, kann auf diese Geräte oder Dinge relativ einfach unberechtigt zugegriffen werden. Hier lohnt es sich, die Authentifizierung mit mehreren Faktoren zu sichern.

7 Anwendungsgebiete/-Ideen

Das IoT ist ein recht weitgefasster Oberbegriff. Es lässt sich für jeden Lebensbereich ein passender Ausdruck finden, der die IoT-Idee in sich trägt. Nachfolgend werden hierzu einige wichtige Schlagwörter kurz beschrieben:

Smart Factory
Dies ist ein Anwendungsgebiet von Industrie 4.0 und meint nichts anderes als eine Fabrik, welche die Fertigung komplett ohne menschlichen Eingriff durchführen kann. Alle benötigten Informationen werden selbstständig ermittelt und verarbeitet. Zum Beispiel werden die Daten zur Bearbeitung eines Werkstückes mittels Sensoren direkt vom Werkstück gelesen und an die bearbeitende Maschine weitergegeben.

Smart Home
Diverse elektrische und elektronische Geräte im eigenen Heim lassen sich vom Besitzer über das Internet oder Netzwerk steuern oder stellen sich dank der in der Wohnung verteilten Sensoren auf die Umgebung ein. Dazu gehört zum Beispiel auch ein internetfähiger Kühlschrank, der automatisch neue Milch bestellen kann, sobald der Vorrat zuneige geht. Oder er kann anhand seines aktuellen Inhalts Rezepte vorschlagen.

Smart City
Darunter versteht man einen kompletten urbanen Raum, in dem Menschen und die sie umgebende Technologie (Sensoren, Aktoren) unmittelbar miteinander (inter-)agieren können.

Smart Grid
Vernetzung im intelligenten Stromnetz der jeweiligen Elemente zur Stromerzeugung, Verteilung, Verbrauch und vor allem Verbrauchsmessung, um den Strom zeit- und punktgenau dort bereitzustellen, wo er gebraucht wird.

Connected Car
Im Prinzip ein an das Internet angebundenes Fahrzeug. Bestimmte Funktionen lassen sich so über das Internet steuern. Während der Fahrt erhält das Fahrzeug Informationen aus dem Internet. In der Zukunft könnten selbstfahrende Autos so auch selbstständig ihre Route aufgrund aktueller Informationen anpassen.

Wearables
Kleine Computer und Sensoren, die in Brillen, Kleidung und Schmuck eingearbeitet und teilweise mit anderen Geräten oder dem Internet verbunden sind. Sie bringen dem Träger zusätzliche Informationen, ohne dass er aktiv eingreifen muss. Zu Wearables gehören Fitnessbänder, Smartwatches und Augmented-Reality-Brillen.

eHealth
Im Sinne von IoT werden darunter digitale Lösungen verstanden, die den elektronischen Austausch medizinischer Informationen zwischen Patienten und Medizinern oder unter Medizinern automatisieren. Dazu gehören auch in Patienten eingepflanzte Sensoren, die medizinische Messwerte direkt an den behandelnden Arzt oder medizinische Instrumente übermitteln.

7.1 Anwendungs-Ideen

Wer konnte sich zu Zeiten der Dampfeisenbahn vorstellen, dass die Menschheit in der Zukunft mit dem ICE innert kurzer Zeit bequem quer durch Europa reisen wird? Pioniere gab es immer und wird es immer geben. Im Bereich IoT werden in Zukunft noch viele andere, und uns heute noch unbekannte Anwendungsgebiete, dazu kommen. Stichworte wie die Weiterentwicklung der 3D-Drucker oder Autos, welche sich durch Sprache und Gesten steuern lassen und dank künstlicher Intelligenz erstmals lernfähig sein werden. Die Möglichkeiten der technischen Innovationen sind unendlich.

8 IoT & IDM

8.1 Grundgedanke

Geräte des IoT ähnlich wie Identitäten in und mit einem IDM-System zu verwalten liegt nahe. Der Grundgedanke drängt sich auf, den Lebenszyklus eines Mitarbeiters (repräsentiert durch eine Identität) in einem Unternehmen mit dem Lebenszyklus eines Gerätes zu vergleichen bzw. sogar gleichzustellen. Es tauchen, rein technisch gesehen, viele Gemeinsamkeiten auf und viele Workflows verlaufen ähnlich, wenn nicht sogar parallel.

Doch so einfach kann es bei genauer Betrachtung nicht umgesetzt werden. Die reine Verwaltung von Geräten im IoT ist oberflächlich gesehen zwar sehr ähnlich wie „normale“ Identitäten zu verwalten, spätestens aber bei der Verwaltung von Berechtigungen werden Unterschiede deutlich.

8.2 Unterschied zwischen Mensch und Maschine

Der Entzug oder das Fehlen einer Berechtigung stellt für einen Menschen weniger ein Problem dar, als es für ein Gerät im IoT ist. Ein Mensch stellt fest, dass er beispielsweise nicht mehr auf einen

Ordner zugreifen kann. Der Mensch kann die Situation analysieren, vielleicht hilft eine Fehlermeldung die sagt, dass er nicht berechtigt ist auf diesen Ordner zuzugreifen. Nun kann sich ein Mensch den Zugriff darauf verschaffen, indem er die Berechtigung beantragt oder einen Administrator bittet ihm diesen einzurichten. Ein Gerät kann nur das, wozu es programmiert wurde. Sollte ein nötiger Zugriff entzogen worden sein, wird, je nach Programmierung, das Gerät im schlimmsten Fall in einer Dauerschleife hängen oder gar abstürzen und früher oder später seinen Dienst versagen. Im Besten Fall ist eine Fehlerbehandlung implementiert, mit der das Gerät auf den fehlenden Zugriff aufmerksam machen kann. Zum Beispiel mit einer E-Mail an seinen Administrator.

Die Erteilung einer Berechtigung für ein Gerät ist insofern auch etwas anders, da einem Menschen kommunikativ mitgeteilt werden kann, er könne jetzt auf einen Ordner zugreifen. Einer Maschine muss das über die Programmierung mitgeteilt werden. Die Information eines erteilten Zugriffes muss also demjenigen zukommen, der die Programmierung eines Gerätes beeinflussen kann, um die neue Situation zu respektieren.

Diese Tatsache, dass bei der Verwaltung einer Identität einer natürlichen Person Intelligenz vorausgesetzt werden kann und bei der Verwaltung einer Identität eines Gerätes nicht, ist nicht die einzige Besonderheit. Zwar könnte man so eine Intelligenz einem Gerät des IoT (durch eine geschickte Programmierung) beibringen, jedoch bleibt die Bedingung „Intelligenz voraussetzten“ die gleiche.

8.3 Weitere Herausforderung: Security

Ein Mensch sendet bewusst, wieder nur technisch betrachtet, Informationen nur an ihm bekannte bzw. berechtigte Empfänger weiter. Ein Mitarbeiter würde beispielsweise den Füllstand eines Dieseltanks nur an wirklich berechtigte Empfänger weitergeben. Kriminelle Energien oder ähnliches außen vorgelassen. Ein Gerät sendet diese Informationen immer ab. Eine Prüfung ob der Empfänger berechtigt ist diese Information zu erhalten, findet eher selten statt. Gleiches gilt für einen Anwesenheits-Sensor: Die Information ob jemand zu Hause ist oder nicht, sollte nur für Bewohner oder berechtigte Stellen vorgehalten werden. Kriminelle Energien interessieren sich aber auch für diese Information.

Höhere Sicherheit (wie in unserem Beispiel vereinfacht gesagt eine Prüfung des Empfängers) könnte durch mehr Intelligenz in Form einer intelligenteren Programmierung erreicht werden. Das macht ein Gerät aber teurer. Vorausgesetzt es ist denn überhaupt möglich, einem Gerät mehr Intelligenz zu geben. Es widerspricht in jedem Falle der Voraussetzung: Smarte Geräte müssen günstig funktionieren.

Die Idee, Geräte als Identitäten zu behandeln muss also zwingend dem Sicherheits-Aspekt gerecht werden. Technisch lässt sich eine Blockade der gesendeten Informationen relativ einfach, zum Beispiel mit einer Firewall, lösen. Der Sicherheits-Aspekt muss aber neben der technischen Sicht auch in allen IDM-Prozessen betrachtet werden. Reicht es bei einem Ausscheiden eines Mitarbeiters in der Regel alle Accounts zu sperren und die Identitäten zu deaktivieren, muss bei Geräten unter Umständen mehr getan werden. Ein Mitarbeiter hat ohne funktionierende Accounts wenig Potential Schaden in einem System anzurichten. Ein Gerät, das neben seiner eigentlichen Aufgabe, den Diesel-Füllstand zu melden, noch weitere Dinge könnte, wie E-Mails zu versenden, kann ein höheres Schadenspotential darstellen. Die einfache Deaktivierung der Melde-Funktion reicht in diesem Falle nicht

aus. Alleine die technische Möglichkeit, E-Mails zu versenden kann durch eine Softwarelücke missbraucht werden. Zusätzlich sollte zum Beispiel das Versenden von E-Mails durch das Gerät technisch unterbunden werden oder der Zugang zum eigenen Netzwerk für das Gerät gänzlich abgestellt werden. Gleichzeitig muss hier geprüft werden, ob die Deaktivierung des Gerätes keine Prozesse beeinflusst. Sollte dies der Fall sein, müssen Prozesse neu modelliert und ggf. umprogrammiert werden.

An sich sind der Kreativität der Programmierungen von Geräten des IoT und auch den möglichen Szenarien, die eine (schlechte) Programmierung als Ursache haben könnten, keine Grenzen gesetzt. Sicher ist, dass mit der Verwaltung von Geräten in einem IDM etwas mehr das Thema Security im Vordergrund steht als die reine „Verwaltung" der Geräte. Das ist bedingt durch die Hersteller der Geräte, die meist eigene Software-Lösungen zur Verwaltung ihrer Geräte mitliefern. Wenn sich in einem Portfolio allerdings viele Geräte von eventuell verschiedenen Herstellern befinden, die verschiedenen Aufgaben dienen, gewinnt die Idee einer zentralen Verwaltung durch ein IDM-Tool, trotz höherem Aufwand, wieder an Attraktivität.

8.4 Je mehr verschiedene Geräte, desto interessanter die Verwaltung mittels IDM

Als gutes Argument für die Idee, Geräte des IoT mit einem IDM zu verwalten, stehen standardisierte Workflows, beispielsweise für den „Eintritt" eines Gerätes in ein Unternehmen. Warum sollte man nicht auch für Geräte ein standardisiertes Vorgehen entwickeln, wie man es für seine Mitarbeiter entwickelt hat. Geräte erhalten eine eindeutige Identität, werden erfasst und an eine verantwortliche Stelle übergeben. Insbesondere bei einer großen Menge an vielleicht verschiedenen smarten Geräten, würde so ein standardisiertes Vorgehen, unabhängig vom Einsatzzweck, den administrativen Aufwand durch Tool-Unterstützung verringern und gleichzeitig die Sicherheit im Unternehmen erhöhen.

Die Etablierung eines vorgegebenen Prozesses „Austritt" eines Gerätes aus dem Unternehmen ist der nächste logische Schritt. Die Standard-Prozesskette wird um den Schritt ergänzt für das Gerät einen Eintrag in der Firewall zu erstellen bzw. das Gerät auf eine technische Blacklist zu setzten, die nach dem Ausscheiden des Gerätes eine Kommunikation unterbindet. Eine weitere Idee wäre, dass der Verantwortliche, oder „Vorgesetzte" des Gerätes, dieses ordnungsgemäß abmelden muss. Eine umweltgerechte Entsorgung könnte so auch realisiert werden. Alle diese Maßnahmen, basierend auf Standard IDM-Prozessen, steigern die Sicherheit im Unternehmen und sind im Prinzip für alle Geräte gleich. Je mehr Geräte in einem Unternehmen verwaltet werden müssen, desto interessanter und lukrativer ist es, diese unabhängig vom Anwendungszweck in einem IDM zu verwalten.

8.5 Geräte in die unternehmensweiten Prozesse integrieren

Die Schwierigkeit bei der Umsetzung der Idee liegt nicht in der Anpassung des IDM-Systems oder der Etablierung von standardisierten IDM-Prozessen, deren Adaptierung an Geräte statt an natürliche Personen erfolgt, sondern an der Integration von unternehmensweiten Prozessen, um die vom IDM-Prozess vorgegebenen Maßnahmen überhaupt umsetzten zu können. Um das Beispiel von oben aufzugreifen: Ein Gerät scheidet aus und die Kommunikation des Geräts soll mit Hilfe einer Firewall unterbunden werden. Existiert in dem Unternehmen bereits ein Prozess oder ein Vorgehen, um solch eine Anforderung umzusetzen? Wenn man sich für den Einsatz eines IDM-Systems für die Verwaltung

seiner IoT Geräte entscheidet, wird man sich sehr schnell mit einer Vielzahl solcher Fragen konfrontiert sehen. Und genau diese Fragen, deren Antworten und die Umsetzung der daraus resultierenden Anforderungen machen die Schwierigkeit aus.

8.6 Schnittstellen erleichtern das Leben

Bei der Einführung und Etablierung von Prozessen und Vorgehensweisen im Unternehmen werden IDM-System-Betreiber bald auch mit Fragen zu verschiedensten, auch neuartigen Schnittstellen, konfrontiert werden. Soll zum Beispiel ein Eintrag in der Firewall zur Aussperrung eines Gerätes erfolgen, kann geprüft werden, ob das IDM-System eine E-Mail mit der Aufgabe an einen Administrator schickt oder dem IDM-System beigebracht werden, diesen Eintrag selbst vorzunehmen. So eine Schnittstelle gehört nicht unbedingt zum Standard Out-of-the-box Repertoire eines IDM-Systems. Nichtsdestotrotz erleichtern solche Schnittstellen die tägliche Arbeit ungemein. Die Entwicklung neuartiger Schnittstellen stellt somit auch eine Herausforderung dar.

8.7 Zusammenfassung

Zusammengefasst kann man sagen, dass die Idee, Geräte des IoT mit einem IDM-System zu verwalten, relativ gut umsetzbar ist. Es setzt aber einen starken Partner voraus, der sich in der Identitäten- und Zugriffs-Verwaltung bestens auskennt und sich auch in der Welt des IoT zurechtfindet. Fehlende Prozesse und Standards müssen durch Erfahrung und Expertise im Unternehmen geschaffen und etabliert werden. Nur so kann für das jeweilige Unternehmen und den jeweiligen Einsatzzweck die beste Lösung gefunden und vielleicht eine eigene Definition von IoT formuliert werden.

9 Fazit

Es gibt keine allgemein gültige Definition für IoT. Deswegen ist es wichtig, dass jedes Unternehmen für sich definiert, was es mit IoT meint, was es genau darunter versteht und welchen Einsatzzweck das Unternehmen für IoT sieht.

Da die Maschinen/Dinge noch nicht in der Lage sind, mittels einer einheitlichen Sprache zu kommunizieren, existiert heute noch kein einheitlicher Standard im Bereich IoT. Jeder Einsatz von IoT ist einzigartig und muss anhand von Erfahrungswerten erarbeitet werden können.

Noch kann keiner sagen, welche Entwicklung das IoT macht. Es bleibt abzuwarten, ob die Industrie der Idee eines gemeinsamen Standards folgen wird. Angesichts des riesigen Erfolgspotentials ist jedoch zu befürchten, dass viele Unternehmen nach wie vor ihr eigenes Süppchen kochen werden, um schnellstmöglich Profit abzuschöpfen und eine Abhängigkeit ihrer Kunden zu schaffen.

Dabei dürfen die Gefahren, welche IoT mit sich bringt nicht ausser Acht gelassen werden. In Punkto Sicherheit und Wahrung der Privatsphäre gilt es, Vorsicht walten zu lassen und die notwendigen Vorkehrungen für die (Daten-)Sicherheit zu gewährleisten. Umso wichtiger ist es, sich mit der ganzen Thematik IoT intensiv zu befassen und den Markt und vor allem eventuell aufkommende Standards genau zu beobachten. Das erfolgreiche Umsetzen von Vorhaben und Projekten gelingt dann umso besser, wenn mit einem starken Partner gerechnet werden kann, der Know-how aus dem eigenen Bereich mitbringt und hilft die eigenen Anforderungen erfolgreich zu erfüllen.

10 Glossar

Cyber-Physische Systeme (CPS)
Diese eingebetteten Systeme mehrerer technischer Anlagen sind miteinander vernetzt und können so ihre jeweiligen Abläufe untereinander koordinieren.

Embedded Systems
Dies sind meist recht kompakte Computer, die in anderen technischen Anlagen (Fahrzeuge, Produktionsmaschinen) eingebaut sind und diverse Funktionen der Anlagen steuern.

Digitalisierung
Umwandlung von Informationen von einem analogen in ein digitales Format. In der «Dritten industriellen Revolution» wurde Digitalisierung geboren. Aus diesem Grund wird Digitalisierung gerne im Rahmen von «Industrie 4.0» erwähnt, da man die in analoger Form durchgeführten Schritte eines Wertschöpfungsprozesses in eine digitale Form bringen möchte.

IED (Intelligent Electronic Device)
Hierbei handelt es sich um Geräte in einem Smart Grid, die Daten von Sensoren verarbeiten und automatisch Schritte zur besseren Lastenverteilung einleiten.

Internet of Everything
Dies ist lediglich ein anderer Begriff für das Internet der Dinge. Cisco nutzt ihn für Marketingzwecke, um seine IoT-Konzepte und Lösungen von der Konkurrenz abzuheben.

Industrie 4.0
Der in Deutschland geprägte Begriff beschreibt die weitergehende Automatisierung und Individualisierung von Produktionsprozessen mit Hilfe von IoT-Technologien. Die Produktionsmaschinen werden zu Cyber-Physischen Systemen, die autonom den Fertigungsprozess steuern. Industrie 4.0 ist eine von der Deutschen Regierung unterstützte Strategie. Ähnliche Strategien gibt es in anderen europäischen Ländern. Der Begriff «Industrie 4.0» ist im Ausland nahezu unbekannt.

Maschine-zu-Maschine-Kommunikation (M2M)
Maschinen und Anlagen tauschen automatisch untereinander Informationen aus, um sich autonom zu regulieren und dafür notwendige Prozesse einzuleiten. Ein Beispiel: Ein Fertigungsroboter signalisiert der Leitstelle den Verschleiß von Bauteilen. Die Leitstelle bestellt daraufhin ohne menschlichen Eingriff Ersatzteile und passt den Produktionsprozess so an, dass der beschädigte Fertigungsroboter geschont wird.

Pervasive Computing
Alle Rechner und Sensoren sind miteinander vernetzt und werten permanent Daten über den Menschen und die Umgebung aus. Sie werden dabei von Menschen häufig nicht mehr als eigenständige Objekte wahrgenommen. Man spricht auch von "Rechnerdurchdringung".

Smart Objects
Intelligente Objekte bilden die Grundlage für das Ubiquitous Computing und das Internet der Dinge. Es sind Gegenstände, deren ursprüngliche Funktion dank eingebauter Sensoren, Mikroprozessoren und Netzwerkadaptern (zum Teil) erweitert wurde.

Ubiquitous Computing
Dieser Begriff wird ins Deutsche auch mit "allgegenwärtige Rechner" übersetzt. Die Rechner sind überall zu finden und unterstützen den Menschen bei seinen täglichen Aufgaben. Durchaus sind sie auch in anderen Gegenständen eingebaut. Ubiquitous Computing ist eine Voraussetzung für Pervasive Computing.

11 Verwendete Quellen:

[1] https://www.expertenderit.de/blog/iot-definitionen-was-ist-eigentlich-das-internet-der-dinge

[2] https://de.wikipedia.org/wiki/Internet_der_Dinge

[3] https://www.bundestag.de/blob/192512/cfa9e76cdcf46f34a941298efa7e85c9/internet_der_dinge-data.pdf

[4] http://wirtschaftslexikon.gabler.de/Definition/internet-der-dinge.html

[5] http://www.faz.net/aktuell/wirtschaft/cebit/cebit-was-eigentlich-ist-das-internet-der-dinge-13483592.html

[6] http://www.itwissen.info/Internet-of-things-IoT-Internet-der-Dinge.html

[7] https://digitaler-mittelstand.de/trends/ratgeber/internet-der-dinge-eine-kurze-definition-mit-4-beispielen-20287

12 Porträt

12.1 Mihael Zadro

Mihael Zadro verfügt über umfangreiche und mehrjährige Erfahrungen aus dem Bereich Testmanagement und befasst sich seit knapp acht Jahren mit dem Thema Identity & Access Management. Seit 2014 ist Mihael Zadro IAM Business Consultant bei der IPG-Gruppe und unterstützt Unternehmen in der Beratung, Umsetzung und Einführung kundenspezifischer IAM-Lösungen.

12.2 IPG-Gruppe

Die IPG-Gruppe ist auf die Konzeption, Integration, den Betrieb und die Ausbildung von IAM-Lösungen spezialisiert. Das Unternehmen, gegründet 2001 in Winterthur, bietet inzwischen auch in den Niederlassungen in Deutschland und Österreich Lösungen für den umfassenden Schutz von Benutzerdaten sowie Zugriffsrechten. Zu den Kunden zählen Unternehmen aller Branchen wie auch Organisationen der öffentlichen Verwaltung. IPG ist bevorzugter Partner für bedeutende Software-Hersteller in der Schweiz, Deutschland und Österreich und beschäftigt über 60 Mitarbeitende. www.ipg-group.com