High-Level-Risikoanalyse im Bereich Internet of Things

Stefan Schiebeck · Sandra König
Stefan Schauer · Martin Latzenhofer

Austrian Institute of Technology
Center for Digital Safety & Security
{stefan.schiebeck | sandra.koenig
stefan.schauer | martin.latzenhofer}@ait.ac.at

Zusammenfassung

Das Internet of Things (IoT, zu Deutsch „Internet der Dinge“) ist einerseits durch eine hohe Komplexität, andererseits durch eine rasante Entwicklung bedingt durch das Zusammenwachsen von Informations- und Kommunikationstechnologie (IKT) mit intelligenten Sensorikanwendungen und immens hohem Anwendungspotential geprägt. Aktuell ist es ein vordringliches Ziel, das IoT-Anwendungsfeld durch Architekturansätze zu strukturieren, die es erlauben, eine transparente Entwicklung bei gleichzeitiger Einhaltung von Mindestkriterien für die Informationssicherheit sicherzustellen. Ein kritischer Erfolgsfaktor hierfür ist die Integration von Informationssicherheitsgrundsätzen bereits in der Designphase, anstatt diese nachträglich als Add-on einzuarbeiten. Im Rahmen des FFG FIT-IT-Projekts RISIoT[1] wird eine praktikable Einteilung und IoT-Risikolandkarte entwickelt, die neben dem aktuellen Stand der Literatur ExpertInnen-Knowhow aus unterschiedlichen Branchen berücksichtigt. Dieser Beitrag entwickelt dazu 14 Anwendungsdomänen und leitet diesbezügliche High-Level-Risiken ab, die sich in einer Risikomatrix übersichtlich visualisieren lassen. Eine Priorisierung ermöglicht so eine stärkere Fokussierung der momentanen Aktivitäten von Wissenschaft, Forschung und Industrie auf die nächsten Entwicklungsschritte und den aktiv-konstruktiven Umgang mit der aufgekommenen Komplexität.

1 Motivation

In den letzten Jahren ist der Begriff Internet of Things (IoT, im Deutschen „Internet der Dinge“) immer mehr in den Fokus der Öffentlichkeit gerückt. Dies beinhaltet auch Forschungsprojekte wie die von der FFG (Österreichische Forschungsförderungsgesellschaft mbH) geförderte Studie RISIoT[1], welche im Herbst 2016 gestartet wurde. Ziel dieser Studie ist es, einen Überblick über IoT-spezifische High-Level-Risiken zu erarbeiten sowie darzustellen, welche Faktoren den Einsatz von IoT in Österreich bremsen oder hemmen können.

Trotz der erhöhten öffentlichen Aufmerksamkeit fehlt ein einheitliches Verständnis dieses Begriffs „Internets der Dinge“. Eine Definition des Institute of Electrical and Electronics Engineers (IEEE), die dem intuitiven Verständnis nahe kommt, beschreibt IoT als ein „*Netzwerk von Dingen – ausgestattet mit Sensoren – welche mit dem Internet verbunden sind*“ [Isac15, selbst

[1] RISIoT – “Market analysis and risk assessment to accelerate the adoption of the Internet of Things in Austrian enterprises”

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 213-224.

übersetzt]. Noch unübersichtlicher ist die Verortung des Begriffs IoT im Spannungsfeld der Informationssicherheit. Das Hauptproblem dabei ist, dass Sicherheitsaspekte bei der Entwicklung von IoT-Systemen kaum berücksichtigt wurden und auch heute noch das Bewusstsein für mögliche Risiken sehr unterschiedlich ausgeprägt ist. Angesichts dieser Probleme ist es wenig überraschend, dass einheitliche Standards und Architekturmodelle für IoT momentan noch nicht in einer angemessenen Detailtiefe vorhanden sind. Bestehende Ansätze sind nicht zuletzt aufgrund der herrschenden Komplexität meist domain-spezifisch; beispielsweise fokussiert sich das Referenzarchitekturmodell Industrie 4.0 [Plat17] speziell auf Logistik. Eine einheitliche Charakterisierung von IoT erweist sich aufgrund der Vielfältigkeit der möglichen Anwendungen als schwierig. Diese reichen vom Gesundheitswesen über Informations- und Kommunikationstechnologie (IKT), Energie, Sport und Militär bis hin zu zahlreichen Smart-Anwendungen in den Bereichen Wohnen und Leben [Iso14]. Einige dieser Anwendungsgebiete sind durch mehr oder weniger erfolgreiche Attacken in den Fokus der Öffentlichkeit gerückt, etwa durch einen medienwirksamen Angriff auf die Deutsche Telekom [Chaz16]. Gemäß einer aktueller Studie, welche die Analysen von Firmen wie Cisco, Ericsson, Gartner, IDC, Harbor Research, ABI Research, GE und McKinsey zusammenfasst, wird erwartet, dass bis 2020 die Anzahl verbundener Geräte die 50-Milliarden-Marke erreichen wird [Knud17]. Dies wird die bereits jetzt sichtbaren Probleme verschärfen und neue entstehen lassen. Im Fokus wird dabei neben der Analyse der anfallenden Datenmengen (z.B. durch Big Data) vor allem auch die Interoperabilität der verschiedenen verwendeten Technologien aber auch der Konzepte (insbesondere der Architekturen) stehen. Ein wesentlicher Bestandteil einer angestrebten Standardisierung wird die Entwicklung einer einheitlichen Terminologie sein.

Der vorliegende Artikel gibt einen Überblick über die unterschiedlichen Risiken im Zusammenhang mit IoT. Aufgrund der oben beschrieben Breite der Anwendungsbereiche für IoT und der damit einher gehenden Fülle an möglichen Bedrohungsszenarien bleibt dieser Überblick dabei bewusst auf einer generischen Ebene. Vorrangiges Ziel dabei ist, eine stimmige Kategorisierung der Risiken durchzuführen. Dabei unterscheidet die Einteilung zwischen 14 Hauptanwendungsgebieten sowie sechs High-Level-Risiken. Auf Basis dieser generischen High-Level-Risiken, die sich entsprechend für die unterschiedlichen Anwendungsgebiete konkretisieren lassen, wird eine Risikomatrix erstellt, welche die Wichtigkeit und eine notwendige Priorisierung der Risiken reflektiert.

2 Domänen und Anwendungsfälle

Wie im vorherigen Abschnitt bereits erwähnt, gibt es aktuell keine einheitliche Sicht auf das Thema IoT. Die International Standardization Organization (ISO) versucht als eine der ersten Organisationen mit der ISO 30141 (aktuell nur in einer Entwicklungsversion aus dem Jahre 2016 [Iso16] verfügbar) einen Überblick über die verschiedenen Domänen zu schaffen, in denen das IoT-Konzept eingesetzt wird. Dabei wurden *14 Domänen* identifiziert, welche von IKT und Smart Cities über den Finanz- und Banken- sowie den Transportsektor bis hin zur öffentlichen Sicherheit reichen, wie Abbildung 1 darstellt. Im Folgenden werden diese kurz beschrieben und durch Berichte über Vorfälle aus diesen Fachbereichen ergänzt.

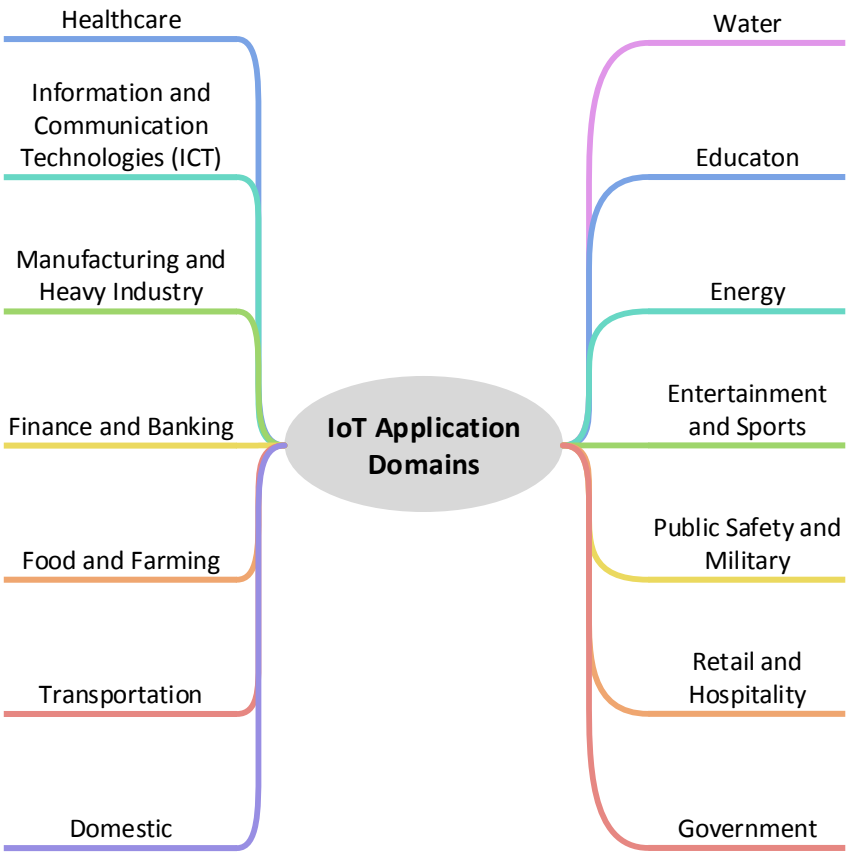

Abb. 1: IoT-Anwendungsdomänen und -fälle [Iso14]

- **Gesundheitswesen**
  Anwendungsfälle: Ferndiagnose, -überwachung und -behandlung, Tracking von Medikamenten inklusive kryptographischer Sicherheitsmaßnahmen für Fälschungssicherheit, Arzneimittel- und Krankenaktenmanagement, Mehr-Sprachen-Unterstützung sowie erweiterte Zugriffsmöglichkeiten, Schnittstellen für Menschen mit Behinderungen.
  Medienwirksame Ereignisse in dieser Domäne betreffen z.B. die Manipulation von Herzschrittmachern, welche u. A. per Fernsteuerung ermöglichen, dem Patienten einen Schock von 830 Volt zu verabreichen [Kirk12], sowie die „WannaCry“ Ransomware-Infektionen, welche neben üblichen IKT-Systemen auch einige medizinische Geräte in über 40 Krankenhäusern verschlüsselten [Cimp17].
- **Informations- und Kommunikationstechnik (IKT) Industrie**
  Anwendungsfälle: Geräte-Inventarisierung und -Tracking, automatisiertes Netzwerkmanagement inklusive Fernwartung, physikalische Überwachungsmaßnahmen für (Licht-)Leitungen, Verteilerpunkte, unabhängigen Stromversorgungen (USV) und Zugriffskontrollmechanismen.
  Im November 2016 wurde versucht die Kabel-Breitband-Router der Kunden der Deutschen Telekom AG zu übernehmen [Chaz16] und als Teil des Mirai-Botnets zu verwenden. Aufgrund einer Fehlkonfiguration des Angriffscodes kam es lediglich zu tagelangen Ausfällen von insgesamt 900.000 der 20 Millionen Endgeräte.
- **Produktion und Schwerindustrie**

Anwendungsfälle: Inventar-, Prozess-, Equipment-, Produktions-, Safety-Überwachung und -Management, Defekt- und Rückruf-Management inklusive vorausschauendem Service-Management basierend auf Big Data Analytics, Produkt-Service-Bündelungen[2], Zugriffskontrolle für Arbeiter und Lieferanten.
Die Produktionsgüterindustrie ist laut IBM's Cyber Security Intelligence Index [Ibm16] aktuell eine der am häufigsten gehackten Branchen. Die üblichen Sicherheitsvorfälle betreffen Wirtschaftsspionage, Ransomware und Social-Engineering-Angriffe, wie z.B. das „Fake-President"-Schema.

- **Finanzwesen und Bankwesen**
  Anwendungsfälle: Point-of-Sale (POS) Terminals, fern-identifizierbare Geldautomaten, allgemeine Erweiterung der Service-Funktionalitäten für Desktops und mobile Endgeräte, Produkt-Service-Bündelungen im Kontext von Versicherungen und Kreditvergaben[3].
  Aufgrund des intrinsischen Wertes der Finanzindustrie wird die Branche vermutlich langfristig ein interessantes Ziel für Angreifer bleiben. Ein kürzlich erschienener Bericht [Seal16] zeigt sogar das Potential auf, mit Hilfe von Cyberangriffen das Finanzsystem eines Landes zu destabilisieren.
- **Lebensmittel und Landwirtschaft**
  Anwendungsfälle: Überwachung chemischer und umgebungsbezogener Bedingungen, Produktions- und Nutztier-Überwachung, Qualitäts- und Defekt-Management von verarbeiteten Nahrungsmitteln, Ablauf- und Abfallmanagement, Automatisierungen im Bereich Nahrungsmittelbestellung und -lieferung.
  Ein Bericht bezüglich der internationalen Einführung von IoT-Konzepten im Bereich der Smart und Connected Farms zeigt Kosten- und Produktionsoptimierungspotentiale auf und schätzt die Auswirkungen bis zum Jahr 2050 auf eine Zunahme der Lebensmittelproduktion von 70 Prozent. Die Möglichkeiten der lückenlosen Überwachung der Produktion, Verarbeitung und Verteilung innerhalb der gesamten Lieferkette werden in Zukunft helfen, Risiken durch Lebensmittelbetrug zu minimieren.
- **Transport**
  Anwendungsfälle: unterstütze/autonome Fahr-Technologien für Züge, Flugzeuge, Automobile, Schiffe und Raumfahrzeuge, dynamische Verkehrsleitsysteme[4], Verkehrswegüberwachung inklusive vorausschauende (predictive) Instandhaltung, Vehicle-to-Vehicle-Kommunikation (V2V).
  Bereits 2008 geling es einem Kind mit Hilfe einer Infrarotfernbedienung Zug-Weichensysteme zu manipulieren und so vier Züge entgleisen zu lassen [Knop08], obwohl diese damals noch nicht an das Internet angebunden waren. Einem Bericht aus dem Jahr 2015 über entdeckte Schwachstellen in 471.000 Automobil-Entertainment-Systemen [Gree15], welche die Fernverwaltung von Dashboard-Funktionen, Lenkung, Beschleunigungs- und Bremssystem sowie der Schaltung erlauben, folgte der erste Bericht über einen Todesfall aufgrund einer Fehlfunktion des Automobil-Autopiloten Mitte 2016 [Gols16]. Berichten

[2] z.B. ein Service, das es dem Sofa erlaubt zu erkennen, wenn die Schlüssel in den Spalt gerutscht sind.

[3] z.B. können intelligente Kraftfahrzeuge Daten bzgl. Nutzerverhalten an Versicherungsunternehmen übertragen um – auf Wunsch des Kunden – risikobasierte Prämien zu ermöglichen. Das gleiche Konzept kann natürlich für Health- und Fitness-Tracker eingesetzt werden.

[4] z.B. Verkehrsampeln die auf Umfeldbedingungen reagieren.

zufolge gelang es einem Cybersecurity-Berater, ebenfalls in die Steuersysteme eines Passagierflugzeuges einzudringen und die Kontrolle über die Turbinen zu erlangen [Pere15].

- **Wohnen**
  Anwendungsfälle: automatisierbare Heizung, Belüftung und Klimatisierung, Beleuchtungsmanagement, Leck Detektion, Rauch- und Kohlenmonoxid-Melder, Alarmanlagen und Überwachungssysteme, Intelligente Haushaltsgeräte, Energiesystem-Management.
  Der vermehrte Einsatz von IoT-Produkten im häuslichen Bereich führte bereits mehrfach zu Problemen, u. A. gab es Berichte über Schwachstellen in Babyfonen [StBe15], über IoT-Produkte mit Datenschutzbedenken [HiPK16] sowie über großflächig angelegte Distributed-Denial-of-Service-(DDoS)-Angriffe [Kreb16].
- **Wasser**
  Anwendungsfälle: Fernwartung, Überwachung und automatische Aufbereitung von Trinkwasser, Korrosionsschutz, Sediment-Management.
  Einem anonymisierten Bericht von Verizon zufolge kam es 2016 zu einer erfolgreichen Kompromittierung der Steuersysteme eines Wasserwerkes [Kova16], bei dem Einstellungen der Wasserverteilung und -behandlung manipuliert wurden. Forscher der Universität von Georgien zeigten zudem die Möglichkeiten von Ransomware auf, kritische Infrastrukturen zu infizieren und Lösegeldforderungen zu stellen [Kris16].
- **Ausbildung**
  Anwendungsfälle: Augmented Reality/Virtual Reality, Fernunterricht, Zugriff auf Live-Daten (z.B. Sattelitenbilder, Wetterdaten, marine Sonden, etc.).
  Ein chinesischer Spielzeugkonzern wurde 2015 Oper einer Cyberangriffes, bei dem die personenbezogenen Daten von fünf Millionen End-Anwendern von (Lern-) Spielzeug, sowohl jene der Eltern als auch der Kinder, gestohlen wurden [Lui15].
- **Energie**
  Anwendungsfälle: Koordination von Energieerzeugung, -verteilung, -speicherung und -verbrauch durch Überwachungs- und Steuermöglichkeiten der Netzkomponenten (Smart (Energy) Grid).
  Durch den Aurora Generator Test wurde bereits 2007 gezeigt, dass Cyberangriffe das Potential haben, Teile eines Stromnetzes oder Netzkomponenten physisch zu zerstören [Mese07]. Der erste medienwirksame Vorfall ereignete sich 2010 mit der Malware Stuxnet [Kush13], mit dessen Hilfe Zentrifugen manipuliert wurden, um das iranische Atomprogram zu sabotieren. Im Jahr 2016 wurden die Betreiber des westukrainischen Stromnetzes Oper eines Cyberangriffes [Zett16], bei dem über 230.000 Menschen für mehrere Stunden vom Stromnetz getrennt wurden. Sogar mehrere Monate nach diesem Vorfall müssen Teile der Systemkomponenten immer noch manuell bedient werden, da Angreifer die Firmware kritischer Komponenten gebrickt[5] haben.
- **Unterhaltung und Sport**
  Anwendungsfälle: Augmented Reality/Virtual Reality, Tourismus-Anwendungen (Mehrsprachigkeit, Navigation, etc.), Ticket- und Eintritts-Management, Spielerstatistiken sowie Gesundheits-, Equipment und Material-Informationen.
  Aufgrund der hohen Anzahl an Unterhaltungsgeräten können diese für DDoS-Angriffe verwendet werden, wie bereits 2016 gezeigt wurde [Kreb16]. Ebenfalls können potentielle Beeinträchtigungen des Datenschutzes entstehen, wie durch eine Empörungswelle in

[5] Bricken bedeuten ein elektronisches Gerät dauerhaft unbenutzbar zu machen (useful as a brick).

Verbindung mit Samsungs Smart-TV-Datenschutz-Policy gezeigt wurde [Whit16]. Die Anwender wurden informiert, keine persönlichen Gespräche in der Nähe des Fernsehgerätes zu führen, da das Mikrofon des Gerätes zur Optimierung der Sprachsteuerung potentiell sämtliche Raumgeräusche aufzeichnen und an Dritte versenden könnte.

- **Öffentliche Sicherheit und Militär**
  Anwendungsfälle: Grenz- und Perimeterüberwachung und -schutz, Asset-Tracking und Lokalisierung, Asset-Fernsteuerung (z.B. Roboter, Drohnen, etc.), Waffen-Tracking und -Identifikation, Katastrophenmanagement.
  Die Notwendigkeit von Cybersicherheit im militärischen Kontext wurde einerseits durch Sicherheitsvorfälle wie die versuchte Infiltration der südkoreanischen Cyber-Kommandozentrale [Paga16], andererseits durch proaktive Kampagnen wie das „Hack my Army"-Programm der US Regierung [Hack16] unterstrichen. Aufgrund der kostengünstigen Verfügbarkeit von Drohnen am Verbrauchermarkt kam es in der Öffentlichkeit bereits zu unterschiedlichen Sicherheitsvorfällen, von Datenschutzproblemen bis zu Kollisionen mit Flugzeugen. Drohnen können zudem in Verbindung mit RF-Transmittern[6] eingesetzt werden, um größere geografische Bereiche und deren IoT-Geräte automatisiert zu mappen.
- **Einzelhandel, Gastgewerbe und Beherbergung**
  Anwendungsfälle: Inventar-Management und -Logistik, standortbezogene und benutzerbezogene Werbung, Sicherheitsmaßnahmen gegen Diebstahl und Betrug, Facility-Management und -Überwachung.
  Wie aus anderen Domänen bekannt, erfolgen Angriffe hier meist mit Hilfe von präparierten E-Mails (Malware, Fake-President, etc.). Beispielsweise wurden 2016 Point-of-Sale-Terminals in über 350 Geschäftsstellen des Einzelhandelsunternehmens Eddie Bauer mit Malware infiziert, welche über Monate hinweg Kreditkarten-Daten der Kunden an die Angreifer weiterleiteten [Vija16].
- **Staat**
  Anwendungsfälle: eGovernment-Anwendungen, Authentisierungs- und Zahlungssysteme, Asset-Tracking und -Management, Zustelldienste, Überwachung der Luft- und Wasserqualität, Wasser- und Kanalisations-Netz-Überwachung und -Steuerung, Facility-Management, Eigentumsmanagement und -instandhaltung.
  Aufgrund mehrerer Sicherheitsvorfälle wurden seit des US-Wahlsieges von Donald Trump Mutmaßungen darüber angestellt, dass die US-Wahl mit Hilfe von Cyberangriffen durch Russland indirekt manipuliert wurde [Fish16] (Hillary-Clintons-Email-Affäre).

3 Charakteristika und High-Level-Risiken

Trotz unterschiedlicher Einsatzgebiete von IoT-Produkten teilen diese einige neuartige Charakteristika und damit verbundene Risiken. Dazu gehört insbesondere der Einsatz in unsicheren oder exponierten Umgebungen, welcher Angreifern physischen Zugriff ermöglicht (z.B. im Falle von Smart Meter). Damit wird einem Angreifer erlaubt, Hardware-Komponenten mit verschiedenen Reverse-Engineering-Methoden zu analysieren, Geheimnisse (z.B. Passwörter) oder Schwachstellen in der Software zu identifizieren und auszunutzen. Zudem verfügen viele

[6] Radio-Frequency-Transmitter für standardisierte Protokolle wie z.B. WLAN, Bluetooth, ZigBee, Low-Power RF, etc.

IoT-Produkte über sehr eingeschränkte Ressourcen. Die Vorsitzende der Federal Trade Commission warnte vor kurzem davor, dass die geringe Größe und damit limitierte Leistungsfähigkeit vieler vernetzter Geräte den Einsatz von kryptographischen Methoden und anderen Sicherheitsmaßnahmen behindert. Auch die Aktualisierungsmöglichkeiten von billigen, zum Teil sogenannter „Wegwerf-IoT-Produkten", seien unzureichend oder schlichtweg nicht vorhanden [Rang15].

Das Fehlen internationaler Standards und Referenzmodelle erschwert außerdem die Auswahl geeigneter Architekturen, Software- und Hardware-Plattformen, Kommunikationsprotokolle, technischer Sicherheitsmaßnahmen und Entwicklungsprozesse. Diese führt zu Kompatibilitätsproblemen zwischen Technologien und Protokollen. Die Tatsache, dass Informationssicherheit in vielen Fällen kein primärer Geschäftstreiber ist, erschwert zudem die Entwicklung sicherer IoT-Produkte, zumal das Prinzip Time-to-Market einen wesentlich höheren Einfluss auf die Etablierung eines Produktes hat als Sicherheitsaspekte. Diese Charakteristika führen direkt oder indirekt[7] zu unterschiedlichen High-Level- oder Folge-Risiken wie in Abbildung 2 dargestellt. Die wichtigsten identifizierten High-Level-Risiken [Clou16] werden kurz beschrieben.

- **Unzureichende Sicherheitsmaßnahmen, potentiell flächendeckend angreifbar:** Bei Unternehmen, die IoT Produkte entwickeln, steht oft die rasche Produktion sowie die einfache Handhabung des Produkts im Vordergrund. Regeln welche die Produkte sicherer machen (z.B. Risikoanalysen, sichere Softwareentwicklungsverfahren, etc.) werden daher selten verwendet oder nur teilweise umgesetzt. Gerade bei kleineren Unternehmen fehlt oft das Bewusstsein für potentielle Risiken von IoT-Produkten. In vielen Fällen kann dies zu Schwachstellen führen, welche potentiell flächendeckend ausgenutzt und entsprechende Folgerisiken entstehen können.
- **Beeinträchtigung des Datenschutzes:** Sammeln IoT-Produkte Informationen über den Nutzer, verfügen über GPS, Kamera, Mikrofon oder ermöglichen die Daten Verhaltensanalysen, so können entsprechende Datenschutzrisiken für die Betroffenen entstehen.
- **Beeinträchtigung von Safety-Aspekten:** Verfügen IoT-Produkte über Aktuatoren (Cyber Physical Systems) oder anderweitig manipulierbare Elektronik (z.B. Akku-Ladestrom, CPU-Spannung, etc.), so können potentiell Safety-Aspekte, z.B. durch physische Zerstörung oder Brand, beeinträchtigt werden.
- **Missbrauch für DDoS-Angriffe:** Günstige IoT-Produkte erhöhen außerdem die Wahrscheinlichkeit, dass eine Software- oder Hardware-Schwachstelle gefunden und flächendeckend ausgenutzt wird. Durch eine große Verbreitung solcher günstigen (und einfach zu kompromittierenden) IoT-Produkte bieten sich Angreifern auch die Möglichkeit, mit einfachen Mitteln große Bot-Netzwerke aufzubauen und für ihre Zwecke zu nutzen.
- **Einsatz von Drohnen zur flächendeckenden Identifikation von IoT-Produkten**
  Sind IoT-Produkte einfach in der Installation, d.h. lassen sich diese einfach finden und konfigurieren, so kann dies auch über geringfügig größere Entfernungen (außerhalb der eigenen Wohnräume) mit entsprechenden Radio-Frequency-Empfängern, montiert auf

[7] Unter „indirekten" Risiken werden hier Folgerisiken verstanden, d.h. potentielle Auswirkungen, die sich aufgrund der direkten Risiken ergeben können. Der mögliche Einsatz von IoT-Produkten in unsicheren und/oder physikalisch exponierten Umgebungen führt (direkt) zu potentiell flächendeckend angreifbaren Produkten aufgrund unzureichender Sicherheitsmaßnahmen. Indirekt (d.h. als Resultat eines erfolgreichen Angriffes) können dadurch Datenschutz-, Safety-Aspekte etc. beeinträchtigt werden.

adaptierten Drohnen, geschehen. So ist es möglich, sehr kommunikationsfreudige Geräte auf engem Raum (z.B. eng bebaute Stadtteile) effizient zu identifizieren und in weiterer Folge anzugreifen.

- **Interferenz mit kritischen Infrastrukturen**
  Je nach Use-Case, Anzahl und Leistungsfähigkeit der IoT-Produkte und ausgenutzter Schwachstelle können in weiterer Folge potentiell Interferenzen mit kritischen Infrastrukturen entstehen (z.B. Manipulation von Smart-Metern, DDoS-Angriffe, etc.).

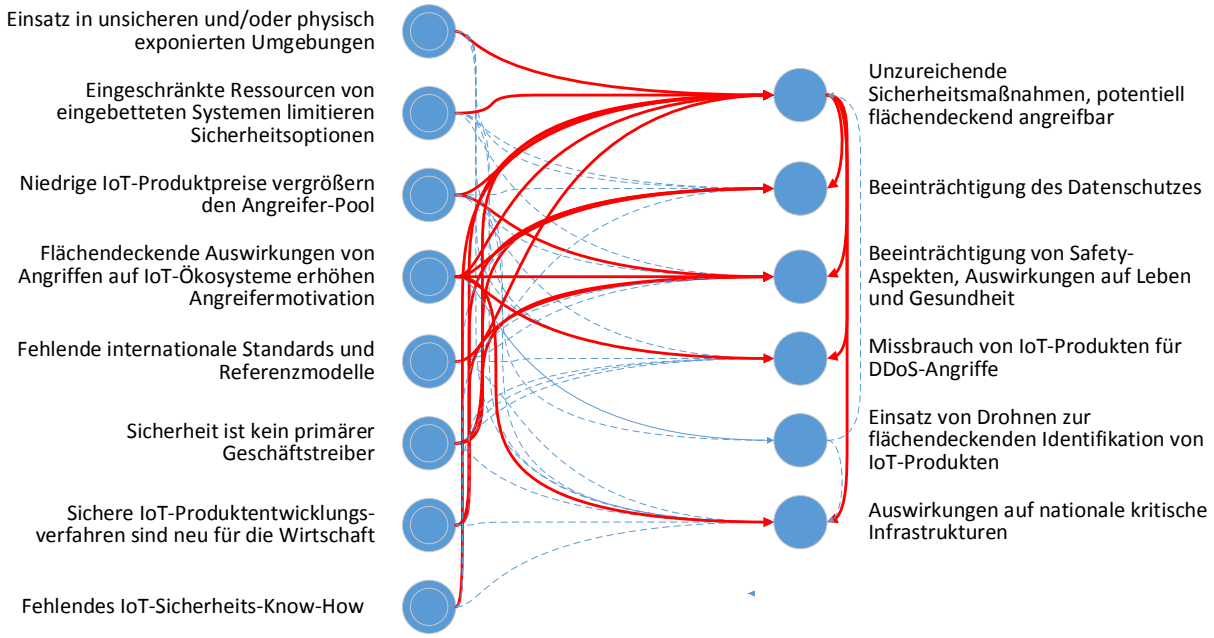

Abb. 2: IoT-Charakteristika und deren direkte (durchgezogene Linien) und indirekte (gestrichelte Linien) Risiken und Folgen

Diese High-Level-Risiken [Csa16] lassen sich in weiterer Folge mit allen in Abschnitt 2 vorgestellten Domänen in Beziehung setzen und entsprechend in einer High-Level-Risikomatrix darstellen (siehe Abbildung 3). Somit wird ein Überblick über die Risiken mit der höchsten Priorität für die einzelnen Domänen erlangt. Die Risiko-Matrix richtet sich dabei vor allem an österreichische Unternehmen, die IoT einsetzen möchten und einen ersten Eindruck von potentiellen Risiken erhalten wollen, als auch an Ministerien und regierungsnahe Organisationen, die vermehrt mit Sicherheitsfragen im Kontext IoT in Kontakt kommen. Dabei wird zu Gunsten eines sektorenübergreifenden Überblicks bewusst auf eine detailliertere Analyse für jeweilige Domänen verzichtet, da die Rahmenbedingungen der einzelnen Unternehmen zu unterschiedlich sind.

Sowohl in Bezug auf Eintrittswahrscheinlichkeit als auch auf die Auswirkungen der Risiken in den verschiedenen Domänen wurden die Einschätzungen im Zuge eines Workshops mit Experten aus dem Projekt RISIoT erarbeitet. Um für die Bewertung eine allgemeine Basis zu verwenden, wurde eine sechststufige, qualitative Skala verwendet, welche in einer Studie aus dem Jahr 2015 gemeinsam mit mehreren Ministerien erarbeitet wurde [SPLS15]. In Bezug auf die Eintrittswahrscheinlichkeit bewegt sich diese Skala von „äußerst unwahrscheinlich“ bis äußerst wahrscheinlich“ und in Bezug auf die Auswirkungen von „unbedeutend“ bis „schwerwiegend“. Für die Erstellung der High-Level-Risikomatrix wurden für diese Stufen keine konkreten Schwellwerte hinterlegt, sondern die Risiken relativ zueinander bewertet. Für eine detailliertere

Bewertung können jedoch domänenspezifische Werte für die jeweiligen Stufen herangezogen werden.

In der Risikomatrix aus Abbildung 3 ist eine Korrelation zwischen Eintrittswahrscheinlichkeit und Auswirkung zu erkennen. Dies liegt unter anderem daran, dass eine Bewertung des Schadens oft aus der Sicht des Angreifers erfolgt und vom Worst-Case-Schaden ausgeht. Unsicherheiten bezüglich der Auswirkungen tragen ebenfalls dazu bei, dass im Zweifel der erwartete Schaden als hoch eingeschätzt wird.

4 Conclusio

Das Internet der Dinge ist aktuell in einer Vielzahl von Bereichen zu finden und zahlreiche Produkte, Systeme und Technologien werden unter dem „Label“ IoT auf den Markt gebracht. Durch diese Fülle an unterschiedlichen Systemen und Technologien ist es nicht nur schwierig, eine einheitliche Definition für das Internet der Dinge zu geben, sondern auch eine vom Anwendungsbereich unabhängige Informationssicherheitsarchitektur für IoT-Produkte zu erstellen. Dadurch ist ein Großteil der aktuellen IoT-Systeme offen gegenüber einer Vielzahl von Angriffen. Die meisten Nutzer sowie auch viele der Hersteller sind sich dieser Bedrohungen und der damit verbundenen Risiken jedoch nicht bewusst.

In diesem Artikel wird eine High-Level-Risikomatrix präsentiert, die einen groben Überblick über generische Risiken im IoT-Umfeld geben soll. Primäres Ziel ist es dabei nicht, eine detaillierte Risikoanalyse für eine Technologie oder einen Anwendungsbereich zu erhalten, sondern ein allgemeines Bewusstsein in Bezug auf alle Risikofelder im Zusammenhang mit IoT zu stimulieren. Die Einordnung der Risiken in einer Risikomatrix, die nach Auswirkungspotential und Eintrittswahrscheinlichkeit aufgespannt wird, erfolgte zunächst in einem Workshop durch die Projektbeteiligten. Dieses Abbild soll in einer folgenden Phase auch durch Anspruchsgruppen aus anderen Branchen und Perspektiven erfolgen, wodurch man bei ausreichend hoher Anzahl an Beteiligten empirisch gesicherte Aussagen treffen und einen Trend ableiten kann.

Im Detail zeigt die Risikomatrix, dass jene High-Level-Domains tendenziell die größten Risiken generieren, wenn sie Mensch und Gesellschaft in Leib- und Leben bedrohen – z.B. Gesundheit, Transport, öffentliche Sicherheit und Militär. Ein folgender Schwerpunkt im risikoreichen Bereich ist der Heim- und Haushalts- sowie teilweise der Lebensmittelbereich. Der Finanzbereich, Schwerindustrie und Fertigung sind dabei je nach High-Level-Risiko etwas verstreuter verortet, ebenso bestimmte Risiken im Lebensmittelbereich. Als eher mit gering einzuschätzenden Risiken präsentiert sich der Unterhaltungs- und Sportbereich sowie Bildung.

Die identifizierten High-Level-Risiken sowie die hier präsentierte Risikomatrix ist Teil einer Studie, die aktuell von der IDC, der OCG, der TU Wien und dem AIT im Zuge des KIRAS-Forschungsprojekts RISIoT durchgeführt wird. Diese Studie umfasst auch einen Stakeholder Workshop, an welchem die bisherigen Ergebnisse mit TeilnehmerInnen aus verschiedenen Branchen diskutiert wurden.

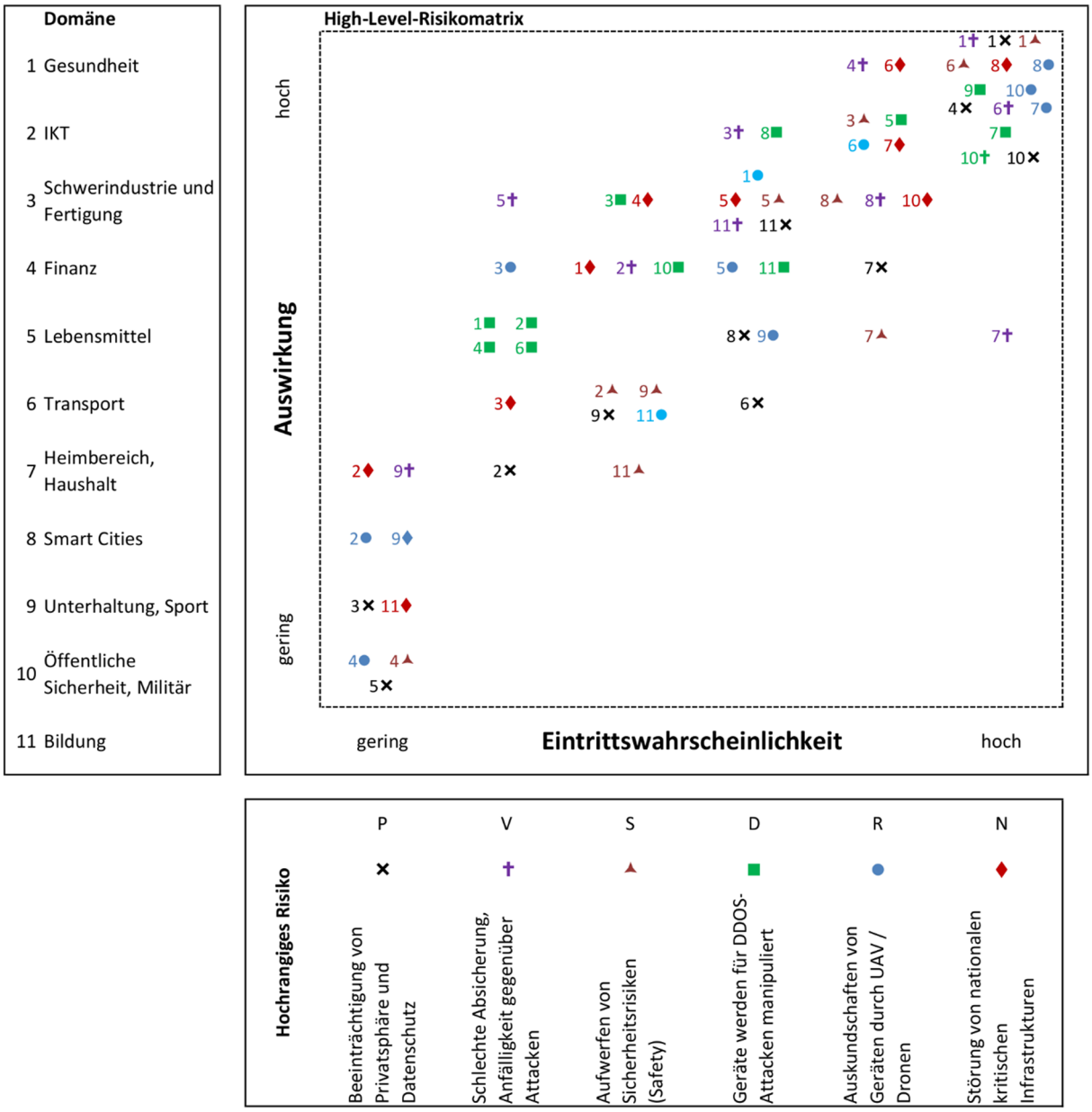

Abb. 3: High-Level-IoT-Risikomatrix

Literatur

[Chaz16] G. Chazan: Deutsche Telekom warns cyber attack hit up to 900,000 customers. URL https://www.ft.com/content/58d8a27e-b56a-11e6-961e-a1acd97f622d. – abgerufen am 2017-02-23.

[Cimp17] C. Cimpanu: WannaCry Ransomware Infects Actual Medical Devices, Not Just Computers. URL https://www.bleepingcomputer.com/news/security/ wannacry-ransomware-infects-actual-medical-devices-not-just-computers/.

[Clou16] Cloud Security Alliance: Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products, 2016

[Csa16] CSA: Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products (2016)

[Fish16] M. Fischer: Russia and the U.S. Election: What We Know and Don't Know. URL https://www.nytimes.com/2016/12/12/world/europe/russia-trump-election-cia-fbi.html?_r=1. – abgerufen am 2017-05-04.

[Gols16] J. Golson: Tesla driver killed in crash with Autopilot active, NHTSA investigating. URL http://www.theverge.com/2016/6/30/12072408/tesla-autopilot-car-crash-death-autonomous-model-s. – abgerufen am 2017-03-08.

[Gree15] A. Greenberg: Hackers Remotely Kill a Jeep on the Highway–With Me in It | WIRED. URL https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. – abgerufen am 2017-03-08.

[Hack16] Hackerone: Vulnerability disclosure for U.S. Dept Of Defense. URL https://hackerone.com/deptofdefense. – abgerufen am 2017-06-12.

[HiPK16] Andrew Hilts, Christopher Parsons, Jeffrey Knockel: Every Step You Fake. A Comparative Analysis of Fitness Tracker Privacy and Security (2016)

[IBM16] IBM: Reviewing a year of serious data breaches, major attacks and new vulnerabilities (2016)

[Isac15] ISACA: Internet of Things: Risk and Value Considerations. An ISACA Internet of Things Series White Paper. URL http://www.isaca.org/Knowledge-Center/Research/Documents/Internet-of-Things_whp_Eng_0115.pdf?regnum=. – abgerufen am 2017-03-06

[Iso14] ISO: IoT Application Domains (2014)

[Iso16] ISO: ISO/IEC CD 30141. Internet of Things Reference Architecture (IoT RA) (2016)

[Kirk12] J. Kirk: Pacemaker hack can deliver deadly 830-volt jolt. URL http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html. – abgerufen am 2017-04-20.

[Knop08] D. M. Knop: TV-Fernbedienung lässt Züge entgleisen [Update] | heise Security. URL https://www.heise.de/security/meldung/TV-Fernbedienung-laesst-Zuege-entgleisen-Update-177790.html. – abgerufen am 2017-03-08.

[Knud17] L. L. Knud: IoT Analytics. URL https://iot-analytics.com/iot-market-forecasts-overview/. – abgerufen am 2017-02-23

[Kova16] E. Kovacs: Attackers Alter Water Treatment Systems in Utility Hack: Report. URL http://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report. – abgerufen am 2017-05-04.

[Kreb16] B. Krebs: Hacked Cameras, DVRs Powered Today's Massive Internet Outage – Krebs on Security. URL https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/. – abgerufen am 2017-04-28.

[Kris16] R. Krishnan: Ransomware attacks on Hospitals put Patients at Risk. URL http://thehackernews.com/2016/04/hospital-ransomware.html. – abgerufen am 2017-05-04.

[Kush13] D. Kushner: The Real Story of Stuxnet. URL http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. – abgerufen am 2017-05-04.

[Lui15] S. Lui: Educational Toy Maker Hacked, Parents And Kids' Data Stolen. URL https://www.lifehacker.com.au/2015/12/educational-toy-maker-hacked-data-of-parents-and-kids-stolen/. – abgerufen am 2017-05-04.

[Mese07] J. Meserve: Mouse click could plunge city into darkness, experts say - CNN.com. URL http://edition.cnn.com/2007/US/09/27/power.at.risk/index.html. – abgerufen am 2017-05-04.

[Paga16] P. Paganini: South Korea 's military cyber command was hacked last monthSecurity Affairs. URL http://securityaffairs.co/wordpress/51887/cyber-warfare-2/south-korea-hacked.html. – abgerufen am 2017-05-04.

[Pere15] E. Perez: FBI: Hacker Chris Roberts claimed to hack into flights. URL http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/. – abgerufen am 2017-03-08.

[Plat17] Plattform Industrie 4.0: Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0), Bundesministerium für Wirtschaft und Energie (2017)

[Rang15] S. Ranger: Welcome to the dystopian Internet of Things, powered by and star-ring you. URL http://www.zdnet.com/article/welcome-to-the-dystopian-internet-of-things-powered-by-and-starring-you/. – abgerufen am 2017-03-23.

[Seal16] T. Seals: Russia Says it Foiled a Major Nation-State Hack on Financial System. URL https://www.infosecurity-magazine.com/news/russia-says-it-foiled-a-major/. – abgerufen am 2017-03-08.

[SPLS15] S. Schauer, B. Palensky, M. Latzenhofer, M. Stierle: GeRBA. Gesamtstaatliche Risiko- und Bedrohungsanalyse. Studie im Rahmen des KIRAS-Forschungsprogrammes. Wien, 2015

[StBe15] M. Stanislav, T. Beardsley: Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities (2015)

[Vija16] J. Vijayan: Eddie Bauer Reports Intrusion Into Point Of Sale Network. URL http://www.darkreading.com/attacks-breaches/eddie-bauer-reports-intrusion-into-point-of-sale-network/d/d-id/1326686.

[Whit16] R. Whitwam: Samsung reminds Smart TV owners their personal conversations may be recorded - Geek.com. URL http://www.geek.com/apps/samsung-reminds-smart-tv-owners-their-personal-conversations-may-be-recorded-1647353/. – abgerufen am 2017-05-04.

[Zett16] K. Zetter: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. URL https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. – abgerufen am 2017-05-04.