interact

Whitepaper

Datenmanagement, Datenschutz und Sicherheit in vernetzten Systemen

www.interact-lighting.com

Inhaltsverzeichnis

Vorwort

Moderne Beleuchtung bietet mit vernetzten Systemen ganz neue Möglichkeiten, Licht mit zusätzlichen Mehrwerten zu verbinden. Doch Datensammlung und -analyse, drahtlose Kommunikation und neue Schnittstellen bringen auch neue Herausforderungen mit sich. Was zeichnet ein sicheres System aus? Wie sicher sind meine Daten in vernetzten Systemen? Und was ist mit dem Datenschutz? Nach dem Motto „Es zahlt sich aus, paranoid zu sein“, implementieren unsere Experten Sicherheitsvorkehrungen über den gesamten Systemlebenszyklus, von der Installation, über den Betrieb und die Wartung bis zur Entsorgung des vernetzten Beleuchtungssystems. Dieses Whitepaper soll dazu beitragen, Ihnen die wichtigsten Überlegungen und Begriffe zum Thema Systemsicherheit und Datenschutz verständlich zu machen und zusätzlich Impulse für den Umgang mit IoT-Daten und und ihre Nutzung geben.

01. Sicherheit, Datenschutz und vernetzte Beleuchtung

1.1 Was ist das Internet der Dinge (IoT)?

Das Internet der Dinge (Internet of Things, IoT) wird als neue industrielle Revolution bezeichnet. Es verbindet physische und digitale Welten und verändert so bereits heute die Art und Weise, wie Unternehmen, Regierungen und Verbraucher mit der physischen Welt interagieren. Aber was ist das IoT eigentlich genau?

Laut Gartners „IT-Glossary“ ist das IoT „ein Netzwerk physischer Objekte, die Technologien enthalten, welche es ihnen ermöglichen, mit ihren internen Zuständen oder der externen Umgebung zu kommunizieren, zu interagieren oder diese zu erfassen.“[1] IoT-Geräte erfassen Daten durch Sensoren verschiedener Art – seien es Bewegungsmelder in der Decke eines Büroraumes, Geräuschpegelsensoren auf einer innerstädtischen Straße oder Sensoren, die physiologische Zustände und Veränderungen in Personen erfassen können. Sie kommunizieren miteinander über integrierte, drahtgebundene oder drahtlose Übertragungsverfahren. Solche vernetzten IoT-Geräte können z. B. Thermostate, Energiezähler oder Trackingsysteme sein, aber auch tragbare Geräte zur Überwachung der persönlichen Fitness und Vitalfunktionen. Jedes digitale Gerät, das aussagekräftige Daten über sich selbst, seine Nutzung und seine Umgebung sammeln oder austauschen kann, ist ein Kandidat für die Teilnahme am IoT.

Die von solchen Geräten erzeugten Daten unterschiedlichster Art werden häufig in IoT-Anwendungen in der Cloud gesammelt, verarbeitet und analysiert, um daraus Informationen und konkrete Erkenntnisse zu gewinnen.

Das IoT ist eine relativ junge Technologie und seine Infrastruktur entwickelt sich stetig weiter. Seine potenziellen Auswirkungen sind allerdings bereits enorm: Das McKinsey Global Institute (MGI) prognostiziert, dass „das Internet der Dinge im Jahr 2025 insgesamt zwischen 3,9 und 11,1 Milliarden Dollar pro Jahr umsetzen wird, was etwa 11 % der Weltwirtschaft entspricht.“[2] Business Insider prognostizieren, dass bis 2020 24 Milliarden Geräte mit dem Internet verbunden sein werden – also „durchschnittlich vier Geräte für jeden Menschen auf der Erde“[3].

Die schiere Datenmenge, die von diesen Milliarden von vernetzten Geräten gesammelt wird, erfordert eine besondere Kombination von Technologien, Analyseverfahren, Softwareplattformen und Rechenleistung. Man bezeichnet diese großen Datenmengen als „Big Data“. Big Data stellt neue Herausforderungen an das Datenmanagement, die mit herkömmlichen Ansätzen nicht gelöst werden können. Und es birgt auch neue Risiken.

1.2 Vernetzte Leuchten und das IoT

Künstliche Beleuchtung ist überall dort, wo Menschen arbeiten und leben. Wird sie durch Vernetzung intelligent gestaltet, ergeben sich daraus Anwendungsmöglichkeiten über die reine Beleuchtung hinaus, z. B. Datensammlung und Datenanalyse, sowie die Verknüpfung mit anderen intelligenten Systemen. Aber das ist noch nicht alles: Ist das Beleuchtungssystem vernetzt, kann es zusätzlich als Plattform für Sensornetzwerke und als Basis für die Bereitstellung von IoT-Anwendungen dienen. Beleuchtung bildet immer schon ein natürliches Netzwerk, das – wenn es intelligent ist – zu einem einheitlichen, zusammenhängenden IP-Netzwerk zusammenwachsen kann, in dem unterschiedliche Netzwerke wie Verbrauchsmessung, Beleuchtung, HLK, Videoüberwachungssysteme, technische Sicherheit und Zeitsteuerung integriert werden können. Ein solches integriertes Netzwerk ermöglicht neue, innovative Nutzerfunktionen für die Gebäudeintelligenz und bietet gleichzeitig Gebäudeeigentümern und -betreibern detailliertes Energiemanagement sowie neuartige Steuerungs-, Analyse- und Integrationsfunktionen.[4]

Auch intelligente Städte setzen zunehmend auf integrierte Netzwerke, um Bürgern und Bürgerinnen einen Mehrwert zu bieten: Vernetzte Straßenbeleuchtung schafft – ganz ähnlich wie die vernetzte Deckenbeleuchtung – hierfür eine ideale Infrastruktur. Sie ermöglicht die flächendeckende Bereitstellung von Sensoren, Breitbandkommunikationsgeräten und anderen vernetzten Geräten und bietet zusätzlich Schnittstellen (APIs) für die Integration weiterer kommunaler Netzwerke.

Da LED-Leuchten über beliebig in das System integrierbare Sensoren (z. B. Tageslicht-, Präsenz-, Bewegungs-, Geräusch- und Luftqualitätssensoren) Daten sammeln und austauschen können, entstehen zum Teil große Datenmengen, die verwaltet werden müssen.

1.3 Herausforderungen für Sicherheit, Privatsphäre und Datenschutz in vernetzten Systemen

Eine der größten Herausforderungen im Zusammenhang mit dem IoT ist die Sicherheit, da sind sich führende Analysten und Forscher einig. Sowohl eine von McKinsey im Jahr 2015 durchgeführte Studie[5], als auch Gartners Internet of Things Backbone Survey aus dem Jahr 2016, identifizierten „Sicherheit als das wichtigste Anliegen" aus technologischer und administrativer Sicht.[6] Wie kann man die Vernetzung und den Datenverkehr durch so viele miteinander verbundene Systeme ausreichend absichern? Wie schützt man das wachsende Angebot an kostbaren digitalen Ressourcen – z. B. vertraulichen Unternehmensdaten, städtischer Infrastruktur, Informationen über Privatpersonen, Transaktionsdaten und Heimgeräte?

Zu den wichtigsten Bedrohungen für Sicherheit und Privatsphäre gehören böswilliger Zugriff, Denial-of-Service und Diebstahl von Diensten, insbesondere von Daten. Angreifer nutzen zudem zunehmend unzureichend gesicherte IoT-Geräte, um in anderen Bereichen Störungen zu inszenieren.

IoT-Hacks infizieren vernetzte Endgeräte mit Malware,um einen massiven Datenstrom freizusetzen, der Websites und andere Online-Ressourcen mit einem so genannten Distributed Denial of Service (DDoS)-Angriff lahmlegt.

Im Jahr 2016 nutzten Hacker zum Beispiel das riesige IoT-Botnet Mirai, das Sicherheitslücken im IoT ausnutzt. Mirai wurde benutzt, um einzelne Websites anzugreifen und vorübergehend zum Erliegen zu bringen, und führte durch den Angriff auf Internet Service Provider und Internet-Backbone-Unternehmen zu Verbindungsunterbrechungen auf der ganzen Welt.[7]

Ein DDoS-Angriff in Finnland schaltete im November 2016 bei Minusgraden die Heizungsanlagen in mehreren Wohnblöcken in Lappeenranta ab.[8] Da die Zahl der unzureichend gesicherten vernetzten Geräte steigt, erwarten Sicherheitsexperten, dass die Zahl von DDoS- und anderen Angriffen zunehmen wird. Während die Abschaltung der Heizungsanlage in Finnland unbeabsichtigt zu sein scheint, ist es nicht allzu schwer, sich Angriffe vorzustellen, die direkt auf vernetzte Systeme in Städten, Büros und Wohnungen gerichtet sind, zum Beispiel auf die Heizung, Gebäudesicherheit oder Beleuchtung.

Mit Interact-Systemen wird die Beleuchtung zum IoT-Netzwerk. Während sich die Spezifikationen von System zu System unterscheiden, teilen sich alle Systeme eine globale Plattform mit diesen Komponenten:

- Lichtgeräte: vernetzte Leuchten, Sensoren und Lichtsteuerungen
- Hard- und Software: Schnittstellen, Server, Switches, Verkabelung und Datenkommunikation
- Managementsoftware: für das Beleuchtungssystem und die IoT-Anwendungen, die das Beleuchtungssystem hostet
- Cloud-Dienste: für das Hosting von Softwareanwendungen und für die Erhebung von Daten aus beleuchteten Bereichen
- APIs: offene Schnittstellen zur Anbindung von Interact an andere Komponenten und Verwaltungssysteme im digitalen Gesamtsystem sowie zur Entwicklung von Apps und anderen Software-Komponenten wie Dashboards
- Analytics: Eine Analyseplattform, um die Rohdaten aus den angeschlossenen Systemen in praxistaugliches Know-how umzuwandeln

Ein sicheres IoT-System berücksichtigt für jede dieser Komponenten deren besondere Sicherheitsanforderungen im Hinblick auf Datenschutz, Daten- und Systemsicherheit sowie Data Governance.

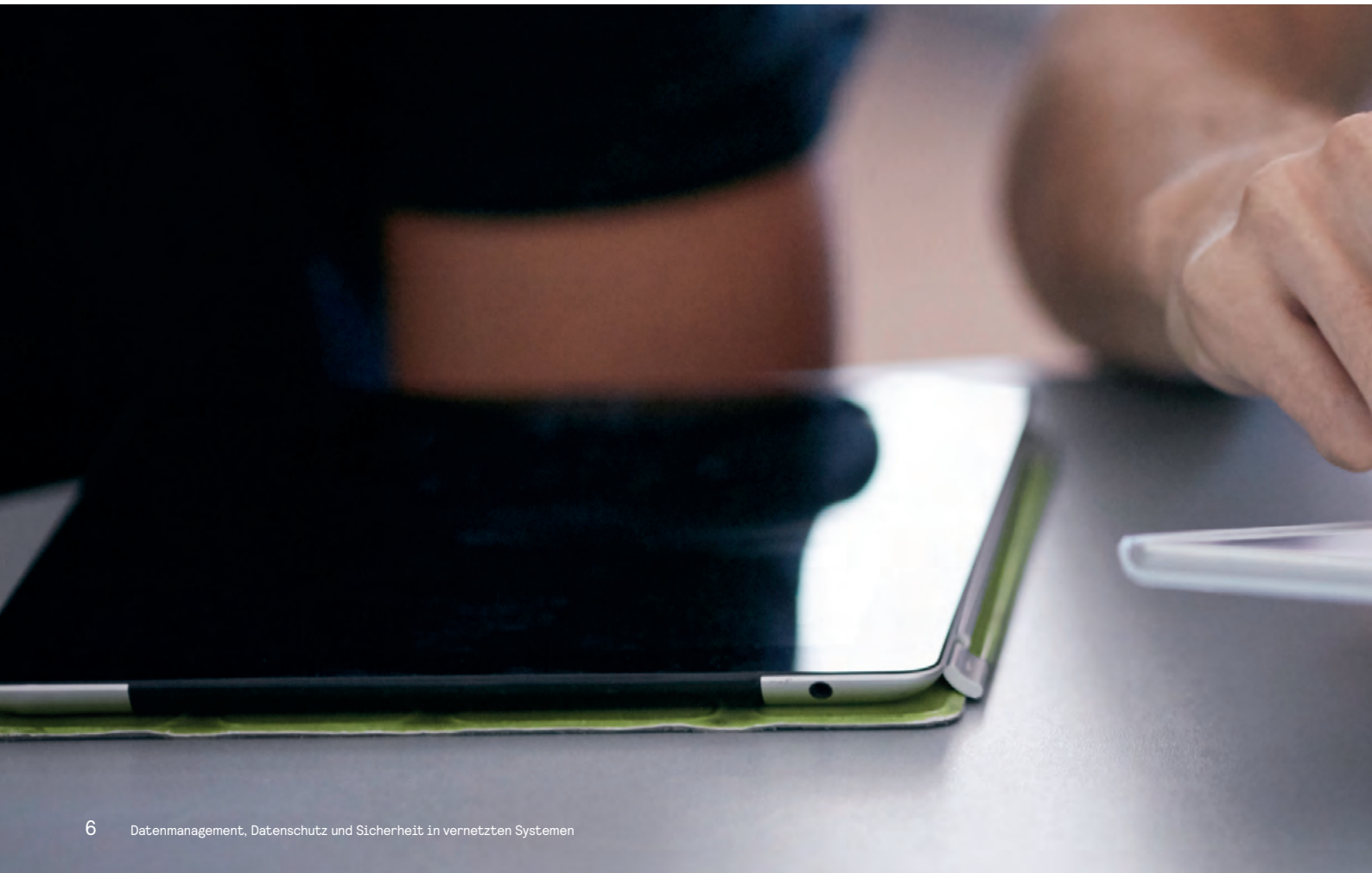
Das Hacken von Babyfonen, intelligenten Kühlschränken, Thermostaten, Medikamenteninfusionspumpen, Kameras und sogar dem Radio in Ihrem Auto ist ein Sicherheitsalptraum, der in Zeiten des IoT denkbar ist, schreibt IoT-Experte Ahmed Banafa. Sicherheitsbedenken werden sich nicht länger auf den Schutz sensibler Informationen und Vermögenswerte beschränken. Unser Leben und unsere Gesundheit selbst könnten das Ziel von Hackerangriffen werden.[9]

Auch vernetzte Beleuchtungssysteme bieten als komplexe Systeme theoretisch zahlreiche Angriffsmöglichkeiten. Diese müssen daher durch geeignete Richtlinien und Verfahren bereits in der Konzeption und Herstellung des Systems adressiert werden. Auf diese Weise kann das Risiko eines Angriffs auf vernetzte Geräte, Schnittstellen, Gateways, Bridges und andere Netzwerkhardware, Cloud-Schnittstellen und -Infrastrukturen, interne und externe APIs sowie mobile Apps minimiert werden.

Unsere Sicherheitsexperten haben, frei nach dem Motto, „es lohnt sich, paranoid zu sein“, dutzende solcher Risiken in vernetzten Beleuchtungssystemen identifiziert und adressiert.

Zusätzlich werden spezifische Risikofaktoren in bestimmten Anwendungsbereichen bedacht. Während viele Sicherheitsrisiken für alle vernetzten Beleuchtungsanwendungen gleich sind, stehen im kommunalen Bereich die Gewährleistung und Sicherheit von Verkehr, Straßenbeleuchtung und Gefahrenabwehr im Mittelpunkt. Im Bereich intelligenter Gebäudeanwendungen stehen der Schutz der Unternehmenswerte und die Privatsphäre der Mitarbeiter im Vordergrund. Im Handel geht es besonders um den Schutz der Zahlungs- und Transaktionsdaten sowie der persönlichen Daten der Kunden, während Smart Home-Anwendungen Risiken für die Hausbewohner berücksichtigen müssen.

Auf dieser Basis definieren wir wirksame Sicherheitsmaßnahmen und setzen sie um: von der Herstellung über den Betrieb, bis hin zur sicheren Außerbetriebnahme. Denn Sicherheit hängt immer vom schwächsten Glied ab. Ein wichtiger Kernbereich ist dabei die sichere Nutzung von Daten und der sichere Umgang mit ihnen.



02.
Daten verstehen: Wichtige Begriffe und Modelle

2.1 Mehrwert schaffen mit Daten: Wie lassen sich Daten im Unternehmen effektiv nutzen?

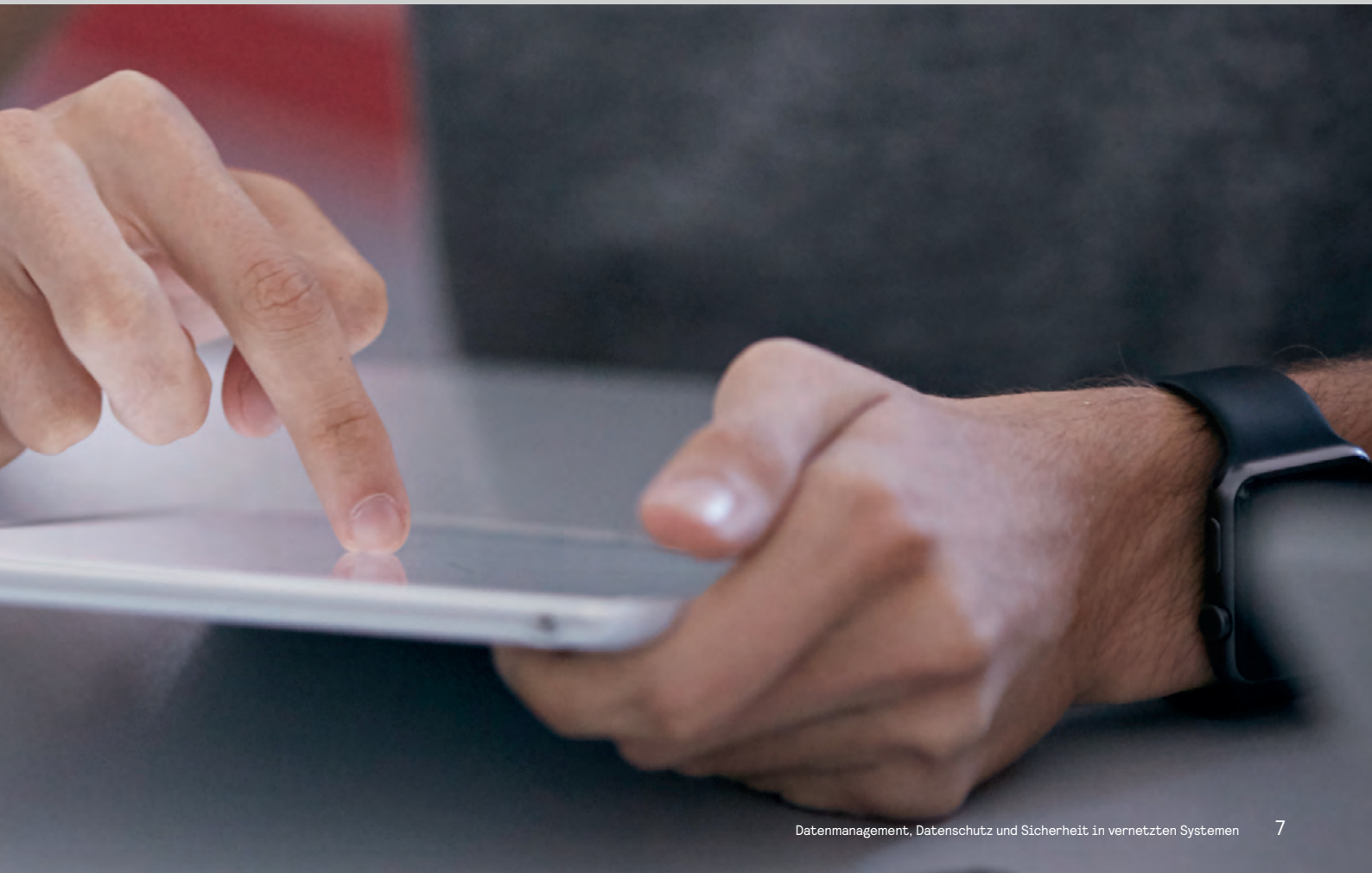
Intelligente vernetzte Infrastrukturen erzeugen große Datenmengen – in Städten, am Arbeitsplatz, im Einzelhandel oder zu Hause. Diese Daten können genutzt werden, um Abläufe zu vereinfachen, Kosten für die Bereitstellung von Services zu senken und die Bedürfnisse von Kunden, Bürgern und Mitarbeitern besser zu verstehen. So können Wettbewerbsvorteile erzielt oder durch neue, datengestützte Produkte und Dienstleistungen, neue Einnahmequellen erschlossen werden.

Unternehmen können die so gewonnenen Datenmengen zusätzlich mit relevanten Daten aus externen Quellen kombinieren, um ein tieferes Verständnis für das Nutzerverhalten zu gewinnen. Beispielsweise kann eine Stadt Energie sparen, indem sie Sensoren, Steuerungen und Software einsetzt, die Daten darüber sammeln und analysieren kann, wann und wo sich Menschen aufhalten. Das Licht kann so gezielter eingesetzt und – bei geringerem Energieeinsatz – das Sicherheitsgefühl in der Stadt verbessert werden.

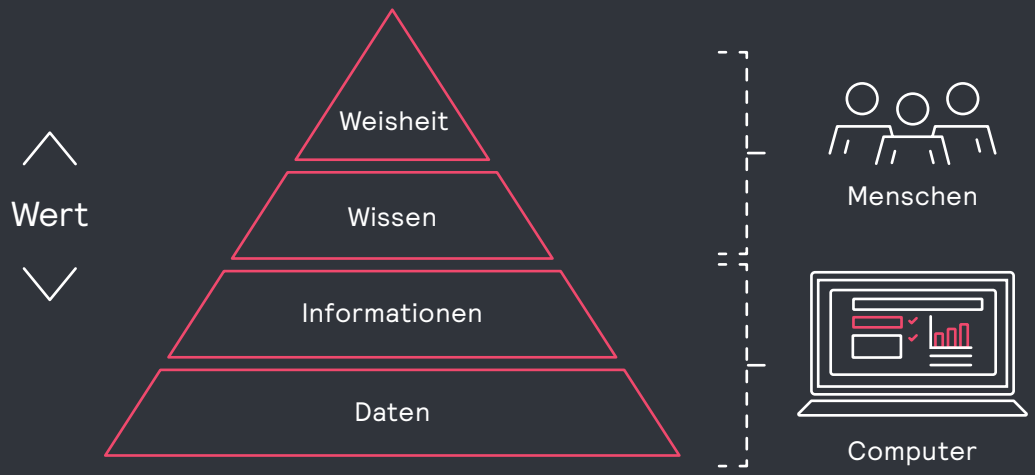
Ebenso können Unternehmen Daten über die Auslastung und Nutzung von Arbeitsplätzen sammeln und analysieren, um Licht, Klimatechnik, Heizung, Lüftung und andere Dienstleistungen effizienter einzusetzen. Auf diese Weise können Kosten gesenkt, Abläufe verbessert und die Arbeitsumgebung für die Mitarbeiter angenehmer gestaltet werden.

Um Daten jedoch sicher und effizient nutzen zu können, ist es sinnvoll, zunächst einmal zu verstehen, welche Arten von Daten es gibt und wie aus Daten Erkenntnisse gewonnen werden können.

In den nächsten Abschnitten beleuchten wir daher genauer, was Daten überhaupt sind und wie sie nutzbar gemacht werden können. Wir erklären, was der beste Ansatz für ein Datenlebenszyklusmanagement ist, und wie sinnvolle Sicherheits- und Datenschutzmaßnahmen in vernetzten Systemen aussehen können.



2.1.1 Von Daten zu Weisheit – die DIKW-Pyramide



2.1.2 Was sind Daten und wie entstehen aus Daten nützliche Erkenntnisse?

Allgemein ausgedrückt sind Daten eine Sammlung von Zahlen oder Zeichen. Daten können gemessen, gesammelt, analysiert und in verschiedenen Formaten wie Tabellen, Diagrammen, Grafiken und Bildern dargestellt werden. Konzeptionell bezeichnet der Begriff Daten die Bereitstellung oder Kodierung von Informationen oder Kenntnissen in einer für eine bessere Nutzung oder Verarbeitung geeigneten Form[10].

Daten allein haben wenig Wert. Um mit Ihnen „etwas anfangen zu können", also handlungsrelevante Erkenntnisse zu erhalten, müssen sie aufbereitet und kontextualisiert werden.

Das Modell der DIKW-Pyramide veranschaulicht, welche Verarbeitungsschritte notwendig sind, um aus Daten handlungsrelevante Erkenntnisse zu erhalten. DIKW steht für „Data, Information, Knowledge and Wisdom" oder „Daten, Informationen, Wissen und Weisheit". Um Informationen zu erhalten, müssen Daten verarbeitet werden. Verarbeitete und interpretierte Informationen müssen analysiert werden, um Wissen zu erhalten. Und zuletzt müssen Prinzipien auf das Wissen angewendet werden, um Weisheit zu erhalten.

ohne Kontext

Im Kontext der DIKW-Pyramide sind Daten eine Reihe von Symbolen oder Zeichen, die Reize oder Signale darstellen. Diese Signale haben keine Bedeutung und keinen Wert, bis sie in eine brauchbare Form und einen sinnvollen Kontext gebracht werden.

Beispiele für Daten sind:
rot
1466005743
-33.882816, 151.204150

Fügt man Daten eine Beschreibung hinzu, um sie nutzbar zu machen, erhält man Informationen.

mit Beschreibung

Wenn wir den vorherigen Beispieldaten eine Beschreibung hinzufügen, erhalten wir zum Beispiel folgende Informationen:

Die Ampel wurde am 15. Juni 2016 um 15:49:03 Uhr GMT an der Ecke Pitt Street und George Street rot.

mit Wissen

Wissen bringt neue Zusammenhänge und Regeln in die Information ein:

Ich fahre auf die Ampel zu, die gerade rot geworden ist. Die Regeln besagen, dass ich mein Auto anhalten muss, wenn die Ampel rot ist.

mit Weisheit

Weisheit baut auf Wissen und Erfahrung auf, die im Laufe der Zeit gesammelt wurden. Man könnte sagen, dass sie darin bestehen, „zu wissen, was richtig ist". Die Weisheit, die auf dem Wissen in unserem Beispiel aufbaut, könnte in etwa so ausgedrückt werden:

„Über eine rote Ampel zu fahren ist illegal, gefährlich und potenziell tödlich. Also halte ich mein Auto besser an."

Weil Weisheit bedeutet, Wissen und Erfahrung für ein höheres Ziel zu nutzen, ist sie tiefer und menschlicher als Wissen. Es erfordert ein Gespür für Gut und Böse, richtig und falsch, ethisch und unethisch. Sie beinhaltet das Verstehen von Menschen, Objekten, Ereignissen und Situationen und die Bereitschaft sowie die Fähigkeit, Wahrnehmung, Urteilsvermögen und Handeln im Sinne des bestmöglichen Vorgehens einzusetzen. Als solche ist Weisheit an sich subjektiv.

Wie die DIKW-Pyramide zeigt, erhalten Daten Bedeutung und Wert aus ihrer zielgerichteten Verarbeitung – im Hinblick auf einen übergeordneten Sinn und ein betriebswirtschaftliches Ziel. Für Unternehmen erfordert dies ein grundlegendes Verständnis von Daten und einen organisatorischen Fokus auf Datenmanagementprozesse. Es ist zu diesem Zweck zunächst wichtig zu erkennen, dass es verschiedene Kategorien von Daten gibt, die unterschiedliche Anforderungen an ihre Verarbeitung und Verwaltung stellen.

2.2 Welche Kategorien von Daten gibt es? Datenstruktur, Datengröße, Datenbewegung und Datenquelle

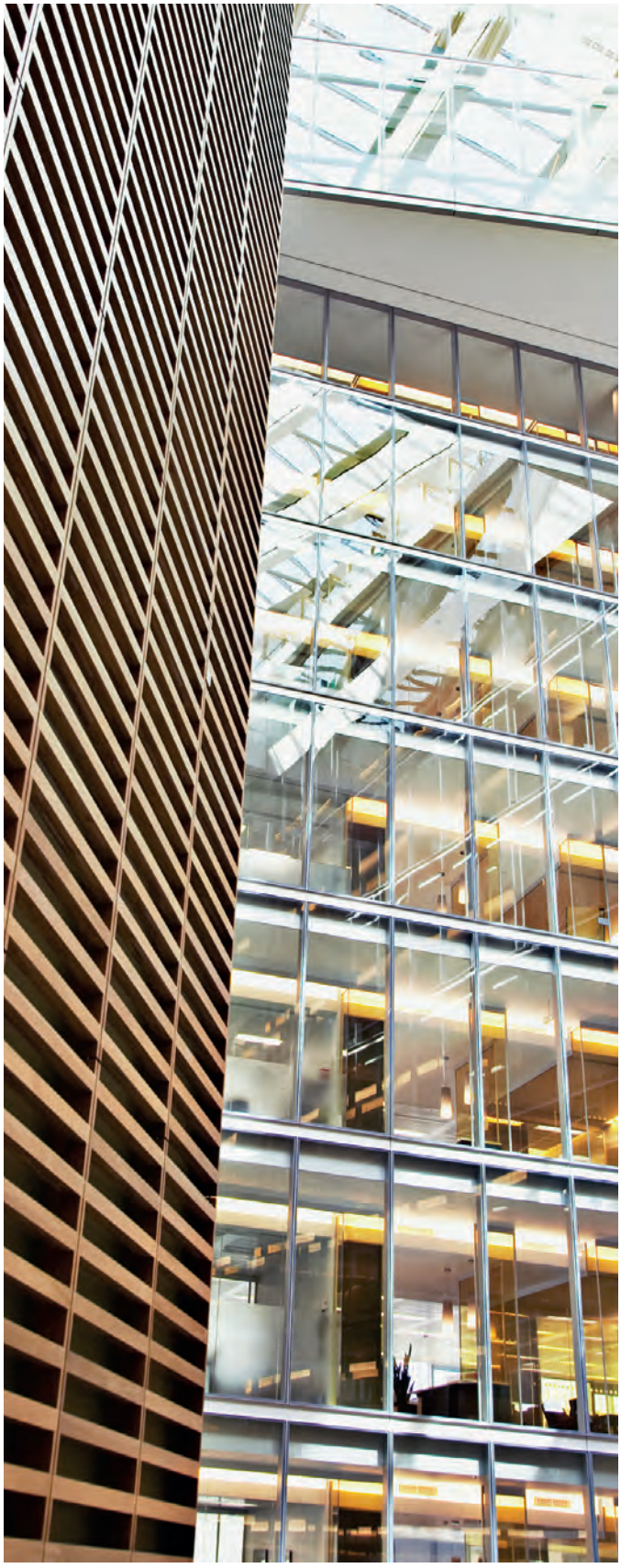
Verschiedene Arten von Daten lassen sich nach ihrer Struktur, Größe, Bewegung und Quelle kategorisieren. Für einen effektiven Datenmanagementprozess ist es unerlässlich, sich ein genaues Bild zu machen, in welche Kategorie die zu verarbeitenden Daten fallen und welche Herausforderungen und Möglichkeiten damit verbunden sind.

2.2.1 Datenstruktur: strukturierte, halbstrukturierte und unstrukturierte Daten

Strukturierte Daten sind Daten mit einer übergeordneten Organisation. Ein definiertes Datenmodell oder Datenschema gibt vor, welche Arten von Daten aufgezeichnet werden und wie sie gespeichert, verarbeitet und abgerufen werden, indem es zum Beispiel die Dateneingabe einschränkt (Anzahl der Zeichen, spezifische Begriffe, numerische Bereiche) und/oder den Datentyp vorgibt (numerisch, Währung, alphabetisch, Name, Datum, Adresse). Beispiele für strukturierte Daten sind Daten aus Datenbanken und Software wie Customer Relationship Management, Transaktionsmanagement, Supply Chain Management, oder auch Mitarbeiterinformationen und Systemprotokolle. Ein Vorteil von strukturierten Daten ist, dass sie leicht abgefragt und analysiert werden können. In der Vergangenheit wurden strukturierte Daten typischerweise in relationalen Datenbanken und Tabellenkalkulationen verwaltet.

Halbstrukturierte Daten sind strukturierte Daten, denen eine strenge Datenmodellstruktur fehlt. Tags oder andere Marker erlauben es, bestimmte Elemente innerhalb der Daten zu identifizieren, während die Daten selbst keine starre Struktur haben. Ein Beispiel dafür sind Fotos oder andere Grafiken, die mit Tags wie Ersteller, Datum, Ort und Schlüsselwörtern versehen werden können, um sie zu organisieren und wiederzufinden. Um halbstrukturierte Daten zu verwalten, werden verschiedene Dateisysteme und -formate verwendet.

Unstrukturierte Daten sind Daten, die entweder kein vordefiniertes Datenmodell haben oder nicht in einer vordefinierten Weise organisiert sind. Unstrukturierte Daten sind typischerweise textlastig, können aber auch andere Datentypen wie Daten und Zahlen enthalten. Mit herkömmlichen Programmen ist es aufgrund der Unregelmäßigkeit und Mehrdeutigkeit der Daten schwierig, aus unstrukturierten Daten Informationen zu schöpfen. Techniken wie Data Mining, Natural Language Processing (NLP) und Textanalyse bieten verschiedene Methoden, um Muster in unstrukturierten Daten zu finden oder anderweitig zu interpretieren. Beispiele für unstrukturierte Daten sind Social Media, Web Content und Call Center Logs.



2.2.2 Datenumfang: Was ist Big Data?

Im Gegensatz zu Daten, die in den Speicher eines Computers passen und von traditionellen Datenverarbeitungsanwendungen verwaltet werden können („Small Data"), bezeichnet man Daten, die so groß oder komplex sind, dass sie nicht mit herkömmlichen Datenverarbeitungsprogrammen verarbeitet werden können, als „Big Data". Die Verarbeitung solch großer Datenmengen kann Software erfordern, die auf zehn, hunderten oder sogar tausenden von Servern parallel läuft. Was als „Big Data" gilt, hängt allerdings immer von den Fähigkeiten der Benutzer und ihrer Werkzeuge ab. So ändert sich die Definition von „Big Data" ständig parallel zum technischen Fortschritt.

2.2.3 Wie bewegen sich Daten? Data at Rest, Data in Motion und Fast Data

Daten, die statischer Natur sind, d. h. in einem dauerhaften Speicher (Festplatte, Datenträger) in beliebiger digitaler Form (z. B. Datenbank, Data Warehouse, Tabellenkalkulation, Dateien) gespeichert sind, werden meist als „Data at Rest" (Daten im Ruhezustand) bezeichnet. Der Begriff „Data in Motion" bezeichnet Daten, die verarbeitet werden, ohne sie zu speichern („on the fly").

Die Datengeschwindigkeit (Velocity) gibt an, ob Daten schnell oder langsam erzeugt, gespeichert, analysiert und visualisiert werden. Schnelle Datengeschwindigkeit („Fast Data") bedeutet, dass Daten in kurzer Zeit verarbeitet werden, heute meist in Echtzeit oder nahezu in Echtzeit. Traditionell wird dieses Konzept als Daten-Streaming bezeichnet. Jede Veränderung der Daten im Laufe der Zeit, einschließlich der Datenflussrate, der Formatierung und der Zusammenstellung der Daten, wird als Variabilität der Data in Motion bezeichnet. Eine hohe Variabilität bedeutet viele Datenverarbeitungsprozesse und damit einen sprunghaften Anstieg des Datenaufkommens in einer begrenzten Zeitspanne. Um solche Daten effizient bewältigen zu können, sind neue Verfahren notwendig.

2.2.4 Datenquelle: interne und externe Daten

Daten können gemäß der Datenquelle oder -herkunft als intern oder extern kategorisiert werden: Daten, die aus internen Systemen (z. B. Unternehmenssysteme, IT etc.) kommen, werden als intern bezeichnet, während Daten, die von Drittanbietern stammen, als extern bezeichnet werden. Beispiele für externe Daten sind Social Media-, Wetter- oder Verkehrsdaten von Drittanbietern.

Herkömmliche unternehmenseigene Informationsmanagementsysteme befassen sich mit strukturierten oder höchstens halbstrukturierten Daten, „Small Data" und „Slow Data", „Data at Rest" und internen Daten. IoT-Daten sind jedoch oft unstrukturierte Datenströme, liefern große Datenmengen und enthalten externe Daten. Um diese Daten strukturiert und sicher verwalten und nutzen zu können, sind neue Systemarchitekturen notwendig.

2.3 Was bestimmt den Wert von Daten?

Der Wert von Daten wird durch die folgenden Faktoren bestimmt:

1. Der Wert der Daten steigt mit ihrer Nutzung.

Daten sind umso wertvoller, je mehr wir sie tatsächlich nutzen. Denn mit den Daten verbundene Kosten sind in erster Linie nutzungsunabhängige Fixkosten wie Anschaffung, Speicherung und Wartung. Der Kostenaufwand für die Nutzung der Daten ist dagegen vernachlässigbar. Da Daten unendlich teilbar sind und sich nicht abnutzen, kann ihr Wert durch optimale Nutzung vervielfacht werden. Umgekehrt verursachen Daten, die nicht verwendet werden, unnütze Kosten wie Anschaffungs-, Speicher- und Wartungskosten. Um wertvoll zu sein, müssen Daten leicht auffindbar und einfach zu verwenden sein und so oft wie möglich weiterverarbeitet werden.

2. Der Wert der Daten nimmt mit der Zeit ab.

In den meisten Fällen sind Daten umso wertvoller, je aktueller sie sind, wobei dies stark anwendungsabhängig ist. Im Laufe der Zeit werden Daten immer weniger relevant und sind schließlich überholt.

3. Der Wert der Daten steigt mit ihrer Qualität.

Der Begriff der Datenqualität umfasst Merkmale wie Richtigkeit, Exaktheit, Kohärenz, Vollständigkeit, Vertrauenswürdigkeit (nachvollziehbare Herkunft) und Aktualität. Nur wenn die Daten korrekt, vollständig, aktuell und vertrauenswürdig sind, kann man aus ihnen einen echten Mehrwert generieren. Schlechte Datenqualität, die zu schlechten Entscheidungen oder operativen Fehlern führt, kann sehr kostspielig sein.

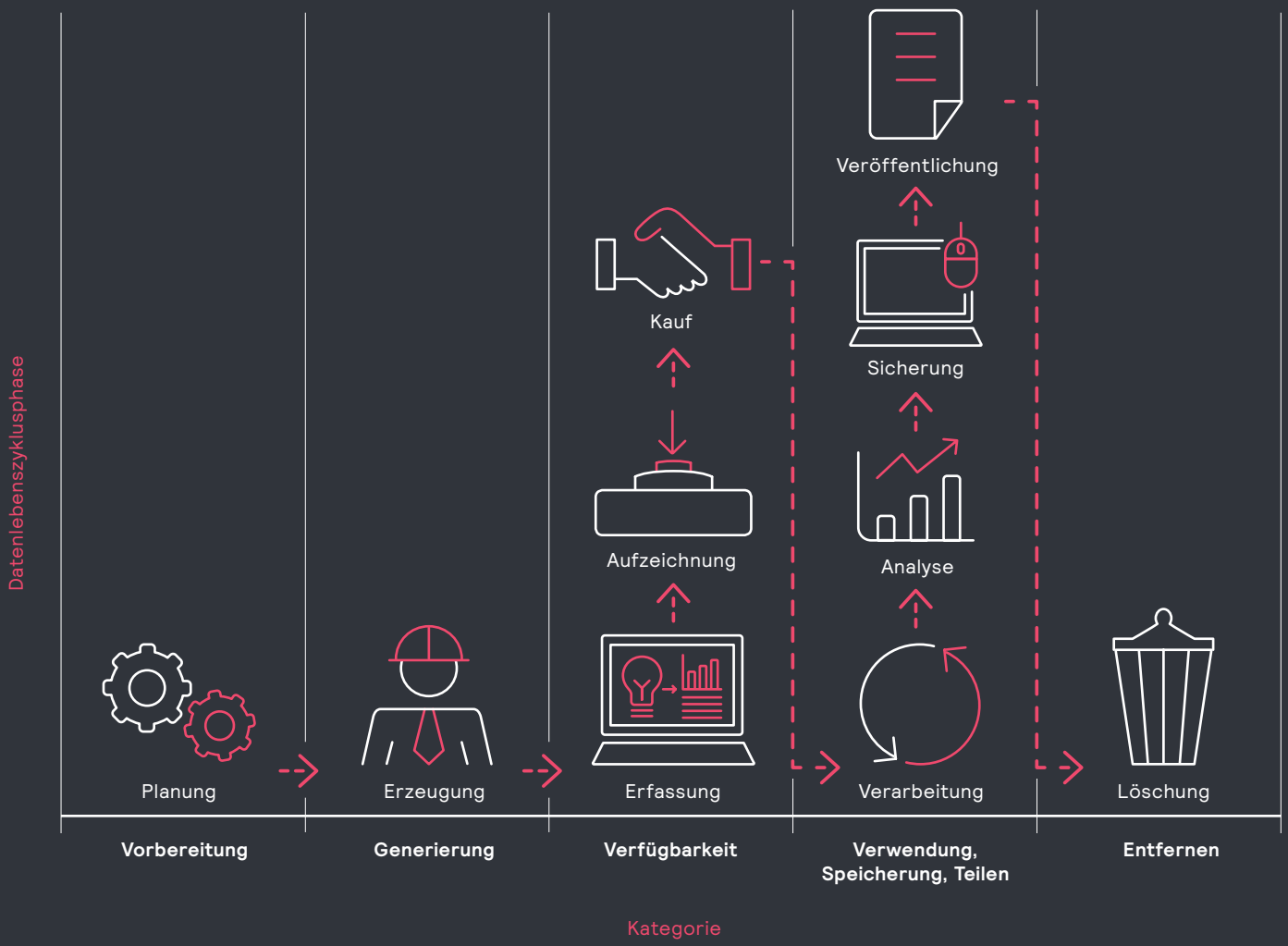
4. Der Wert der Daten steigt, wenn sie mit anderen Daten verknüpft werden.

Ein Mehrwert entsteht zum Beispiel, wenn mehrere Datenquellen kombiniert werden, um neue Daten oder wichtige Erkenntnisse zu gewinnen. Durch Aufbereitung der Daten kann die Datenqualität verbessert und sichergestellt werden. Metadaten können hinzugefügt und Daten indiziert werden, um Kontext zu schaffen und die Zugänglichkeit zu verbessern.

In Abgrenzung zur Datenerzeugung werden bei der Datenerfassung die erzeugten Daten direkt oder indirekt gemessen. Stellen Sie sich zum Beispiel eine Kamera vor, die Fahrzeuge aufzeichnet, die eine Straße entlangfahren. Die Daten werden durch die vorbeifahrenden Fahrzeuge automatisch erzeugt, die Kamera erfasst die Daten.

2.4 Der Datenlebenszyklus

Datensicherheit muss über den gesamten Lebenszyklus hinweg gewährleistet sein. Hierzu muss jede der verschiedenen Phasen der Verarbeitung, Speicherung, Konvertierung und Analyse von Daten gesichert sein. Die einzelnen Phasen sind in der Abbildung schematisch dargestellt:



Planung
Die erste Phase des Datenlebenszyklus ist die Planung. Hier wird die Art der benötigten Daten festgelegt, Strategien zur Erfassung der Daten sowie die Zuweisung von Personal-, Rechen- und Systemressourcen[11]. Diese Phase umfasst auch die Entwicklung und Beschaffung der benötigten Ressourcen (z. B. Software).

Datenerzeugung
Der zweite Schritt des Datenlebenszyklus ist die eigentliche Erzeugung der Daten. Unter Erzeugung versteht man die direkte, indirekte oder automatische Generierung von Daten, welche Eigenschaften einer zugrunde liegenden Datenquelle repräsentieren. Die Datenquelle kann eine physikalische Umgebung, eine Organisation, ein Gerät oder sogar ein Computerprogramm sein, das Daten erzeugt, die für einen Prozess oder ein Ziel relevant sind.

Datenerfassung
In Abgrenzung zur Datenerzeugung werden bei der Datenerfassung die erzeugten Daten direkt oder indirekt gemessen. Stellen Sie sich zum Beispiel eine Kamera vor, die Fahrzeuge aufzeichnet, die eine Straße entlangfahren. Die Daten werden durch die vorbeifahrenden Fahrzeuge automatisch erzeugt, die Kamera erfasst die Daten.

Datenaufzeichnung
Einmal erfasste Daten werden aufgezeichnet. Die Aufzeichnung ermöglicht es, die Daten über das für die Erfassung erforderliche Zeitfenster hinaus zu nutzen.

Datenakquisition
Unter Datenakquisition versteht man die Beschaffung von Daten, die von Organisationen außerhalb des eigenen Unternehmens gemessen oder aufgezeichnet wurden. Diese Phase ist kein notwendiger Bestandteil des Datenlebenszyklus. Wenn eine Datenbeschaffung durch Dritte erforderlich ist, findet die Erstellungs-, Erfassungs- und Aufzeichnungsphase vor oder während der Planungsphase statt, da sie von einem in der Planungsphase identifizierten Datenlieferanten verwaltet wird. Die Akquisition der Daten erfolgt nach ihrer Erfassung oder Aufzeichnung. In einem Vertrag wird festgelegt, wie Dritte die erfassten Daten verwenden dürfen.

Datenverarbeitung
Alle Phasen bis zu diesem Zeitpunkt betreffen die Verfügbarkeit von Daten in ihrer Grundform. Sobald die Daten verfügbar sind, erfolgt die Verarbeitung. Hier werden die Daten so transformiert, angereichert und mit anderen Daten kombiniert, dass daraus aussagekräftige Ergebnisse und Schlussfolgerungen abgeleitet werden können. Datenverarbeitung ist die Formatierung und Zusammenführung von Daten. Erst in der letzten Phase – der Datenanalyse – werden daraus für die Unternehmensziele nutzbare Assets generiert.

Datenanalyse
In der Phase der Datenanalyse werden die Daten untersucht, um Muster zu identifizieren, Rückschlüsse zu ziehen und Konsequenzen zu definieren, die für die finalen Unternehmensziele von Bedeutung sind. Techniken des maschinellen Lernens, Big Data, Signalverarbeitung, Bildverarbeitung und statistische Analyse werden in dieser Phase angewendet. In Anlehnung an die DIKW-Pyramide verwandelt die Datenanalyse Informationen in Wissen.

Datensicherung
Die Datensicherung stellt sicher, dass die Daten sowie die daraus abgeleiteten Zwischen- und Endergebnisse nach festgelegten Richtlinien und Regeln für einen bestimmten Zeitraum sicher aufbewahrt werden, sei es als Backup oder für eine mögliche zukünftige Verwendung. Zusätzliche Metadatengenerierung, Dokumentation und Datenarchivierung sind ebenfalls Aspekte der Datensicherung.

Veröffentlichung von Daten
Im Rahmen der vertraglich und urheberrechtlich festgelegten Möglichkeiten kann internen Nutzern oder Dritten zu Daten und daraus abgeleiteten Ergebnissen Zugang gewährt werden. Verschiedene Benutzer können unterschiedliche Zugriffsrechte auf alle oder eine Teilmenge der Daten/Ergebnisse erhalten.

Entsorgung von Daten
Am Ende der Reise müssen die Daten an allen Orten, an denen sie gespeichert sind, gelöscht oder archiviert werden. Nach Abschluss dieser Phase dürfen keine Kopien der Daten zur Verwendung an irgendeinem Ort aufbewahrt werden.


mr.p
at Siam

03.
Datenmanagement und Data Governance

Um Sicherheit und Datenschutz in den wachsenden Anwendungsfeldern von IoT und Smart Systems zu gewährleisten, ist strategisches Datenmanagement von entscheidender Bedeutung. Datenmanagement in diesem Sinne umfasst alle Disziplinen, die notwendig sind, um Daten als wertvolles Gut sicher und effizient zu verwalten.

Auch wenn Daten aus unterschiedlichen Quellen stammen, sollten sie idealerweise an einer zentralen Stelle zusammengeführt und verwaltet werden. Moderne Datenmanagement-Applikationen verwalten Daten über den gesamten Lebenszyklus und zeigen heterogene Datenbestände in einer einheitlichen Ansicht, natürlich in Echtzeit. Wenn Datenbestände von der Erfassung bis zur Löschung zentral gesteuert und mit einer unternehmensweiten Datenmanagementstrategie aufeinander abgestimmt werden, lässt sich der Wert der Datenbestände maximieren.

Erfolgreiches Datenmanagement muss:

- Den gesamten Datenlebenszyklus betrachten
- Zugriff auf alle erfassten Daten ermöglichen
- Die Datenqualität sicherstellen
- Eine einheitliche Sicht auf alle Datenbestände bieten, um eine systemübergreifende und unternehmensweite Integration zu ermöglichen
- Die Verarbeitung, Konvertierung und Anreicherung von Daten berücksichtigen
- Grundsätze und geeignete Verfahren für die Datenverwaltung festlegen, um umfassende Datensicherheit und Datenschutz sicherzustellen

3.1 Wie kann Datenmanagement konkret umgesetzt werden?

Im Bild sieht man das Modell eines Datenmanagement-Konzepts. Ein solches Konzept betrachtet Datenbestände von der rechtskonformen Erfassung bis zur sachgerechten Löschung der Daten. Es kann sehr komplex sein und die Zusammenarbeit zahlreicher Abteilungen und Funktionen erfordern. Daher ist Data Governance – die Umsetzung einer sicheren Handhabung von Daten im gesamten Betrieb – eine Querschnittsaufgabe, die alle Hierarchieebenen betrifft. Sie beinhaltet in erster Linie Risikominimierung, Durchsetzung von Compliance und Sicherheitsfragen.

Ein Datenmanagement-Konzept muss die folgenden Bereiche berücksichtigen:

Datenerwerb
Erwerb von Daten verschiedener Struktur, Umfang und Geschwindigkeit aus verschiedenen Quellen, z. B. IoT, Unternehmen, Social Media.

Datenübertragung
Verteilung von Daten von der Erfassung bis zur Speicherung oder Endanwendung. Diese Funktion kann auch eine Pipeline zur Datenanreicherung enthalten, um die Datenqualität zu verbessern.

Datenspeicherung
Speicherung von Daten für unterschiedliche Anforderungen. Zwischenspeicherung von Daten (Storage Sink oder Staging Area), wirtschaftliche Speicherung großer Datenmengen (Data Lake oder Reservoir), primäre Speicherung strukturierter Daten (Data Warehouse) und Speicherung kritischer Unternehmensdaten (Enterprise Data Warehouse).

Datenmanagement
Management von Daten über mehrere Datenspeicher hinweg. Implementierung von Governance-Strukturen zur Qualitätssicherung, sowie zum Management der Daten über den gesamten Lebenszyklus hinweg. Bereitstellung und Anpassen von Daten aus verschiedenen Quellen, so dass diese gemeinsam verwendet werden können (ETL).

Datenzugriff
Eine Zugriffsebene. Sie ermöglicht die Übertragung von Daten zwischen verschiedenen Anwendungen sowie die Virtualisierung von Daten bei Bedarf.

Datenanalyse und -verarbeitung
Eine Anwendungsoberfläche für die Verwendung der Daten (Big Data Sandbox Discovery, Business Analytics, Datenmodellierung und -transformation).

Data Governance
Dezentrale Funktionen zur Implementierung aller Datenmanagement- und Sicherheitsprozesse. Verantwortlich für Risikomanagement, Compliance und Sicherheit.

Dieses Modell einer Datenmanagement-Architektur ist allgemein und damit nicht anwendungsspezifisch. Es berücksichtigt keine spezifischen Anforderungen von privaten oder öffentlichen Clouds, die Bedingungen vor Ort oder die Besonderheiten hybrider Implementierungen.

3.2 Wie kann Data Governance konkret umgesetzt werden?

Data Governance ist eine umfassende Disziplin, die alle Ebenen der Unternehmung berührt. Während technische Lösungen durch Richtlinien gesteuert werden müssen, müssen solche Richtlinien zugleich auf die Bedürfnisse der Organisation ausgerichtet sein. Es werden geeignete Kennzahlen benötigt, um die Effektivität des Datenmanagements zu überwachen und kontinuierliche Verbesserungen zu ermöglichen. Und vom Standort eines Cloud-Servers können Datenschutz und andere relevante regionale Gesetze und Vorschriften abhängen, so dass Data Governance auch geografisch betrachtet werden muss.

Data Governance stellt sicher, dass Richtlinien, Prozesse und Verfahren sicher und effizient funktionieren, z. B.:

- Einhaltung gesetzlicher, regulatorischer und datenschutzrechtlicher Bestimmungen
- Sicherheitsmaßnahmen für Konten, Netzwerke und Daten
- Werterhalt und Wertmaximierung, wie in den Grundsätzen zum Wert von Daten definiert

Umsetzung der Grundsätze zum Wert von Daten (siehe Abschnitt 2.3) in der Data Governance:

- Der Wert der Daten steigt mit der Nutzung: Zugriff auf Daten sicherstellen, durch Bereitstellung, Nutzerzugriff und -autorisierung
- Der Wert der Daten nimmt mit der Zeit ab: Umsichtiges Management von Daten über den gesamten Lebenszyklus
- Der Wert der Daten steigt mit der Qualität: Sicherstellen, dass Daten vollständig, genau und vertrauenswürdig sind. Datenanreicherung und -herkunft, Metadaten etc.
- Der Wert der Daten steigt, wenn sie mit anderen Daten integriert werden: Kombinieren von Daten durch geeignete Technologien und Richtlinien

Data Governance, Risikomanagement, Compliance und Sicherheit müssen im Unternehmen daher idealerweise als vertikale Funktion über alle Ebenen hinweg dargestellt werden. Governance-Richtlinien müssen Top-Down durch alle Ebenen gesteuert und schließlich in der Datenarchitektur technisch umgesetzt werden. Präzise definierte organisatorische Rollen und Verantwortlichkeiten sind notwendig, um effektive Richtlinien zu entwickeln, zu implementieren und durchzusetzen.

Zu den Schlüsselrollen gehören:

Governance-Gremium
Für die Entwicklung von Richtlinien, Vorgaben und Strategien sorgt ein multidisziplinäres Team mit exekutiven Befugnissen. Es besteht aus Vertretern der Leitungsebene (z. B. ein CIO), sowie verantwortlichen Mitarbeitern aus Sicherheits-, Datenschutz- und Compliance-Teams und greift zusätzlich auf technisches Fachwissen aus IT-Management, Datenmanagement und verwandten Funktionen zu. Das Team berichtet an den Information Owner und gibt dem Custodian die strategische Richtung vor.

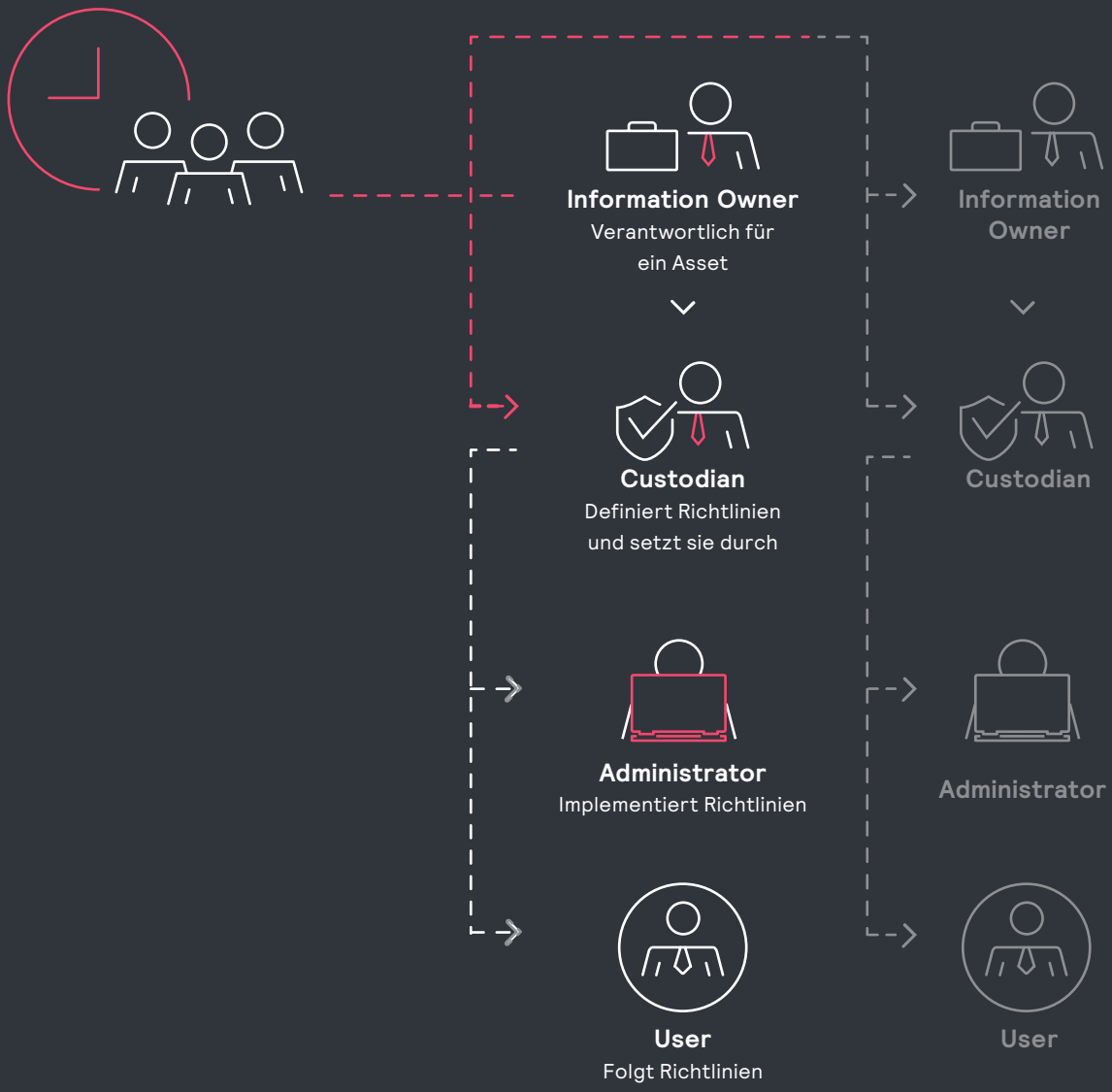
Information Owner
Genehmigt die vom Governance-Gremium aufgestellten Regeln und ist verantwortlich für die Gesamtheit der Datenbestände. Ein Information Owner delegiert die Umsetzung an den Custodian.

Custodian
Empfängt Richtlinien vom Governance-Gremium. Definiert konkrete Regeln für den Umgang mit den Assets und setzt diese im Namen des Information Owners durch. Der Custodian delegiert die Implementierung der Regeln an den Administrator.

Administrator
Implementiert die Regeln für alle Assets und berichtet an den Custodian.

User
Befolgt die Regeln. Gibt Anforderungen und Feedback an den Custodian.

Als User fungiert oft eine Unternehmensgruppe oder eine Unterorganisation. Innerhalb einer Unternehmensgruppe kann es mehrere Information Owner geben. Die Rollen Custodian und Administrator können geschäftsgruppenübergreifend sein. Um Silobildung zu vermeiden, sollten Governance-Richtlinien nicht nur in einzelnen Unternehmensgruppen eingeführt werden. Stattdessen braucht es ein geschäftsbereichsübergreifendes Führungsorgan mit Exekutivbefugnis, das Governance-Richtlinien festlegt und den Informationsaustausch fördert. Erfolgreiche Data Governance erfordert die Aus- und Weiterbildung aller Mitarbeiter sowie eine Unternehmenskultur, die Data Governance-Grundsätze und -Werte anerkennt und unterstützt.



3.3 Überlegungen zu unternehmensübergreifendem Datenmanagment und Data Governance

Die oben skizzierten Modelle beschreiben den „Idealzustand“ für Data Management und Data Governance innerhalb einer Organisation (Stadt/Unternehmen). Zusätzliche Herausforderungen bringt das übergreifende Datenmanagement zwischen Städten, Unternehmen und Partnern mit sich:

- Um die semantische Interoperabilität zwischen den Organisationen zu gewährleisten, sind Standards notwendig, z. B. für Metadaten und Ontologien (die formale Benennung und Definition der Typen, Eigenschaften und Zusammenhänge von Datenbeständen).
- Offene Architekturen und APIs sind erforderlich, um den Datenaustausch zwischen verschiedenen Systemen in verschiedenen Organisationen zu ermöglichen.
- Um Datenintegrität, -wert und -verfügbarkeit im gesamten Ökosystem zu gewährleisten, sind unternehmensübergreifende Governance-Richtlinien erforderlich. Dies kann entweder nach einem zentralisierten Top-Down-Ansatz erfolgen, oder mit einem dezentralisierten Ansatz, unterstützt durch automatisierte Transaktionen und Governance-Management durch Blockchain-ähnliche Technologien.

04.
Datenschutz und Datensicherheit

Datenschutz bezeichnet allgemein formuliert, das Recht des Einzelnen, seine persönlichen Daten für sich zu behalten. Dazu gehören z. B. (aber nicht ausschließlich) Daten, die auf Social Media geteilt werden, sowie jede Art von demographischen oder persönlichen Daten. Vom Datenschutz betroffene Daten in einem intelligenten System könnten zum Beispiel Arbeitnehmerdaten wie Kommen- und Gehenzeiten, Gehalts- und andere Personaldaten sein oder auch die Interessen und Vorlieben von Bürgern, ihre Bewegungen in der Stadt, die Einkaufsgewohnheiten eines Kunden oder seine Kredit- und Bankdaten.

Bei der Datensicherheit geht es hingegen vornehmlich um den Schutz eines Unternehmens, einer Organisation oder einer Behörde vor unerwünschtem externen Zugriff auf die eigenen Systeme. Während die Ziele von Datenschutz und Datensicherheit zum Teil übereinstimmen können, sagt der Schutz der Daten vor Cyberangriffen (Datensicherheit) noch nichts darüber aus, ob diese Daten auch vor dem unerlaubtem Zugriff durch Mitarbeiter geschützt sind oder sogar als zusätzliche Einnahmequelle verkauft werden (Datenschutz).

4.1 Welche Arten von Daten müssen geschützt werden?

Um zu definieren, mit welcher Sensibilität bestimmte Daten gehandhabt werden müssen, ist folgende Kategorisierung hilfreich:

Datenschutzrelevante Daten
Persönlich identifizierbare und persönlich sensible Daten. Durch Gesetze und ethische Grundsätze besonders geschützt.

Vertrauliche Daten und Geschäftsgeheimnisse
Geschäftsrelevante Daten wie Strategien, Pläne, Formeln, Rezepte und operative Prozesse können ganz oder teilweise vertraulich sein, abhängig von den Richtlinien und Vereinbarungen eines Unternehmens mit Partnern und anderen Dritten.

Öffentliche Daten
Daten ohne Datenschutz- oder Vertraulichkeitsprobleme. Diese Daten können ohne Einschränkungen gesammelt und weitergegeben werden.

4.2 Rechtliche und ethische Risiken erkennen

Die Erhebung, Überwachung, Verarbeitung und Speicherung von Daten aus intelligenten Systemen kann rechtliche und ethische Risiken bergen. Der potenzielle Nutzen der gesammelten Daten muss immer abgewogen werden gegenüber dem potenziellen Schaden, den die Sammlung, Speicherung und Nutzung dieser Daten für die Privatsphäre von Einzelpersonen und Gruppen sowie ethische Normen und Standards der Gesellschaft haben könnte. Dabei müssen die Belange aller möglicherweise betroffenen Parteien berücksichtigt werden. Es ist daher wichtig, genau abzuwägen, 1) welche Daten gesammelt werden, 2) welche mögliche Relevanz diese Sammlung für den Datenschutz hat und 3) welche Mittel zur Anonymisierung ggf. ergriffen werden können, um Rückschlüsse auf einzelne Personen wirksam zu verhindern.

4.3 Sensible Daten durch geeignete Verfahren anonymisieren und schützen

Es gibt eine Reihe von Mechanismen und Technologien, um personenbezogene und vertrauliche Daten zu schützen:

Bei der Anonymisierung werden personenbezogene Daten aus Datensätzen entfernt oder maskiert.

Bei der Pseudoanonymisierung ersetzen Pseudonyme (künstliche Identifikatoren) identifizierbare Elemente in Datensätzen. Ist es erforderlich, die anonymisierten Daten zu einem späteren Zeitpunkt erneut identifizieren zu können, kann ein Code zur Umkehrung der Verschlüsselung an einem separaten, sicheren Ort aufbewahrt werden.

Das Verfahren k-Anonymity unterdrückt (entfernt) und/oder verallgemeinert (durch eine breitere Kategorie ersetzt) Datenpunkte so, dass jede in einem Datensatz enthaltene Person nicht von mindestens k-1 Personen unterschieden werden kann, deren Informationen auch im Datensatz erscheinen. Zum Beispiel werden Daten in einem Feld durch Sternchen ersetzt (Unterdrückung) oder das spezifische Alter von Personen mit einem Altersbereich, in den mehrere Personen fallen (z. B. zwischen 35 und 50 Jahren), ersetzt (Verallgemeinerung). Der Wert von k bestimmt, wie viele nicht unterscheidbare Datensätze der k-Anonymitätsprozess erzeugen wird. Beispielsweise würde die 2-Anonymität sicherstellen, dass der Datensatz einer Person nicht von mindestens einer anderen Person im Datensatz unterschieden werden kann (k=2 und 2-1 = 1), während die 3-Anonymität sicherstellen würde, dass der Datensatz einer Person nicht von mindestens zwei anderen Personen im Datensatz unterschieden werden kann (k gleich 3 und 3-1 = 2).

Auch mit Hilfe der Datenstörung kann die Vertraulichkeit der einzelnen Datensätze sichergestellt werden. Diese Datensicherheitstechnik versieht Datenbanken mit einem „Rauschen“. Dies können Werteverzerrungsansätze sein, die eine Art Randomisierungsverfahren direkt auf die Werte in einem Datensatz anwenden, oder Wahrscheinlichkeitsverteilungsansätze, die eine Art Algorithmus zur Transformation der Daten verwenden. Die Datenstörung ermöglicht es dem Benutzer, wichtige, nicht verzerrte Zusammenfassungsinformationen zu ermitteln. Diese Methode wird häufig verwendet, um die Privatsphäre von elektronischen Gesundheitsakten zu schützen.

Differential Privacy, eine weitere vielversprechende Technik, beinhaltet Mechanismen, die verhindern, dass Angreifer unterscheiden können, ob eine bestimmte Person in einer Datenbank enthalten ist oder nicht. Sie ermöglicht möglichst präzise Rückschlüsse auf eine Gesamtbevölkerung (statistische Verteilung), ohne dabei etwas über einzelne Personen preiszugeben.

05.
Wie ist ein sicheres Beleuchtungssystem konzipiert?

Um vertrauliche Unternehmensdaten, Kundendaten und andere Unternehmenswerte zu schützen, müssen vernetzte Systeme sicher konzipiert sein. Um sicherzustellen, dass das System als Ganzes sicher ist, wird es ganzheitlich betrachtet — einschließlich aller beteiligten Personen und Prozesse:

1) **Ein sicheres Beleuchtungssystem entwickeln**
   Was müssen Systemarchitekten tun, um ein sicheres System zu entwerfen?
2) **Sichere Entwicklungsprozesse**
   Wie können alle relevanten Sicherheitsaspekte in allen Phasen des Entwurfs, der Implementierung und des Einsatzes berücksichtigt werden?
3) **Sicherheit über den gesamten Lebenszyklus**
   Wie kann die Sicherheit in allen Phasen der Systemlebensdauer gewährleistet werden: von der Herstellung bis zur Inbetriebnahme, während der Wartung sowie während und nach der Außerbetriebnahme?

5.1 Ein sicheres Beleuchtungssystem entwickeln

Der erste Schritt zur Entwicklung eines sicheren Systems ist die Bestimmung seiner Angriffsfläche. Die Angriffsfläche eines Systems ist formal definiert als die Summe der Angriffsflächen der einzelnen Komponenten des Systems – inklusive ihrer Schnittstellen – sowie aller Angriffsvektoren. Ein Angriffsvektor bezeichnet einen möglichen Angriffsweg sowie die Technik, die ein unbefugter Eindringling verwenden kann, um in ein fremdes Computersystem einzudringen. Auf dieser Basis können mögliche Risiken beurteilt, zu sichernde Komponenten identifiziert und relevante Sicherheitsmaßnahmen sowie sinnvolle (externe) Penetrationstests definiert werden. Das Diagramm zeigt eine typische, etwas vereinfachte Architektur eines Beleuchtungssystems für den Innenbereich (für Systeme wie Straßen-, Fassadenbeleuchtung, u. ä. grundsätzlich ähnlich). Seine Angriffsfläche besteht im Wesentlichen aus sieben Komponenten:

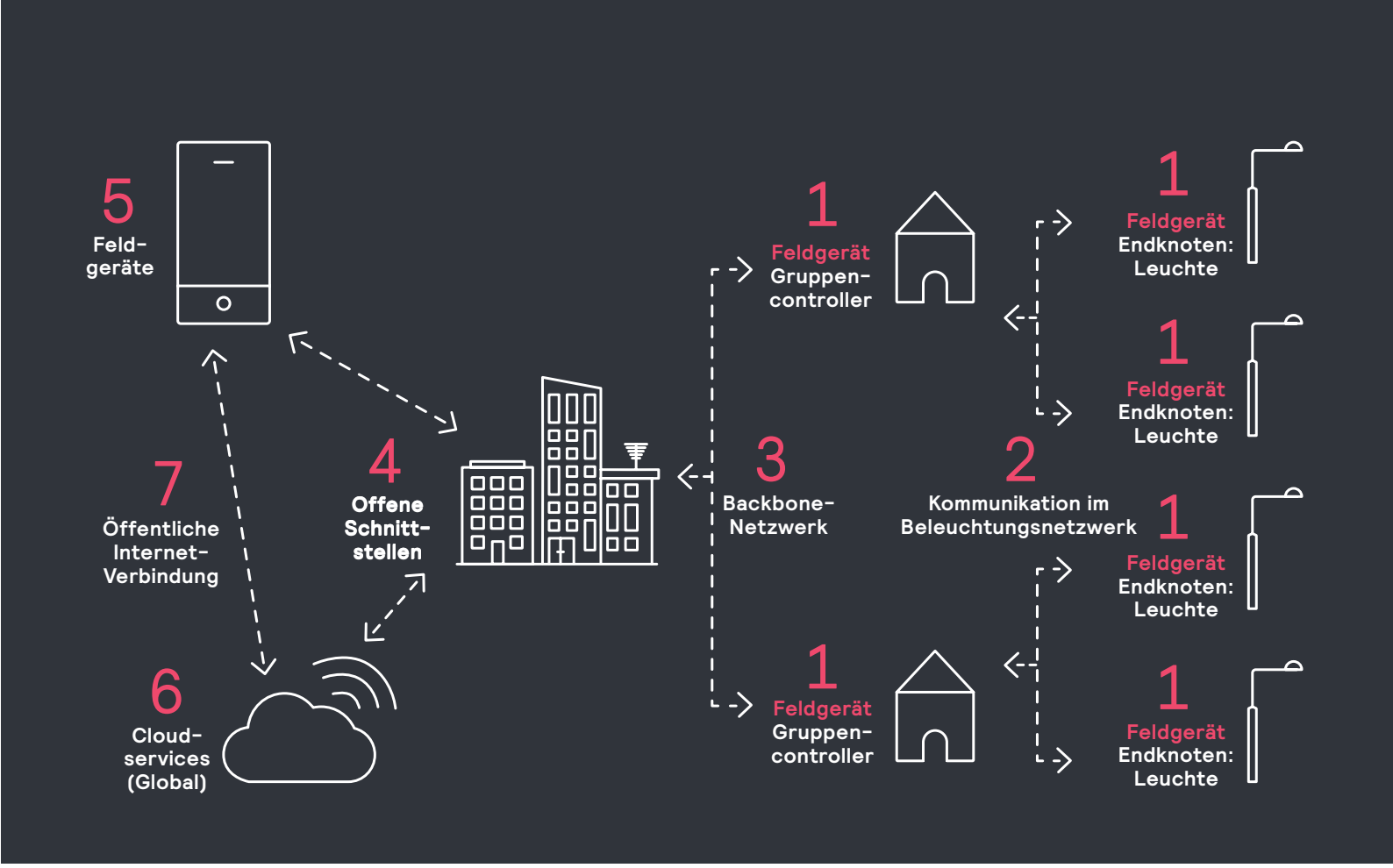
5.1.1 Feldgeräte

Feldgeräte (1 in der Grafik) sind entweder Endknoten (Leuchten, die mit anderen Endgeräten kommunizieren) oder Gruppencontroller (Geräte, die zwischen dem Leuchten- und dem IP-Netzwerk als Schnittstelle fungieren). Feldgeräte müssen einfach zu installieren,bei Bedarf austauschbar sein und bleiben typischerweise mehrere Jahrzehnte in Betrieb.

Feldgeräte sind anfällig für direkte, physische Hacker-Angriffe, da sie z. B. in öffentlich zugänglichen Bereichen installiert sind. Sie müssen daher so konzipiert sein, dass die Kompromittierung eines Gerätes nicht zu einer Gefährdung des gesamten Systems führen kann, d. h. Änderungen an einem Feldgerät dürfen sich nur auf das Gerät selbst, aber niemals auf das gesamte System auswirken (Containment). Indem Debug-Schnittstellen im Gerät deaktiviert bzw. mit einem Passwort geschützt werden, können die Auswirkungen von Angriffen auf Hardwarekomponenten eingedämmt werden. Encryption Keys werden niemals unverschlüsselt von einer Hardwarekomponente auf eine andere übertragen und Schlüsseldaten nicht in einem Speicher abgelegt, der von Angreifern leicht ausgelesen werden kann. Enthält ein Speicher Encryption Keys, wird dieser nach Beendigung der Verschlüsselung so schnell wie möglich gelöscht.

Um zu verhindern, dass Angreifer Seitenkanalangriffe durchführen können, z. B. indem sie Störsignale einspeisen, den Stromverbrauch messen oder das Timing beeinflussen, enthalten hochwertige Systeme speziellen Soft- und Hardware-Schutz.

Feldgeräte müssen durch regelmäßige Updates gesichert werden, weil sie über einen sehr langen Zeitraum im Einsatz sind. Da Angreifer das System mit unechten Firmware-Updates zeitweise oder dauerhaft unbrauchbar machen könnten, überprüfen sichere Feldgeräte automatisiert die Echtheit von Updates.



5.1.2 Sicheres Leuchten-Netzwerk
Im Beleuchtungsnetzwerk (2 in der Grafik) kommunizieren Leuchten untereinander und mit Gruppencontrollern. Durch unerlaubten Zugriff auf das Netzwerk kann sowohl die Verfügbarkeit als auch die Vertraulichkeit des Netzwerks gefährdet sein. Um die Verfügbarkeit zu sichern, darf es keinen Systembestandteil geben, dessen Ausfall den Ausfall des gesamten Systems nach sich zieht (Single Point of Failure). Aus diesem Grund kommunizieren Feldgeräte stets über mehr als einen Kommunikationsweg. Moderne Protokolle wie Zigbee sichern die Vertraulichkeit der Kommunikation standardmäßig durch einen Verschlüsselungsalgorithmus sowie den Schutz vor Wiederholung einmal abgerufener Nachrichten (Replay Protection).

5.1.3 Sicheres Backbone-Netz
Der besonders schützenswerte Kernbereich des Beleuchtungsnetzwerks (Backbone-Netz, 3 in der Grafik) umfasst die (IP-basierte) Kommunikation zwischen Gruppencontrollern und Lichtmanagementsystem. Die am Backbone angeschlossenen Geräte nutzen komplexere Sicherheitsstandards und -protokolle als die Feldgeräte, z. B. TLS (ein Upgrade von SSL) und VPNs, um die Authentizität von Kommunikationspartnern zu überprüfen und den Schutz der Daten sicherzustellen. Um die Gefährdung des Backbone gegenüber dem Rest des internen Netzwerks weiter zu reduzieren, ist die Isolierung von Datenströmen mit Hilfe virtueller lokaler Netzwerke (VLAN) möglich.

5.1.4 Sichere lokale Schnittstelle zum Lichtmanagementsystem
Schnittstellen ermöglichen es, das Beleuchtungssystem aus dem lokalen IT-Netzwerk heraus zu steuern und zu warten sowie ggf. an die lokale Haustechnik anzubinden (4 in der Grafik). Da diese Dienste normalerweise auf einem lokalen Webserver laufen, muss dessen Sicherheit ebenfalls gewährleistet sein. Eine ordnungsgemäße Authentifizierung und Autorisierung aller Nutzer schützt die Integrität des Systems und der Systemprotokolle. Schutz vor gängigen Angriffen aus dem Netz bieten geeignete Antivirus- und Schutzprogramme sowie regelmäßige Patches. Sichere Programmierung sowie eine regelmäßige risikobasierte Bedrohungs- und Schwachstellenbewertung komplettieren das Bild[12].

5.1.5 Sichere Apps und webbasierte Anwendungen
Auch Mobile Apps und Browseranwendungen fungieren als Schnittstellen zum Beleuchtungssystem. Da die Absicherung des Geräts, auf dem die Anwendung ausgeführt wird, unbekannt ist, werden auf solchen Geräten keine Sicherheitszertifikate oder sensible Daten gespeichert. Apps werden grundsätzlich als separates Produkt behandelt und vor Veröffentlichung auf bestimmte Schwachstellen (z. B. OWASP Mobile Top 10) getestet. Für einen sicheren Browser-Zugriff aus dem Web testen vertrauenswürdige Anbieter auf häufige Schwachstellen wie Cross-Site-Scripting, Cross-Site Request Forgery usw.

5.1.6 Sichere Cloud-basierte Lichtmanagement-Services

Ein häufiger Vorbehalt gegenüber Cloud-basierten Diensten (6 in der Grafik) ist die Angst vor möglichen Angriffen über das Internet. Dennoch setzen heute alle namhaften Anbieter auf Cloud-Dienste, da die Nachteile der Technologie durch ihre zahlreichen Vorteile mehr als aufgewogen werden. So ist es viel einfacher und schneller, ein zentrales, Cloud-basiertes System durch regelmäßige Sicherheitsupdates wirksam vor Angriffen zu schützen, als viele einzelne, lokale Systeme. Da es sich dennoch um potentiell besonders gefährdete Komponenten handelt, erfordern Cloud-basierte Lichtmanagement-Services äußerste Sorgfalt in allen Sicherheitsaspekten. Das Sicherheitsdesign eines sicheren Cloud-Services ist skalierbar, um eine maximale Verfügbarkeit zu gewährleisten und wird durch externe Penetrationstests und Audits nach etablierten Standards ergänzt.

5.1.7 Sichere Internetverbindung

Auch eine öffentliche Internetverbindung (7 in der Grafik) kann bei der Vernetzung von Beleuchtungskomponenten (z. B. von der Cloud zu einer mobilen App) eine Rolle spielen und muss dementsprechend geschützt sein. Die im Web bewährten Protokolle wie TLS und IPSec bieten einen bewährten und sicheren Standard für die Vernetzung von Kommunikationsschnittstellen.

5.2 Sichere Entwicklungsprozesse

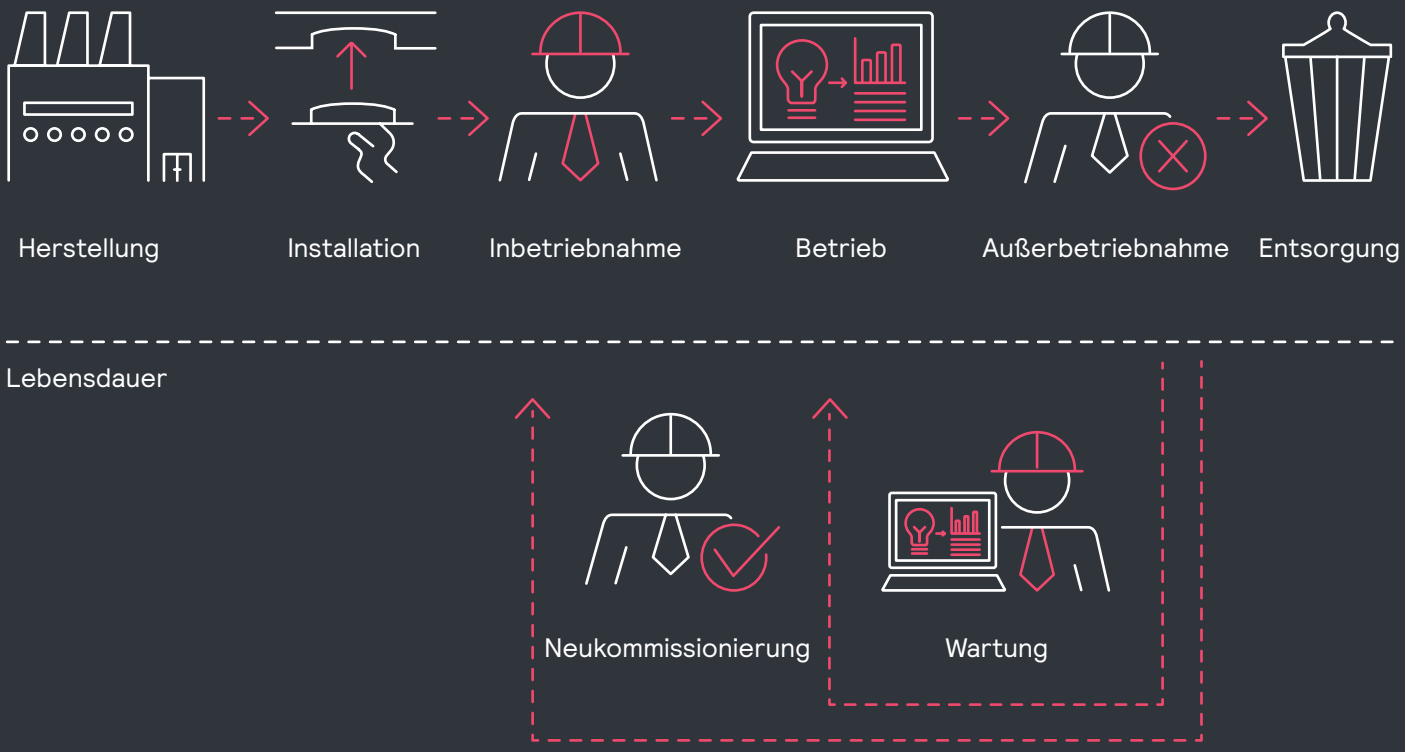
Als „Secure Engineering“ bezeichnet man die Entwicklung eines sicheren Beleuchtungssystems von der Planung, über den Entwurf bis hin zur Implementierung und dem Einsatz des Systems. Einen sehr hohen Standard ermöglicht Secure Engineering nach dem vom Open Web Application Security Project (OWASP) entworfenen Security Development Lifecycle (SDL)-Prozess sowie der Security Software Development Life Cycle (SDLC)-Methode. Beide bieten einen kompletten Katalog von Entwicklungsprozessen, Meilensteinen, Arbeitsweisen und Schulungen.

5.3 Sicherheit über den gesamten Lebenszyklus

Der Lebenszyklus eines vernetzten Systems besteht (typischerweise) aus Herstellung, Inbetriebnahme, Wartung, Außerbetriebnahme und Entsorgung. Um die ganzheitliche Sicherheit des Systems zu gewährleisten, müssen Sicherheitsaspekte integraler Bestandteil jeder Lebenszyklusphase sein und alle Phasen lückenlos verbunden werden. Denn die Sicherheit des gesamten Systems ist nur so stark wie das schwächste Glied. Basis für die Sicherheit des Systems bildet zunächst die sichere Herstellung der Bauteile mit eindeutigen Identifikationsmerkmalen. Diese Identifikationsmerkmale werden zusammen mit einer geeigneten Schlüsselverwaltung im Backend sicher auf dem Gerät gespeichert. Auf diesen Original-Fertigungsschlüsseln basieren sowohl Inbetriebnahme und Wiederinbetriebnahme des Systems als auch die Definition des Betriebsverhaltens der Anlage. An der Richtigkeit und Zuverlässigkeit der zugeordneten Schlüssel hängt daher die Betriebssicherheit des Systems. Die Inbetriebnahme wird zusätzlich durch eine Zugangsbeschränkung auf Basis sachgerechter Authentifizierung und Autorisierung abgesichert. Der Betriebszustand als längste Lebenszyklusphase, wird durch sichere Kommunikationsprotokolle, die sichere Authentifizierung und Autorisierung von Benutzern und Updates sowie eindeutige Schlüssel und Kennwörter gesichert.

Auch die Wartung des Systems durch Software-Updates und Gerätewechsel muss gesondert gesichert werden. Eine sichere Außerbetriebnahme von Geräten aus bestehenden Systemen ist nur durch eine Kombination von Betriebs- und Produktionsschlüssel möglich. Und zuletzt wird auch bei der Entsorgung von Geräten durch eine ordnungsgemäße Schlüsselverwaltung verhindert, dass Unberechtigte Zugang zu Schlüsseln und zur Betriebsumgebung erhalten.

Die Anforderungen an die Sicherheit über den gesamten Lebenszyklus des Systems sind für die verschiedenen Verwendungsbedingungen unterschiedlich. Ein sicheres System wird daher individuell für einen bestimmten Einsatzbereich (Bürobeleuchtung, Industriebeleuchtung, Außenbeleuchtung etc.) konzipiert.



Anmerkungen und Quellenverzeichnis

1. „The Internet of Things." **IT Glossary**, Gartner: http://www.gartner.com/it-glossary/internet-of-things/

2. Manyika, James, et al. „Unlocking the potential of the Internet of Things." McKinsey Global Institute, June 2015: http://www.mckinsey.com/businessfunctions/digital-mckinsey/our-insights/the-internet-of-things-thevalue-of-digitizing-the-physical-world

3. „There will be 24 billion IoT devices installed on Earth by 2020." Business Insider, 9 June 2016: http://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5

4. Huijbregts, Rick. „Re-imagining business value in a digital world." Cisco, May 2016.

5. Bauer, Harald, Burkacky, Ondrej, and Knochenhauer, Christian. „Security in the Internet of Things." McKinsey & Company, May 2017: http://www.mckinsey.com/industries/semiconductors/our-insights/security-in-theinternet-of-things

6. Nuttall, Nathan, Goodness, Eric, Hung, Mark, and Geschickter, Chet. „Survey Analysis: 2016 Internet of Things Backbone Survey." Gartner, 5 January 2017: http://www.gartner.com/doc/3563218/survey-analysis--internet-things

7. „The biggest security threats coming in 2017." Wired, 2 January 2017: http://www.wired.com/2017/01/biggest-security-threats-coming-2017/

8. Doctorow, Cory. „Winter Denial of Service attack knocks out heating in Finnish homes." BoingBoing, 8 November 2016: http://boingboing.net/2016/11/08/winter-denial-of-service-attac.html

9. Banafa, Ahmed. „Three Major Challenges Facing IoT." SemiWiki.com, 25 May 2017: http://www.semiwiki.com/forum/content/6796-three-majorchallenges-facing-iot.html

10. Definitions based in part on the Wikipedia entry on data, at http://en.wikipedia.org/wiki/Data

11. „Data Lifecycle Overview." USGS website: http://www2.usgs.gov/datamanagement/why-dm/lifecycleoverview.php

12. Rubens, Arden. „A Closer Look: OWASP Top 10 Application Security Risks."

Mehr über Interact erfahren:
www.interact-lighting.com

interact

WM-Nr. 5524
Stand 01/2019

www.signify.com