ZVEI:
Die Elektroindustrie

Digitalen Wandel gestalten. Vertrauen schaffen.

Leitlinien der deutschen Elektroindustrie für den verantwortungsvollen Umgang mit Daten und Plattformen

Version 2.0

Zentralverband Elektrotechnik- und Elektronikindustrie

ZVEI:
Die Elektroindustrie

Leitlinien der deutschen Elektroindustrie für den verantwortungsvollen Umgang mit Daten und Plattformen

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Abteilung Innovationspolitik
Charlottenstraße 35/36
10117 Berlin

Verantwortlich: Jochen Reinschmidt
Telefon: +49 30 306960-23
E-Mail: jochen.reinschmidt@zvei.org

www.zvei.org

Januar 2020

Vorbemerkung

Mit der Digitalisierung findet ein grundlegender Strukturwandel in Wirtschaft und Gesellschaft statt. Die deutsche Elektroindustrie, die mit ihren Produkten und Lösungen Bindeglied zwischen analoger und digitaler Welt ist, gestaltet diesen Wandel aktiv mit. Die Digitalisierung der Wirtschaft ist die Voraussetzung, um stabil und nachhaltig zu wachsen, sie schafft einen Mehrwert für die Gesellschaft und trägt zur Lösung globaler Herausforderungen bei. Digitalwirtschaft im industriellen Sektor bedeutet, die Konnektivität sowohl von einzelnen Produkten als auch ganzer Infrastrukturen herzustellen, die über Unternehmen hinausgehen und Lieferanten und Kunden einschließen können.

Der „Rohstoff" der digitalisierten Wirtschaft sind Daten. Heute nutzen Unternehmen der Elektroindustrie diese vor allem dafür, bestehende Geschäftsmodelle und Prozesse zu optimieren. Zunehmend jedoch dienen die Daten auch der Entwicklung neuer Geschäftsmodelle. Dadurch entstehen neue Wertschöpfungsstrukturen und Partnernetzwerke.

Dabei kommt digitalen Plattformen auch im industriellen Kontext ein besonders hoher Stellenwert zu. Sie sind die Drehscheiben, auf denen Marktteilnehmer Daten nutzen und austauschen. Kleinen und mittleren Unternehmen (KMU) und Start-ups bieten offene Plattformen eine Chance, sich in die neu entstehenden Ökosysteme einzubringen. Aber die Nutzung und Verarbeitung von Daten und der Betrieb von Plattformen können auch zu Missbrauch und Konflikten führen.

Um das Potenzial von Daten und Plattformen nutzen zu können, ist neben klaren rechtlichen Regelungen vor allem auch der Aufbau von Vertrauen erforderlich. Dafür ist ein gemeinsames Wertefundament nötig, das im praktischen Handeln konsequent umgesetzt wird.

In Deutschland und Europa steht immer der Mensch im Mittelpunkt und mit ihm die aus dem Schutz der Menschenwürde abgeleiteten Grundrechte. Hierbei kommen im Hinblick auf Daten und Plattformen vor allem dem Schutz der Privatsphäre und dem Schutz personenbezogener Daten besondere Bedeutung zu. Zu unserem Wertefundament zählen zudem die Regeln der sozialen Marktwirtschaft, die einen fairen Wettbewerb definieren, sowie die Umsetzung der globalen Nachhaltigkeitsziele der Vereinten Nationen. Hierin sehen wir das Wertefundament der Elektroindustrie, das unser Handeln leitet und das wir im internationalen Wettbewerb zur Geltung bringen.

Die vorliegenden Leitlinien konkretisieren auf Basis dieses Wertefundaments, woran sich die Elektroindustrie bei der Nutzung von Daten und bei der Gestaltung von Plattformen orientiert.

Wir verstehen die Formulierung der Leitlinien als kontinuierlichen Prozess und als Gesprächsangebot. Auf Grundlage der Leitlinien werden wir uns aktiv in den Dialog über die Rahmenbedingungen der Digitalwirtschaft einbringen. Dass die Leitlinien praktisch umgesetzt werden, verdeutlichen die Beispiele aus der Unternehmenspraxis von ZVEI-Mitgliedsunternehmen im Anhang.

Zehn Leitlinien zum verantwortungsvollen Umgang mit Daten und Plattformen

1 Personenbezogene Daten sind besonders schützenswert

Die informationelle Selbstbestimmung des Einzelnen ist für die Unternehmen der deutschen Elektroindustrie eine zentrale Grundlage der Digitalwirtschaft. Die durch die Datenschutzgrundverordnung (DSGVO) gesetzten Anforderungen an den Datenschutz sehen wir grundsätzlich als einen Wettbewerbsvorteil im internationalen Standortwettbewerb.

2 Fairen Datenzugang ermöglichen

Grundsätzlich sollte jeder Datenerzeuger entscheiden können, wie er mit den von ihm erzeugten Daten umgeht. Der ZVEI lehnt eine Monopolisierung von Daten sowie die Schaffung eines Dateneigentumsrechts ab. Der Zugang und die Nutzung sollten in der Regel zwischen Partnern in fairen Verträgen geregelt werden, die die Interessen beider Seiten in angemessener Weise berücksichtigen. So wird sichergestellt, dass Kunden und Geschäftspartner bestimmen und kontrollieren können, auf welche Daten zugegriffen wird und zu welchem Zweck sie genutzt werden.

3 Datensicherheit durch Security by Design und Security-Lifecycle-Management fördern

Für das Teilen und Nutzen von Daten sind der gegen Missbrauch gesicherte Zugang, die sichere Verarbeitung, die Speicherung und Handhabung von Daten sowie die Erhaltung ihrer Integrität und Vertraulichkeit eine Grundvoraussetzung. Die Unternehmen der Elektroindustrie treten daher dafür ein, Sicherheit so umfassend wie möglich durch einen ganzheitlichen Ansatz zu fördern. Dies umfasst sowohl Security by Design in der Entwicklungsphase als auch Security-Lifecycle-Management über den gesamten Produkt- und Datenlebenszyklus hinweg.
Auf nicht autorisierte bzw. unberechtigte Zugriffe muss schnellstmöglich reagiert werden.

4 Aus Daten gewonnene Wertschöpfung als wirtschaftlich bedeutsames Gut der Unternehmen behandeln

Digitale Wertschöpfung basiert wesentlich auf der Verarbeitung und Auswertung von Daten, zum Beispiel durch Datenanalysetechniken oder die Anwendung von Künstlicher Intelligenz. Wir betrachten die digitale Wertschöpfung durch Datenverarbeitung und -auswertung als wirtschaftlich bedeutsames und schützenswertes Gut. Dadurch wird ein Anreiz zur Innovation geschaffen und gleichzeitig auch der Schutz von Investitionen sichergestellt.

5 Portabilität und Interoperabilität von Daten für wettbewerbliche Nutzung unterstützen

Die Unternehmen der deutschen Elektroindustrie setzen sich aktiv für Wettbewerb ein. Die Möglichkeit, Daten über verschiedene Erzeugungs- und Anwendungskontexte hinaus parallel nutzen zu können, kann durch die Unterstützung von Datenportabilität mittels interoperabler Datenformate und Informationsmodelle auf Basis frei zugänglicher Standards erreicht werden. Auf diese Weise wird ein Datenaustausch bzw. ein Datenpooling zwischen verschiedenen Anbietern möglich und somit Wettbewerb gefördert.

6 Nachhaltige Nutzung von Daten fördern

Der ZVEI setzt sich für einen möglichst umfassenden Zugang und eine nachhaltige Nutzung von nicht personenbezogenen Daten oder von anonymisierten Daten zum gesellschaftlichen Allgemeinwohl und zur Erreichung der globalen Nachhaltigkeitsziele ein. Dabei müssen wirtschaftliche Interessen und mit der Datenbereitstellung verbundene Kosten angemessen berücksichtigt werden.

7 Open Innovation und Co-Creation stärken

In der datenbasierten Digitalwirtschaft werden aus Wertschöpfungsketten flexible Wertschöpfungsnetzwerke mit neuen Partnerkonstellationen. Insbesondere neue Geschäftsmodelle gehen oftmals mit veränderten Akteurskonstellationen einher und sind vielfach eingebettet in neu entstehende Ökosysteme. Diese bieten Start-ups, KMUs und großen Unternehmen Chancen, gemeinsam an der digitalen Wertschöpfung zu partizipieren. Dabei ist der Schutz des geistigen Eigentums der jeweiligen Partner sicherzustellen.

Um den Aufbau solcher Ökosysteme zu unterstützen, setzt sich der ZVEI für neue Kooperationsformen und Ansätze wie Open Innovation und Co-Creation ein, bei denen der Kunde oder der Lieferant zum Innovationspartner wird.

8 Teilhabe an digitalen Plattformen ermöglichen

Industrielle Plattformen sollten einen diskriminierungsfreien, für alle Interessenten offenen Zugang bieten. Zwar kann es notwendig sein, Qualitätsanforderungen oder technologische Voraussetzungen zu definieren, damit Sicherheit und Funktionsfähigkeit der Plattform sichergestellt werden (zum Beispiel durch die Zertifizierung von Komponenten). Diese dürfen jedoch nicht einseitig zulasten einzelner Marktteilnehmer gehen.

9 Transparenten Betrieb von digitalen Plattformen fördern

Eine Plattform vernetzt verschiedene Akteure, die unterschiedliche Interessen verfolgen können. Dazu gehört auch der Betreiber der Plattform. Es ist die Aufgabe des Plattformbetreibers, diese Interessen allen Plattformnutzern so transparent wie möglich zu machen. Dies gilt insbesondere dann, wenn Inhalte oder Funktionalitäten der Plattform von den Interessen einzelner Akteure beeinflusst werden, wie zum Beispiel die Reihenfolge von Suchergebnissen.

Durch geeignete Opt-in-/Opt-out-Funktionen soll Plattformnutzern die Möglichkeit eingeräumt werden, die Nutzung und Verwertung der von ihnen eingebrachten Daten im Plattformbetrieb nachvollziehen und differenziert steuern zu können.

10 Fairen Wettbewerb zwischen digitalen Plattformen ermöglichen

Die Unternehmen des ZVEI setzen sich aktiv für einen international fairen und innovationsfördernden Wettbewerb zwischen Plattformen ein. Plattformen sollten daher so gestaltet werden, dass keine wettbewerbsschädigenden Lock-in-Mechanismen erzeugt werden, die Nutzern einen Wechsel auf andere Plattformen künstlich erschweren. Insbesondere sollte die Migrationsfähigkeit von Daten sichergestellt und die gleichzeitige Nutzung mehrerer Plattformen ermöglicht werden.

Anhang:
Fallbeispiele aus den ZVEI-Mitgliedsunternehmen

1 Personenbezogene Daten sind besonders schützenswert

Fallbeispiel 1:

Befund24 hat einen Marktplatz zur Vermittlung von Ferndiagnoseleistungen im Gesundheitsbereich eingerichtet. Zum Schutz personenbezogener Daten arbeitet die Plattform nach dem Grundprinzip „Privacy by design and by default" gemäß Artikel 25 der Datenschutzgrundverordnung (DSGVO). Die Entwicklung der Befund24-Marktplatzlösung erfolgt dabei gemäß dem Cybersecurity-Entwicklungsprozess von Siemens Healthineers, der unter anderem eine Threat-and-Risk-Analyse (TRA), die Implementierung von Sicherheitsstandards sowie Sicherheitsprüfungen umfasst. Zusätzlich werden regelmäßig externe Penetrationstests durchgeführt. Patientendaten liegen immer verschlüsselt in der Befund24-Cloud. Patienten können etwaige Auskunftsansprüche gegenüber dem Krankenhaus oder Ersteller des Befunds geltend machen.

Weitere Informationen: https://www.befund24.de

Fallbeispiel 2:

Die Bundesdruckerei bietet künftig Datentreuhänderdienste im Gesundheitsbereich (Pseudonymisierung, Berechtigungs- und Einwilligungsmanagement) als Service über eine digitale Plattform an. Mithilfe einer Vertrauensstelle können personenbezogene Daten und Pseudonyme sicher verwaltet werden. Den Nutzdaten werden ausschließlich Pseudonyme zugeordnet. Über ein Berechtigungsmanagement kann der Datengeber entscheiden, wer welche Daten zur Einsicht erhält bzw. diese Berechtigung widerrufen.

Weitere Informationen: https://www.bundesdruckerei.de/de/Themen-Trends/Magazin/Der-Datentreuhaender-als-neutrale-Schutzinstanz

Fallbeispiel 3:

Eaton verwendet unternehmensweit eine einheitliche Richtlinie zum Schutz personenbezogener Daten. Da der Konzern global agiert und es keine belastbare internationale Gesetzgebung zum Schutz personenbezogener Daten gibt, hat Eaton eine für alle Standorte und Tochtergesellschaften weltweit geltende Richtlinie eingeführt, die auf der europäischen Datenschutzgrundverordnung basiert. Damit soll sichergestellt werden, dass mit personenbezogenen Daten von Kunden und Mitarbeitern weltweit gemäß den zurzeit höchsten verfügbaren Sicherheitsstandards umgegangen wird.

Weitere Informationen: https://www.eaton.com/content/eaton/us/en-us/company/policies-and-statements/privacy-cookies-and-data-protection.html

Fallbeispiel 4:

Siemens setzt für MindSphere weltweit eine einheitliche Datenschutzlösung um, die unter Berücksichtigung der Maßstäbe der Datenschutzgrundverordnung (DSGVO) entwickelt wurde. Jedem Kunden wird mit den MindSphere Data Privacy Terms der Abschluss von Vertragsklauseln angeboten, die ihm die volle Kontrolle über die auf MindSphere verarbeiteten Inhalte mit personenbezogenen Daten geben. Dazu zählt die Transparenz über alle eingesetzten Subdienstleister mit Zugriff auf personenbezogene Daten und Auditrechte, um die Einhaltung der vertraglichen Versprechen und datenschutzrechtlichen Anforderungen prüfen zu können. Die MindSphere Data Privacy Terms gelten weltweit und ermöglichen so Compliance sowohl mit europäischem Datenschutzrecht als auch mit lokalen Datenschutzanforderungen in anderen Rechtsordnungen.

Weitere Informationen: https://www.plm.automation.siemens.com/media/global/en/Siemens_MindSphere_Whitepaper_tcm27-9395.pdf

2 Fairen Datenzugang ermöglichen

Fallbeispiel 1:

Die Bundesdruckerei bietet sich als Vertrauenspartner an, um den Datenaustausch zwischen Organisationen zu ermöglichen. Denn wenn sich Organisationen beim Datenaustausch nicht vollständig vertrauen bzw. der direkte Datenaustausch technisch oder rechtlich nicht möglich ist, kann dies den Aufbau von datengetriebenen Geschäftsmodellen verhindern. Als Vertrauenspartner beider Organisationen schaltet sich der Datentreuhänder dazwischen. Die Originaldaten werden dem Datentreuhänder übermittelt und nach der vereinbarten Data Governance analysiert und verarbeitet. Ausschließlich das Ergebnis wird an die berechtigte Organisation weitergegeben.

Weitere Informationen: https://www.bundesdruckerei.de/de/Themen-Trends/Magazin/Der-Datentreuhaender-als-neutrale-Schutzinstanz

Fallbeispiel 2:

Osram hat die Software-Plattform Lightelligence etabliert, die die cloudbasierte Sammlung und Auswertung einer Vielzahl von Daten aus unterschiedlichen Quellen ermöglicht. Nur die jeweiligen Kunden selbst haben die Kontrolle über ihre Daten inne. Mittels eines granularen, transparenten Berechtigungskonzepts wird sichergestellt, dass nicht ungewollt Daten an Dritte herausgegeben werden. Zudem ist es möglich, den Anwendungen Dritter nur die Rechte zu geben, die für deren Funktion notwendig sind. Es existiert eine strikte Trennung zwischen den einzelnen Kunden, die durch verschiedene technische Maßnahmen verifiziert und regelmäßig getestet wird. Osram greift nicht auf die Daten der Kunden zu und nutzt diese nicht für eigene Zwecke.

Weitere Informationen: https://www.lightelligence.io

3 Datensicherheit durch Security by Design und Security-Lifecycle-Management fördern

Fallbeispiel 1:

Befund24 hat einen Marktplatz zur Vermittlung von Ferndiagnoseleistungen im Gesundheitsbereich eingerichtet. Zum Schutz personenbezogener Daten arbeitet die Plattform nach dem Grundprinzip „Privacy by design and by default" gemäß Artikel 25 der Datenschutzgrundverordnung (DSGVO). Die Entwicklung der Befund24-Marktplatzlösung erfolgt dabei gemäß dem Cybersecurity-Entwicklungsprozess von Siemens Healthineers, der unter anderem eine Threat-and-Risk-Analyse (TRA), die Implementierung von Sicherheitsstandards sowie Sicherheitsprüfungen umfasst. Zusätzlich werden regelmäßig externe Penetrationstests durchgeführt. Patientendaten liegen immer verschlüsselt in der Befund24-Cloud. Patienten können etwaige Auskunftsansprüche gegenüber dem Krankenhaus oder Ersteller des Befunds geltend machen.

Weitere Informationen: https://www.befund24.de

Fallbeispiel 2:

Bei Eaton wird jedes digital steuerbare oder vernetzte Produkt oder System bereits bei der Entwicklung im Rahmen eines cybersecurityorientierten Lebenszyklus durch ein globales Center of Excellence (CoE) für Produktcybersicherheit getestet. Vor einer finalen Vermarktung dieser Produkte und Systeme muss dieses Verfahren erfolgreich bestanden werden. Das CoE fungiert, gemeinsam mit den Produktverantwortlichen, als Genehmigungsgremium.

Weitere Informationen: https://www.eaton.com/us/en-us/markets/innovation-stories/Managing-Cybersecurity-Risks.html

Fallbeispiel 3:

Die hohen Sicherheitsanforderungen an automatisierte und vernetzte Fahrzeuge haben großen Einfluss auf das Design von Infineon-Chips als kleinste elektronische Elemente im Fahrzeug. In modernen Fahrzeugen mit 100 und mehr Steuergeräten schützen sogenannte Sicherheitsanker gegen Manipulation oder Diebstahl von Daten. Diese Halbleiterchips mit hochsicheren Verschlüsselungsmechanismen sind entweder direkt in die zahlreichen Mikrocontroller integriert oder als diskrete Sicherheitscontroller eingebaut. Diese Chips schützen gegen Manipulations- und Eindringversuche, sodass eine Verletzung der Datensicherheit abgewehrt werden kann.

Weitere Informationen: https://www.infineon.com/cms/de/discoveries/Fahrzeugsicherheit/?redirId=38066

Fallbeispiel 4:

Phoenix Contact berücksichtigt bereits während der Entwicklungsphase eines Produkts Sicherheitsanforderungen an Soft- und Hardware. Für Automatisierungslösungen wird ein Sicherheitskonzept mit den erforderlichen Schutzmaßnahmen erarbeitet. Beides erfolgt gemäß internationaler Normenreihe IEC 62443. Phoenix Contact hat zudem ein Team als Ansprechpartner für Anwender etabliert, die Sicherheitslücken entdecken, und aktiv über bekannt gewordene Sicherheitslücken informiert. Das Product Security Incident Response Team (PSIRT) hält sich bei der Bearbeitung, Bewertung und Veröffentlichung von Reports und Updates an die Prozesskette der Normenreihe.

Weitere Informationen: https://www.phoenixcontact.com/online/portal/pc/pxc/offcontext/insite_landing_page/!ut/p/z1/xZRRb4IwFIV_DY

Fallbeispiel 5:

Siemens hat in seiner „Charter of Trust" zehn Prinzipien für Cybersicherheit aufgestellt. Dazu gehört auch das Prinzip „Verantwortung in der digitalen Lieferkette übernehmen". Das bedeutet zum Beispiel: Security auch im Wertschöpfungsnetzwerk mit Lieferanten zu verankern. Um dieses zu gewährleisten, wurde ein Roll-out gestartet, das entsprechende Terms & Conditions in allen Einkaufsverträgen sowie die Qualifizierung von 300 Pilot-Zulieferern vorsieht. Siemens unterstützt Geschäftspartner und Lieferanten bei der Umsetzung der „Roadmap to Compliance" mit den notwendigen Sicherheitsstufen bis hin zu externer Zertifizierung.

Weitere Informationen: www.charter-of-trust.com

4 Aus Daten gewonnene Wertschöpfung als wirtschaftlich bedeutsames Gut der Unternehmen behandeln

Fallbeispiel 1:

Das ABB Ability™ Collaborative Operations Center (COC) bietet eine neue Kooperationsform an digitalen Dienstleistungen. ABB Experten setzen sichere cloudbasierte Applikationen ein, mit denen sie je nach Leistungsumfang 24/7, Anlagendaten sammeln, vernetzen, analysieren und proaktiven Auswertungen visualisieren. Kunden erhalten so schnell und effizient Entscheidungsvorlagen zur Verbesserung ihrer Anlagenverfügbarkeit, ihrem Produktionsdurchsatz oder ihrer Produktqualität und steigern damit ihre Kosteneffizienz und die Leistungsfähigkeit ihrer Betriebsprozesse. Hierbei werden Massendaten aus den Anlagen oder Flotten mit tiefgreifenden Branchenkenntnissen verknüpft. Ziel ist es, gemeinsam mit Kunden neue Wertschöpfungspotenziale zu schaffen.

Weitere Informationen: https://new.abb.com/news/detail/4357/abb-ability-collaborative-operations-center-unterstuetzt-die-industrielle-automatisierung

Fallbeispiel 2:

Ein Beispiel für aus Daten gewonnene Wertschöpfung ist die datenbasierte zustandsorientierte Instandhaltung, die eine Analyse der Zustandswerte eines Feldgeräts im zentralen Instandhaltungsmanagementsystem erlaubt.

Werden Betriebsdaten von einer Maschinenflotte gesammelt, so können durch Datenanalyse sinnvolle Wartungszeitpunkte ermittelt werden. Die zugrunde liegenden Auswertungsverfahren können schutzfähig sein. Hierzu hält Siemens Patente im Bereich „System und Verfahren zur zustandsorientierten Instandhaltung".

5 Portabilität und Interoperabilität von Daten für wettbewerbliche Nutzung unterstützen

Fallbeispiel 1:

ABB unterstützt die Entwicklung des Konzepts der Verwaltungsschale und übernimmt es in die eigene Geräte- und Plattformentwicklung. Die Verwaltungsschale erlaubt es, Daten und Dienste von IIoT-Geräten über eine einheitliche Schnittstelle zu verbinden, unabhängig vom Hersteller des Geräts. Zusätzlich können Geräteeigenschaften, standardisiert mittels eCl@ss, herstellerübergreifend ausgetauscht werden.

Weitere Informationen: https://www.youtube.com/watch?v=AXQ0yIonNxk&t=1s

Fallbeispiel 2:

Infineon hat 2018 ein sogenanntes Trusted Platform Module (TPM) speziell für Automobilanwendungen auf den Markt gebracht. Die externe Kommunikation eines Fahrzeugs wird geschützt, indem das TPM – eine Art Tresor – beispielsweise kryptografische Schlüssel generiert, speichert, verteilt und verwaltet. Das TPM entspricht internationalen Standards (ISO/IEC 11889) und trägt so maßgeblich zur Portabilität und Interoperabilität der Daten bei.

Weitere Informationen: https://www.infineon.com/cms/en/product/security-smart-card-solutions/optiga-embedded-security-solutions/optiga-tpm/sli-9670/

Fallbeispiel 3:

Siemens MindSphere bietet an jeder Schnittstelle offene, bidirektionale Kommunikation und Integrierbarkeit zu Applikationen, Maschinen sowie Enterprise-IT-Systemen und anderen IT-Plattformen. Kunden haben außerdem die Möglichkeit, die Datenmodelle nach eigenen Wünschen zu gestalten oder Daten aus dem Backend zu entfernen. Zudem bietet Siemens mit IDL (Integrated Data Lake) und EDI (Enterprise Data Interconnect) eine Methodik an, für die Analyse benötigte Daten aus anderen Data Lakes für Applikationen von MindSphere zu nutzen, ohne ihren Speicherort zu verändern.

Weitere Informationen: https://www.plm.automation.siemens.com/media/global/en/Siemens_MindSphere_Whitepaper_tcm27-9395.pdf

6 Nachhaltige Nutzung von Daten fördern

Fallbeispiel 1:

BLIDS, der Blitz-Informationsdienst von Siemens, ortet Gewitterblitze in Deutschland und weiteren europäischen Ländern.

Neben dem kostenpflichtigen Abo gibt es mit dem BLIDS-Spion einen Satz kostenloser Übersichtsgewitterkarten für Deutschland und andere europäische Länder. Auf Basis von über 155 in Europa verteilten Messstationen können Blitzeinschläge mit einer Genauigkeit von bis zu 200 Meter geortet werden. Siemens stellt via BLIDS-Spion alle 15 Minuten eine aktualisierte Karte zur Verfügung, auf der alle Blitzeinschläge der letzten zwei Stunden vermerkt sind.

Weitere Informationen: https://new.siemens.com/global/de/produkte/services/blids.html

7 Open Innovation und Co-Creation stärken

Fallbeispiel 1:

ABB unterstützt seine Kunden bei der Digitalisierung von Geschäftsprozessen. In Co-Creation-Workshops können Kunden ihre Vorstellungen gemeinsam mit den jeweiligen ABB-Geschäftsbereichen in digitale Lösungen umsetzen. Die Workshops werden je nach Branche, Thema und Aufgabenstellung für den Kunden angelegt. Der Kunde wird in den Innovationsprozess von Anfang an mittels Design Thinking eingebunden. Die neu entwickelten Lösungen und Geschäftsmodelle können so einfacher erprobt werden.

Weitere Informationen: https://new.abb.com/news/de/detail/38997/gemeinsam-im-ace-mehrwert-fuer-kunden-schaffen

Fallbeispiel 2:

Phoenix Contact hat einen offenen Webstore für Lösungen verschiedener Anbieter rund um die Steuerungsplattform PLCnext eingerichtet. Der PLCnext Store stellt Software-Applikationen bereit, mit denen Interessenten eine PLCnext-Steuerung funktional erweitern und diese dann zum Verkauf anbieten können. Mit dem PLCnext Store erhalten die Anwender die unterschiedlichen Apps – von Software-Bibliotheken für eine beschleunigte Programmierung bis hin zu ausprogrammierten Apps, deren Nutzung keine Programmierkenntnisse erfordert.

Weitere Informationen: https://www.plcnextstore.com/

8 Teilhabe an digitalen Plattformen ermöglichen

Fallbeispiel 1:

Die Bundesdruckerei bietet künftig Datentreuhänderdienste im Gesundheitsbereich (Pseudonymisierung, Berechtigungs- und Einwilligungsmanagement) als Service über eine digitale Plattform an. Mithilfe einer Vertrauensstelle können personenbezogene Daten und Pseudonyme sicher verwaltet werden. Den Nutzdaten werden ausschließlich Pseudonyme zugeordnet. Über ein Berechtigungsmanagement kann der Datengeber entscheiden, wer welche Daten zur Einsicht erhält bzw. diese Berechtigung widerrufen.

Weitere Informationen: https://www.bundesdruckerei.de/de/Themen-Trends/Magazin/Der-Datentreuhaender-als-neutrale-Schutzinstanz

Fallbeispiel 2:

Protiq bietet eine offene Plattform für 3D-Druck. Das digitale Geschäftsmodell des Herstellers von 3D-Druck aus Kunststoff, Keramik und Metall sieht vor, dass der Kunde online konfiguriert, bestellt und bezahlt. Protiq betreibt zudem ein offenes Portal, auf dem unterschiedliche Dienstleister ihren 3D-Druck-Service anbieten können. Der Besteller kann auf dem Marketplace frei wählen, welcher Anbieter seinen Auftrag fertigen soll.

Weitere Informationen: https://www.protiq.com/protiqmarketplace/

Fallbeispiel 3:

Drittanbietern wird durch einen nicht proprietären Zugang zur Siemens MindSphere-Plattform ermöglicht, eigene datenbasierte Geschäftsmodelle zu entwickeln. Hierzu können Drittanbieter offene Schnittstellen und flexible Konnektivitätslösungen für Maschinen (herstellerübergreifend und mit beliebigen Protokollen oder Kommunikationsstandards) sowie für diverse Software-Systeme (z. B. ERP, MES) nutzen:

Darüber hinaus wird Drittanbietern über den MindSphere Store eine sichere Vertriebsplattform für industrielle Anwendungen und digitale Dienste zur Verfügung gestellt.

Weitere Informationen: https://www.plm.automation.siemens.com/media/global/en/Siemens_MindSphere_Whitepaper_tcm27-9395.pdf

9 Transparenten Betrieb von digitalen Plattformen fördern

Fallbeispiel 1:

Das ABB Ability™ Data Manifesto dient als Ausgangspunkt für Diskussionen über neue digitale Lösungen und soll die Grundwerte für eine vertrauensvolle Zusammenarbeit im digitalen Bereich bilden. Es beschreibt in drei Punkten, dass Kundendaten nicht in Besitz von ABB übergehen, der Kunde stets weiß, was ABB mit den Daten macht, und die Daten nicht ohne explizites Einverständnis des Kunden weitergegeben werden, unabhängig davon, ob es sich um personenbezogene oder Maschinendaten handelt.

Weitere Informationen: https://www.forbes.com/sites/abb/2017/04/13/a-call-to-action-for-the-internet-of-things-industry-lets-write-a-data-bill-of-rights-for-cloud-customers/#379899109a21

Fallbeispiel 2:

Protiq bietet eine offene Plattform für 3D-Druck. Das digitale Geschäftsmodell des Herstellers von 3D-Druck aus Kunststoff, Keramik und Metall sieht vor, dass der Kunde online konfiguriert, bestellt und bezahlt. Protiq betreibt zudem ein offenes Portal, auf dem unterschiedliche Dienstleister ihren 3D-Druck-Service anbieten können. Der Besteller kann auf dem Marketplace frei wählen, welcher Anbieter seinen Auftrag fertigen soll.

Weitere Informationen: https://www.protiq.com/protiqmarketplace/

10 Fairen Wettbewerb zwischen digitalen Plattformen ermöglichen

Fallbeispiel 1:

ABB unterstützt die Entwicklung des Konzepts der Verwaltungsschale und übernimmt es in die eigene Geräte- und Plattformentwicklung. Die Verwaltungsschale erlaubt es, Daten und Dienste von IIoT-Geräten über eine einheitliche Schnittstelle zu verbinden, unabhängig vom Hersteller des Geräts. Zusätzlich können Geräteeigenschaften, standardisiert mittels eCl@ss, herstellerübergreifend ausgetauscht werden.

Weitere Informationen: https://www.youtube.com/watch?v=AXQ0yIonNxk&t=1s

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main
Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org