Die I4.0 Community cloud

Die Community Cloud als Basistechnologie für Industrie 4.0

JOSEF GLÖCKL-FROHNHOLZER

1 Das Internet der Dinge und Dienste hält Einzug in die Fabrik

Die vierte industrielle Revolution verspricht eine nachhaltige Veränderung der industriellen Produktion und damit der kompletten Wirtschaft. Dies geschieht durch die intelligente Vernetzung von Mensch, Maschinen und Objekten, die eine weitreichende Anpassung der Geschäftsprozesse nach sich zieht. Unternehmen und Produktionsbetriebe stehen hinsichtlich Industrie 4.0 vor neuen Herausforderungen, aber auch vor zahlreichen Chancen. Entscheidend für den Erfolg sind vor allem die zugrunde liegende unternehmenseigene IT-Infrastruktur und der Einsatz von neuen Technologien wie Cloud Computing. Mit dieser Entwicklung halten richtungsweisende Entwicklungen der ITK-Evolution Einzug in die Unternehmensstrukturen: das „Internet der Dinge“ und das „Internet der Dienste“. Beim Internet der Dienste geht es in erster Linie um den onlinebasierten Bezug von Services verschiedenster Entwicklungs- und Dienstplattformen. Das Internet der Dinge hingegen umfasst sämtliche webfähigen Produkte und Gegenstände. Beide Konzepte treiben eine allumfassende und intelligente Vernetzung voran. Dies gelingt mittels cyber-physischer Systeme (CPS). Sie bilden das Verbindungsstück zwischen IT-Infrastruktur und physikalischer Umgebung.

Die beiden Protagonisten der Umwälzung in der Industrielandschaft sind die **Smart Products** und die **Smart Factory**: Smart Products bezeichnen die Einheit aus physischem Produkt und der dazugehörenden digitalen Signatur. Sie enthält Informationen über den kompletten Herstellungsprozesses des Produkts sowie dessen künftigen Einsatz. Auf diese Weise unterstützen Smart Products den Fertigungsprozess aktiv. Die **Smart Factory** hingegen steuert als intelligente, hochvernetzte Fabrik die Produktion dynamisch und standortübergreifend. Den unterschiedlichen Anforderungen der **Smart Products** entsprechend passt sie die Produktionsprozesse flexibel an, um maximal effizient zu arbeiten.

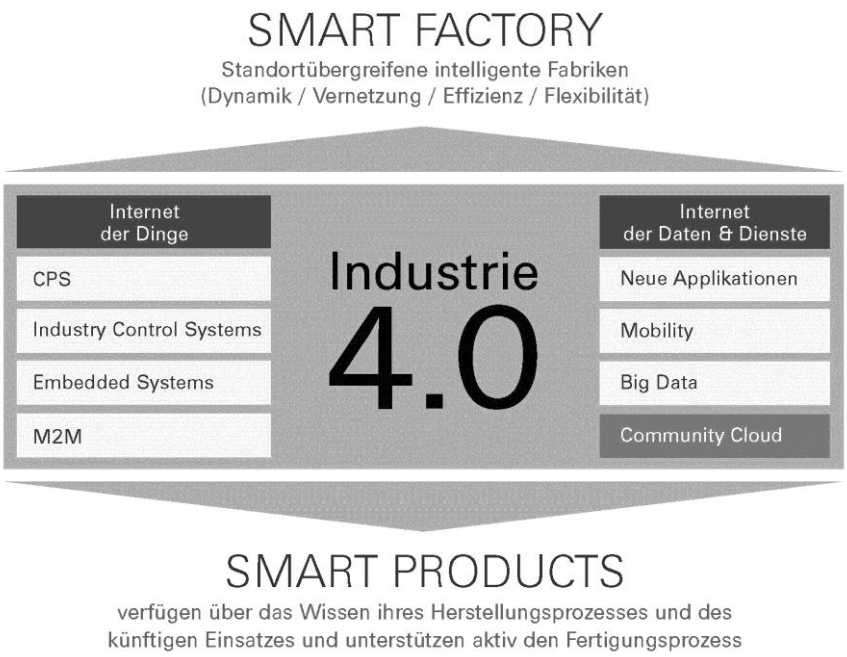

Abbildung 1: Industrie 4.0 bündelt bereits vorhandene Technologien und hebt sie auf ein neues produktives Niveau. Cloud Computing stellt als Basistechnologie unbegrenzte Netz- und Speicherkapazität zur Verfügung.

CPS-Plattformen haben die Funktion, die horizontale Integration verschiedener Technologien und Wertschöpfungsstufen über alle Wertschöpfungsnetzwerke hinweg zu meistern, und zwar in drei wesentlichen Dimensionen: in der digitalen Durchgängigkeit des Engineerings über die gesamte Wertschöpfungskette hinweg, der vertikalen Integration sowie der vernetzten Produktionssysteme.[1] Die Umsetzung von Industrie 4.0 ist nicht zwangsläufig eine unvermittelte Revolution, sondern basiert eher auf einem evolutionären Prozess. Ein Großteil der dafür notwendigen Technologien ist bereits in den Unternehmen vorhanden.

Bei den immer stärker vernetzten Unternehmen mit individuell gewachsener IT-Landschaft zeichnet sich schnell eine der größten Herausforderungen ab: Die Beherrschung des Datenflusses über alle Glieder der Wertschöpfungskette hinweg. Dafür gilt es, Datenaustausch, Datenverteilung, Datenqualität, Datensicherheit und das Datenwachstum übersichtlich abzubilden. In diesem Rahmen erhält die **Orchestrierung und das Management** der hybriden Ausprägung von Cloud Computing als Basistechnologie von Industrie 4.0 eine besondere Relevanz innerhalb des Evolutionsprozesses. Das **Cloud Management** hybrider, virtualisierter Infrastruktur (Storage, CPU, Memory, Netzwerke) formt die Basis für die Kontrolle der CPS-Plattform. Eine solche CPS-Orchestrierung muss sowohl die IT-Services über offene Schnittstellen einbinden als auch die hybriden Cloud Stacks über die Wertschöpfungsstufen managen.

[1] Vgl. Kagermann, Wahlster, Helbig: Umsetzungsempfehlungen, S. 6

Hybride Cloud-Lösungen integrieren die Ressourcen zweier klassischer Cloud-Modelle, der Public und der Private Cloud. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) definiert die Private Cloud als Infrastruktur, die ausschließlich für eine Organisation oder ein Unternehmen betrieben wird. Entweder organisiert und betreibt das Unternehmen selbst diese Ressourcen oder beauftragt damit einen Dritten. Die Private-Cloud-Infrastruktur kann dabei sowohl im eigenen wie auch in einem fremden Rechenzentrum stehen. In einer Public Cloud stellt ein Anbieter Services zur Verfügung, die für die Allgemeinheit meist über öffentliches Internet nutzbar sind. In der Regel hochstandardisiert, bieten diese Services für den Benutzer kaum Möglichkeiten der individuellen Anpassung. Trotz maximaler Flexibilität und Skalierbarkeit ist der Schwachpunkt der Public Cloud vor allem der Datenschutz.

Aufgrund der virtuellen, onlinebasierten Strukturen von Cloud Computing hat neben dem Management des Datenflusses vor allem die **Security** einen systemrelevanten Anteil am Erfolg von Industrie 4.0. IT-Sicherheit im Unternehmensumfeld umfasst zwei wichtige Aspekte: Zum einen die Sicherheit einzelner Prozesse und verschiedener Akteure. Dies ist besonders bei Smart Factories ein sehr komplexer Aspekt, da es sich bei den CPS-basierten Produktionssystemen um hochgradig vernetzte Systemstrukturen handelt. Sie umfassen eine Vielzahl von beteiligten Menschen, IT-Systemen, Automatisierungskomponenten und Maschinen. Zwischen den teilweise autonom agierenden Smart Products und der Smart Factory findet zusätzlich ein kontinuierlicher Daten- und Informationsaustausch mit hohen Anforderungen an Qualität und Verfügbarkeit statt.

Zum anderen ist die ganzheitliche Sicherheit der IT-Landschaft im Betrieb enorm wichtig. Aufgrund des hohen Vernetzungsgrads intern und gegebenenfalls mit Partnern nach außen müssen Unternehmen besonders vorsichtig sein. Hier bietet die Community-Cloud-Architektur den passenden Rahmen für den erhöhten Sicherheitsbedarf solcher vernetzten Wertschöpfungsketten. Eingeordnet in die verschiedenen Cloud-Modelle von Public, Private und Hybrid Cloud rangiert die Community Cloud zwischen dem privaten und dem öffentlichen Cloud-Modell: Mehrere Teilnehmer teilen sich bereitgestellte Ressourcen innerhalb eines strikt regulierten Nutzerkreises. Geschlossene Kommunikationsgruppen erlauben den Austausch von Nachrichten und Daten ausschließlich zwischen den berechtigten Partnern. Die Community Cloud verfügt dabei über einige zentrale Vorteile: Sie stellt einen Schutzraum dar, in dem sowohl mehrere Unternehmen als auch künftig Akteure der Industrie 4.0 (Produkte, Automatisierungssysteme, Programme, etc.) untereinander kritische Daten austauschen und sicher miteinander kommunizieren. Im Vergleich zu einer klassischen Public Cloud bietet die Community Cloud ein deutliches Mehr an Sicherheit. Sie bildet schon durch den beschränkten, klar definierten Nutzerkreis ein vertrauenswürdigeres Umfeld.

Der Weg in die vierte Generation der Industrierevolution wird nur mit **Standards** gelingen, die sich im Kontext der systemrelevanten Technologie Cloud Computing über eine inkrementelle Entwicklung in einer notwendigen Industrie-4.0-Referenzarchitektur etablieren. Der Standardisierungsprozess folgt dabei anderen Regeln als beispielsweise im Anlagen- und Maschinenbau oder der Elektrotechnik. Im Gegensatz zu den Ingenieursdisziplinen, wo Produkte nach den Vorgaben einer Norm entwickelt werden, entwickeln und verbreiten Gemeinschaften aus Unternehmen, Forschungseinrichtungen und Einzelpersonen Standards wie zum Beispiel das offene Betriebssystem Linux. Als Ergebnis dieses gemeinschaftlichen Entwicklungsprozesses entsteht anhand von Best Practise ein verbindlicher Standard. Für den Bereich Infrastructure as a Service (IaaS) im Cloud Computing zeigt die aktuelle Marktentwicklung beispielsweise, dass sich OpenStack als Architekturansatz zahlreicher Anwendungsfälle als De-facto-Standard festigt. OpenStack geht im Ursprung auf die Zusammenarbeit der NASA und dem Managed Service Provider Rackspace zurück. Seit 2012 hingegen entwickelt eine gemeinnützige OpenStack Community die Technologie weiter.

2 Einordung Community Cloud in das Industrie Referenzmodell I4.0

2.1 Industrie 4.0 Cloud Stack der Experton Group

Zur übersichtlichen Darstellung und Zuordnung der Cloud-Orchestrierung und der Security-Anforderungen wird im Folgenden auf den Industrie 4.0 Technology Stack der Experton Group AG referenziert. Es dient als Architektur-Blueprint für die Betriebsprozesse und Technologieplattformen von Industrie 4.0. Basierend auf dem Referenzmodell Open Systems Interconnection (OSI) besteht dieser aus sieben Schichten (Layer).

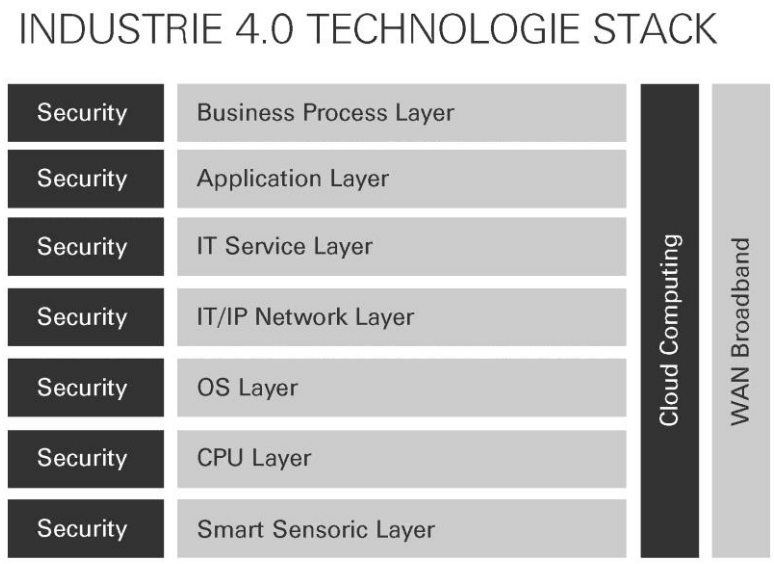

Abbildung 2: Der Architektur-Blueprint zu Industrie 4.0 stellt auf allen Schichten des OSI-Modells die Sicherheit in den Vordergrund. (Quelle: Experton Group AG)

Dabei entsprechen die ersten drei Layer (Smart Sensorik, CPU, OS) in erster Linie den Anforderungen der Automatisierungsprozesse im Maschinenbau oder der Produktion. Die restlichen vier Layer betreffen vor allem die IT im Unternehmen.

- Layer 1 – Smart Sensorik: Sensoren und Aktoren in unterschiedlichster Ausprägung (Hohe Rechenleistung und vernetzt)
- Layer 2 – CPU (zumeist Embedded Industrial Processors): spezialisiert und effizient
- Layer 3 – OS: zumeist embedded Linux, maschinenspezifisch Android, Openstack
- Layer 4 – IT/IP Network: Vernetzung auf IP Basis
- Layer 5 – IT/IP Services: IT-Services und Middelware / Datacenter Storage, Database, etc.
- Layer 6 – Application: ERP/PLT mit starken Industrie 4.0 Bezug
- Layer 7 – Business Processes: Industrie 4.0 relevante Geschäftsprozesse [2]

2.2 Cloud Orchestrierung als Teil der CPS-Plattform

Im Kontext Industrie 4.0 fällt den CPS-Plattformen eine zentrale Orchestrierungs-Rolle zu. Sie vernetzen die verschiedenen Akteure, Objekte und Anwendungen intelligent und hoch effizient aufgrund folgender Merkmale:

- Flexibilität durch schnelle und einfache Orchestrierung von Diensten und Anwendungen einschließlich CPS-basierter Software
- Einfache Verteilung und Inbetriebnahme (Deployment) der Geschäftsprozesse
- Vollständige, sichere und verlässliche Abdeckung des gesamten Geschäftsprozesses
- Sicherheit und Verlässlichkeit angefangen beim Sensor bis hin zur Benutzungsschnittstelle
- Unterstützung mobiler Endgeräte[3]

Um die Komplexität einer Cloud-Umgebung auf Infrastruktur-Ebene beherrschbar zu machen sowie diese während der Betriebsphase optimal zu steuern und auszulasten, bedarf es entsprechender Administrations- und Verwaltungswerkzeuge, der Cloud Management Software. Aufgrund der prozess- und technologieübergreifenden Aufgaben von Cloud Computing übernehmen diese Orchestrierungswerkzeuge eine zentrale Schlüsselposition – vor allem in der hybriden Umgebung einer Community Cloud.

[2] Vgl. Weiss, Zilch, Schmeiler: Experton Group MC-Studie, S. 20

[3] Vgl. Kagermann, Wahlster, Helbig: Umsetzungsempfehlungen, S. 28

2.3 Community Cloud – Secure Communication Platform als Nukleus für Industrie 4.0

Bei der Community Cloud schließen sich „Industrie 4.0“-Akteure mit ähnlichen Interessen zu einer Community zusammen. Eingeordnet in die verschiedenen Cloud-Modelle von Public, Private und Hybrid Cloud rangiert die Community-Cloud zwischen dem privaten und dem öffentlichen Cloud-Modell. Aufgrund der unter Umständen großen Teilnehmerzahl in der Industrie 4.0 Community Cloud betreibt eine für diese Aufgabe vertrauensvolle Instanz das Community-Cloud-Management. Zusätzlich bezieht sie entsprechend der Anforderungen der Community die Cloud-Infrastrukturen (IaaS) von verschiedenen Cloud Service Providern (CSP). Als steuernde bzw. neutrale Instanz fungiert entweder einer der teilnehmenden Cloud User oder ein professioneller CSP. Die gemeinsamen physischen Ressourcen für die Aufgabenerfüllung in Industrie 4.0 stehen als Shared Infrastructure ausschließlich dem beschränkten Nutzerkreis der Community zur Verfügung. Vor allem im Hinblick auf gemeinsame Teilprozesse oder Projekte unterschiedlicher Unternehmen bietet die Community Cloud enorme Vorteile für die Zusammenarbeit.

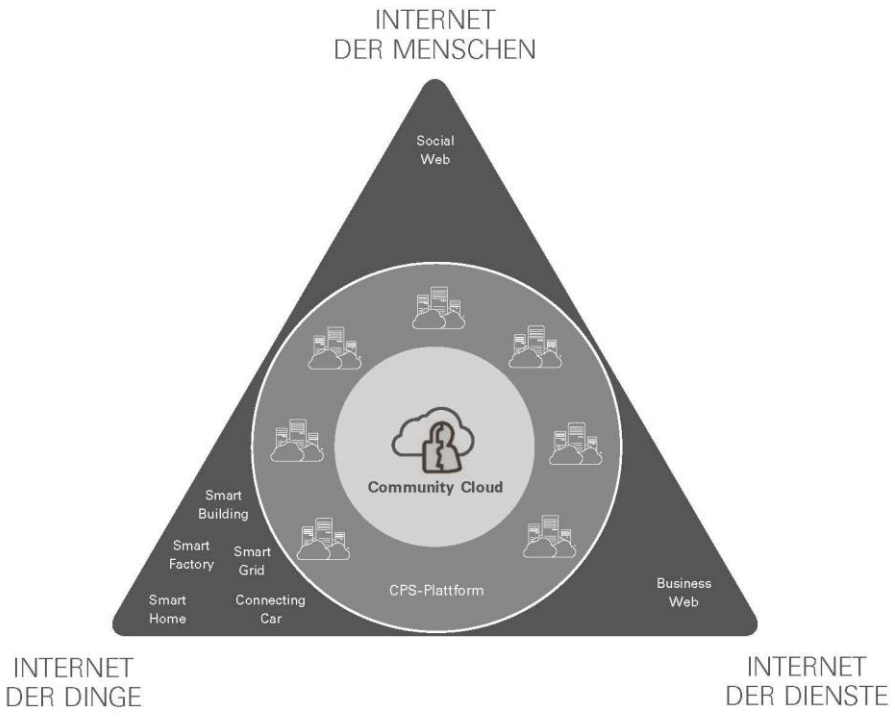

Abbildung 3: Die Community Cloud bildet gemeinsam mit der CPS-Plattform ein zentrales Bindeglied im Zusammenspiel der Akteure von Industrie 4.0.

Besonders branchenspezifische Sicherheitsstandards sind in der Community Cloud leichter umzusetzen. Verschiedene Parameter wie Quality of Service (QoS), Policies, Data Segregation, Business Continuity,

Intrusion Prevention oder Compliance-Anforderungen definiert und setzt die Gemeinschaft individuell nach ihren eigenen Ansprüchen um. So ist sie in der Lage, rechtlichen Rahmenbedingungen einfacher zu entsprechen. Gleichzeitig ist das Einhalten dieser Voraussetzungen im Vergleich zu einer Public Cloud eines Providers viel einfacher zu überprüfen. Mehr Transparenz über diese Rahmenbedingungen gibt es normalerweise nur in der abgeschotteten Privaten Cloud. Daher ist die Bereitschaft, auch sensiblere Daten in die Community Cloud zu legen, deutlich größer, denn hier ziehen alle an einem Strang.

3 I 4.0 Community Cloud

Hybrid-Cloud Management

Die Cloud Management Software ist ein integraler Bestandteil der Community-Cloud. Als Teil der CPS-Plattform spielt sie eine wichtige Rolle auf dem Weg zur Massenadaption von Industrie 4.0. Sie gewährleistet zentrale Aspekte wie Interoperabilität, Datenschutz und das Einhalten der Compliance-Anforderungen. Einerseits managt sie die Komplexität der Datenmigration von privater zur externen Cloud, andererseits unterstützt sie effizient und vollständig automatisiert die Governance des Unternehmens mit den entsprechenden Policies. Multi-Cloud-Management-Systeme übernehmen eine zentrale Schnittstellenfunktion zwischen Hardware-, Middleware- und Softwarekomponenten und bilden einen wesentlichen Teil der Intelligenz einer Cloud-Umgebung. Nur mit ihnen lassen sich die verschiedenen Hard- und Softwarekomponenten effizient, sicher und benutzerfreundlich implementieren. Die Anforderungen an Multi-Cloud-Management-Systeme sind im Kontext von Industrie 4.0 entsprechend hoch. Sie müssen im Wesentlichen vier Eigenschaften aufweisen:

- Agilität: Automatisierte IT-Services (Anwendungen, Infrastruktur, Desktops und alle benutzerdefinierten Dienste), um so schnell auf Geschäftsanforderungen zu reagieren
- Steuerung: Personalisierte, geschäftsrelevante Sicherheitspolicies (Governance) sowie Durchsetzung der Anwendungsbereitstellung (Normen, Ressourcen, Quoten und Service-Levels)
- Auswahl: Investitionsschutz in aktuelle und künftige Technologien durch breite Multi-Vendor- bzw. Multi-Cloud-Unterstützung und skalierbares Design
- Effizienz und Verbesserung von IT-Services durch Kostensenkung

Um die genannten Eigenschaften zu erreichen, benötigen Multi-Cloud-Management-Systeme bedarfsgerechte und effiziente Orchestrierungsfunktionalitäten. Die Anforderungen für eine I4.0 Community Cloud lassen sich in zwei Dimensionen teilen:

Cloud-Orchestrierungs-Funktionalität:

- Automatisierte Provisionierung von Computer, Storage, Memory und Netzwerk-Ressourcen
- Unterstützung multipler Virtualisierungstechnologien und Cloud Stacks
- Multi-mandantenfähige Architektur (Multi-Tenancy)
- Virtual-to-Virtual Conversion (Umzug von Virtual Images auf andere Hypervisoren)
- Standortübergreifendes Rechenzentrums- bzw. Infrastrukturmanagement
- Anpassung und Verwaltung verschiedener SLAs/SLA-Klassen
- Core-Module wie Pricing und Billing, Engine und Reporting in Echtzeit sowie Dashboard-Funktionalitäten
- Hybrid-Cloud-Ansatz mit Verbindung an IaaS-Marktplätze

Security-Orchestrierungs-Funktionalität:

- Rollenbasiertes Benutzerkonzept und Sicherheitsfeatures wie beispielsweise ein Schlüsselverwaltungsmanagement auf Industrie 4.0 Niveau (Ende-zu-Ende-Sicherheitskonzept)
- Identity Management
- Workflow-Engine und Policy Management zur Einhaltung von Governance und rechtlichen Rahmenbedingungen
- Sichere Speicherverwertung durch automatische Zerstörung von Datenrückständen
- Interner Richtliniensupport und vereinfachte Einhaltung von Vorschriften
- Kontrolle über zeitlichen und örtlichen Datenzugriff

Nachfolgendes Schaubild zeigt, bezogen auf den „Industrie 4.0“-Stack der Experton Group AG, die Zuordnung der Orchestrierungs-Funktionalität für eine I4.0 Community Cloud. Eine aktuelle Form dieses Cloud-Modells ist beispielsweise der offene Architekturansatz ECO-Plattform (Elastic Cloud Orchestration) des Softwareherstellers Zimory. Diese Orchestrierungstechnologie basiert auf einer hochflexiblen und adaptierbaren Softwarearchitektur.

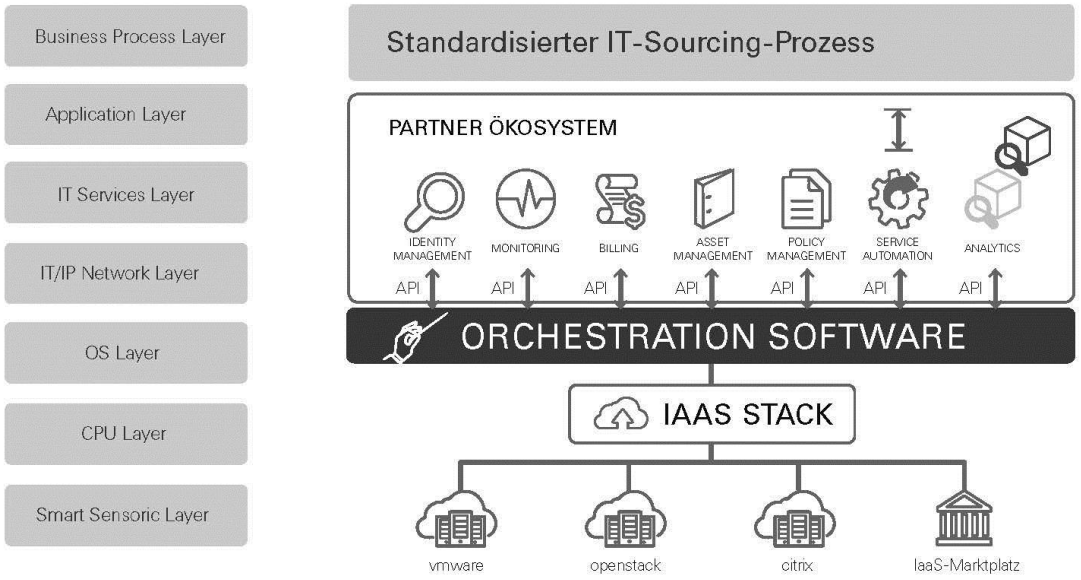

Abbildung 4: Eine zukunftsweisende Orchestrierungsplattform bildet alle Schichten des OSI-Modells ab, hier am Beispiel der ECO-Plattform des Softwareherstellers Zimory.

Die Orchestrierungssoftware bildet den grundlegenden Kommunikationsanker einer Multi-Cloud-Plattform. Sie ist entsprechend dem „Industrie4.0"-Stack-Modell zwischen dem IT/IP-Network-Layer und dem OS-Layer angesiedelt. Als Vermittlungsschicht harmonisiert und öffnet sie die heutige heterogene Landschaft des Cloud Technology Stacks – unabhängig vom genutzten IaaS Stack. In ihrer Grundfunktionalität verbindet und verwaltet eine Orchestrierungs-Software unterschiedliche Cloud-Infrastrukturen. Dafür überwindet sie die Heterogenität der Infrastrukturen und vereint diese mit einer einzigen Management-Ebene sinnvoll zu einem Cloud Service – unabhängig davon, wo sich die einzelnen Cloud-Bestandteile geografisch und technisch befinden. Orchestrierungswerkzeuge ermöglichen im Kontext mit Industrie 4.0 die Kommunikation zwischen mehreren unterschiedlichen Modulen, die jeweils auf betriebswirtschaftliche und technische Anwendungsfälle ausgerichtet sind. Dafür führt sie Funktionalitäten durch die Konfiguration verschiedener Module zusammen, registriert diese und etabliert ihren Geltungsbereich innerhalb der gesamten Architektur.

3.2 Informationssicherheit als Erfolgsfaktor für Industrie 4.0

Informationssicherheit durch die I4.0 Community Cloud

Die Sicherheit spielt eine entscheidende Rolle für den Erfolg von Industrie 4.0. Nur wenn die Sicherheit sensibler Daten wirklich gewährleistet ist, wagen Unternehmen den Schritt zur Cloud und Industrie 4.0.

Aufgrund der zentralen Rolle der Community Cloud in Industrie 4.0 müssen die Risikopotenziale für die Nutzung der Cloud-Infrastrukturen sowohl für die Datenverteilung, Datenspeicherung und die Datenverarbeitung als auch für alle weiteren Anforderungen der Informationssicherheit abgewogen werden. Für jeden Layer ist zu prüfen, welche schützenswerten Informationen und Prozesse vorliegen und wo potenzielle Bedrohungen vorhanden sind. Im Kern geht es dabei, im Hinblick auf einen kontinuierlichen Cloud-Einsatz in Industrie 4.0, um die sogenannten Grundwerte der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit der Informationen. Um diese zu erreichen, müssen innerhalb der Communitiy Cloud Technologien und Verfahren zum Identitätsmanagement, Schutz und Integrität der Daten sowie Data Governance etabliert sein, einschließlich einer Richtlinienverwaltung von Government-Regelungen und geographisch verteilter Daten.

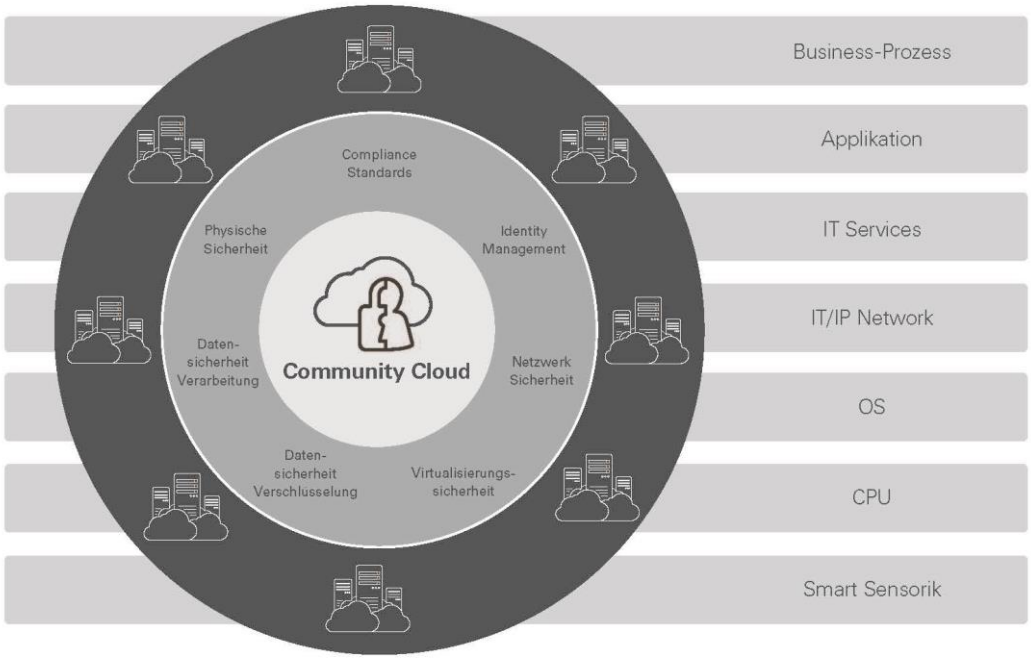

Abbildung 5: In der Industrie 4.0 Community Cloud müssen wesentliche Sicherheitsbausteine etabliert sein, getragen von einem ganzheitlichen Sicherheitskonzept.

Daraus resultiert die Notwendigkeit, speziell bei Industrie 4.0 für den geschützten Datenaustausch mehrere Security-Frameworks zu implementieren. Die Community Cloud bringt bereits einige dieser Security-Frameworks mit. So erlauben beispielsweise geschlossene Kommunikationsgruppen den Austausch von Daten ausschließlich zwischen berechtigen Partnern. Die Community ist ein geschützter Raum, in dem die Teilnehmer an der Wertschöpfungskette entlang untereinander sicher kommunizieren. Die Community Cloud bietet sich für den entsprechenden Einsatz in Industrie 4.0 an, da bereits durch bestehende Lösungen für die physische Sicherheit, Netzwerksicherheit (Ende-zu-Ende-Verschlüsselung), Virtualisierungssicherheit,

Datensicherheit und Authentifizierung sowie das Identitätsmanagement existieren. Diese gilt es nur noch an die jeweiligen Erfordernisse anzupassen.

3.2.2 Governance und Compliances in der I 4.0 Community Cloud

Die erhöhte Sicherheit der Community Cloud ist durch den beschränkten Nutzerkreis begründet, vor allem wenn dieser über klar definierte Eintrittsbarrieren wie Audits oder Zertifizierungen verfügt. Diese Barrieren stellen gleichzeitig das Einhalten von Mindeststandards sicher, auf die sich die Teilnehmer der Community Cloud im Vorfeld geeinigt haben. Das kann beispielsweise die ISO 27001 für Informationssicherheit sein oder die Sicherheitsempfehlungen für Cloud-Computing-Anbieter des BSI (Bundesamt für Sicherheit in der Informationstechnik). Ein weiteres Beispiel wäre der verbindliche Einsatz von FIPS 140-2 (Federal Information Processing Standard) zertifizierten kryptografischen Modulen, die beispielsweise für die Zusammenarbeit mit US-amerikanischen und kanadischen Behörden Pflicht sind. Je einheitlicher und höher die Standards, desto größer auch das Vertrauen in die Sicherheit der Community Cloud – besonders wenn unabhängige Dritte die Standards beispielsweise durch Zertifizierungen bestätigen.

3.2.3. Physische Sicherheit durch die Industrie 4.0 Community Cloud

Die Industrie 4.0 (I 4.0) Community Cloud baut für die Unternehmen einen Schutzraum auf, in dem diese Unternehmen untereinander kritische Daten austauschen und miteinander kommunizieren. Sie bildet für die Teilnehmer schon infolge des transparenten und durch Zugangsvoraussetzungen geprüften Nutzerkreises ein Trustworthy-Umfeld. In der I 4.0 Community Cloud ist klar geregelt, wer die Infrastruktur für die Wolke bereitstellt, wo diese physisch steht und wo die abgespeicherten Daten liegen. Für den physischen Schutz der Daten empfiehlt sich eine Splittung auf unterschiedliche Rechner und Lokationen verteilt. Auf diese Weise ist sichergestellt, dass selbst bei Diebstahl der Hardware die Cloud-Daten nicht vollständig in unbefugte Hände gelangen. Greift die Community beim Bezug der Cloud-Infrastruktur auf eine Marktplatzlösung zurück, so hat sie die Möglichkeit, über die „Governing Regions“ als Produktmerkmal transparent die Lokation der Datenspeicherung und -verarbeitung zu bestimmen. Die Governing Regions legen den Rechtsrahmen fest, der vor allem in Hinblick auf die Informationssicherheit von Kundendaten elementar ist. Darüber hinaus unterstützen Cloud-Marktplätze im Idealfall für alle beteiligten Unternehmen die Einhaltung der Rechtskonformität der Provider durch Definition und Überwachung von Zulassungserfordernissen.

3.2.4 Netzwerksicherheit

Bei der I 4.0 Community Cloud regeln eigene Netzanbindungen der Teilnehmer den Netzwerkzugang. Das funktioniert meist über per IPSec verschlüsselte Virtuelle Private Netzwerke (VPN) oder Multiprotocol Label Switching (MPLS). Das Internet explizit nicht einzubeziehen, bedeutet eine potenzielle Gefahrenquelle auszuklammern, die als Einfallstor für Malware und Attacken dient. Die direkte VPN-Anbindung weist geringere Latenzzeiten und garantierte Verfügbarkeiten auf – und damit eine bessere Performance, welche entsprechende Service Level Agreements (SLAs) gewährleisten. Die Verschlüsselung – in der Regel über IPSec oder TLS mit 2048 Bit Schlüssellänge – ermöglicht zusätzlich den Datenzugriff ausschließlich für berechtige Teilnehmer. Certificate Authorities (CA) geben die entsprechenden SSL/TLS-Zertifikate aus und kontrollieren ihre Gültigkeit. Je länger die Schlüssel und je sicherer die Algorithmen sind, desto stärker und effektiver ist die Verschlüsselung. Einziger Nachteil: Starke Verschlüsselungen stellen hohe Anforderungen an die Systeme und verlangsamen sie während der Verarbeitung verschlüsselter Daten. Daher benötigen sie vor allem im Echtzeit-Gebrauch ausreichend verfügbare Ressourcen.

Virtualisierungssicherheit

Die Virtualisierungssicherheit umfasst eine agentenlose Serversicherheitsplattform zum Schutz dynamischer Rechenzentren mit physischen, virtuellen und cloudbasierten Servern. Diese Plattform setzt Sicherheitsrichtlinien transparent für Virtuellen Maschinen (VM) durch. Diese virtuelle Appliance bietet **agentenlose Integritätsüberwachung, Malware-Schutz, IDS/IPS, Schutz** von **Webanwendungen, Anwendungssteuerung** und **Firewall-Schutz**. Darüber hinaus koordiniert sie den Schutz mit agentenlosen und agentenbasierten Formfaktoren und bietet so anpassbare Sicherheit für virtuelle Server sogar während des Verschiebens zwischen Rechenzentrum und öffentlicher Cloud. Weiterhin ermöglicht die Virtualisierungssicherheits-Plattform den Administratoren das Erstellen von Sicherheitsprofilen auf den Servern. Darüber hinaus übernimmt sie die zentrale Überwachung von Alarmen und vorbeugenden Maßnahmen, gegen vorliegende Bedrohungen. Eine Kernfunktionalität ist hierbei das automatisierte und fortlaufende Einspielen von Sicherheitsupdates.

Datenspeicherung / Datensicherheit durch Verschlüsselung

In Zukunft wird der Vernetzungsgrad der IT-Systeme noch zunehmen. Eine Grundvoraussetzung für ihre Nutzung ist daher eine effektive und sichere Verschlüsselung. Von ihr hängen das eindeutige Authentifizieren von Nutzern, die Datenspeicherung und jede gesicherte Kommunikation ab. Je besser die Verschlüsselung, desto sicherer die Daten: Strong Encryption von Ende-zu-Ende und auf allen Ebenen für Data-in-Motion, Data-at-Rest, das Netzwerk und das festgelegte Community Cloud Datacenter. Die Sicherheits-Architektur muss dafür ein entsprechendes Ende-zu-Ende-Sicherheitskonzept beherrschen. Nur so bietet sie einen

ausreichenden Schutz für Daten in virtuellen und Cloud-Umgebungen. Eine Möglichkeit der Verschlüsselung auf Block-Ebene sind systemweite, separat gespeicherte Schlüssel. Eine weitere, sichere Variante ist das Erzeugen nutzerindividueller Schlüssel, die das System nach dem Abmelden automatisch zerstört. Ein starkes Blockchiffre wie AES256 (Advanced Encryption Standard) mit einer Schlüssellänge von 256 Bit gewährleistet bei dieser Variante eine hohe Sicherheit. Selbstverständlich sollte der Cloud-Betreiber keinen Zugriff auf die Schlüssel der Clients beziehungsweise der Cloud-Nutzer haben.

Datenverarbeitung

Die Prozessoren der gemieteten Maschinen verarbeiten den Programmcode nur im Klartext, was dazu führt, dass eine aktive Programmausführung auf virtuellen Maschinen eine unverschlüsselte Ablage der Programme und der zu verarbeitenden Daten auf den externen Ressourcen verursacht. Daher muss neben der Speicherung auch die aktive Programmausführung verschlüsselt erfolgen, um eine ganzheitliche Informationssicherheit in der Industrie 4.0 zu erreichen. Der kryptografische Schutz eines aktiven Programms ist technisch sehr aufwendig und schwierig. „Der Prozessor muss unter Einhaltung der Vertraulichkeit ein verschlüsseltes Programm auf verschlüsselten Daten auszuführen, ohne beides auch nur partiell zu entschlüsseln.“[4] Für dieses Problem gibt es bereits erste Lösungen, dennoch stellt diese Aufgabenstellung im Bereich der Kryptologie im Zuge der Industrie 4.0 Entwicklungen nach wie vor eine zu überwindende Herausforderung dar.

Identity Management

Datensicherheit funktioniert nur in Kombination mit Identitätssicherheit. Die Smart Products besitzen in der Zukunft eine entsprechende digitale Identität. Somit sind jeweilige Berechtigungen und Rollen von Smart Products und Smart Factories an diese digitalen Identitäten gebunden. Daraus resultieren für die beiden Protagonisten von Industrie 4.0 die gleichen Regeln, wie für die heutige IT: Sichere Daten sind nur möglich, wenn Zutritte, Zugänge, Zugriffe und Weitergaben klar definierten Regeln und Kontrollen unterliegen. Zur Kontrolle der Cloud-Nutzer in Industrie 4.0 bietet sich beispielsweise eine eigene Certificate Authority (CA) an. Die CA erstellt, verwaltet und prüft die von ihr an die einzelnen User oder Geräte ausgegebene Zertifikate. Darüber hinaus legt sie sogenannte Certificate Revocation Lists (CRL) für gesperrte Nutzer an. Die Kontrolle über die CA sollte in jedem Fall beim CA-Betreiber liegen, der gleichzeitig die von der Gemeinschaft der Community Cloud festgelegten Zugangsvoraussetzungen prüft. Nur wer die definierten Sicherheitsstandards erfüllt, erhält von ihm ein gültiges Zertifikat für den Cloud-Zugang. Zu den grundlegenden Mechanismen des Identity Managements einer I 4.0 Community gehören:

[4] Smith, Brenner: Vertrauliche Datenverarbeitung, S. 27

Identitätsmanagement:

- Bereitstellen und Löschen von Accounts
- Workflow-Automation
- Administrationsfunktionen
- Passwortsynchronisation
- Selbständiges Zurücksetzen von Passwörtern
- Zugangskontrolle

Passwortmanagement:

- Einzelanmeldung
- Web-Einzelanmeldung
- Rollenbasierte Zugangskontrolle
- Attributbasierte Zugangskontrolle

4 Einheitliche Standards

4.1 OS-Layer: Openstack

Die jeweiligen Nutzer einer Community Cloud bringen in der Regel unterschiedliche Voraussetzungen ihrer eigenen IT-Infrastruktur mit und verwenden unter Umständen zusätzlich eigene Private Clouds. Werkzeuge zur Cloud Orchestration helfen beim Harmonisieren heterogener IT-Landschaften. Gleichzeitig unterscheiden sie zwischen den Private- und Community-Cloud Ressourcen und bieten den einzelnen Usern einen getrennten Überblick über die genutzten Kapazitäten. Hier sind Standards wichtig, denn ohne diese sind Kompatibilität und Übertragbarkeit virtueller Maschinen und Datenformate in keiner Weise gegeben. Gleiches gilt für das Management der Cloud-Ressourcen genauso wie für Datensicherheit und Datenschutz oder für einheitliche SLAs. In diesem Kontext spielen vor allem zwei Standards eine wesentliche Rolle, Openstack und CIMI. Hersteller, die auf offene Strukturen und offene API setzen, bauen ihre Lösungen auf beiden Standards auf. CIMI bezieht sich in erster Linie auf IaaS, ist aber auch für PaaS oder SaaS nutzbar.

4.2 IT-Sourcing: IaaS-Marktplätze

Ein herstellerunabhängiger IaaS-Marktplatz wie die Deutsche Börse Cloud Exchange schafft die Möglichkeit zur Beseitigung von Marktbarrieren. Transparente Marktplätze für Cloud-Infrastruktur werden daher in Zukunft

eine wichtigen Beitrag zur Erhöhung der Sicherheit für die Industrie 4.0 leisten, da die Kommunikation zwischen Smart Products und Smart Factories über die Wertschöpfungsstufen hinweg erfolgt. Auf solchen Handelsplätzen werden sowohl Anbieter als auch Konsumenten von den strategischen Vorteilen und den standardisierten Rahmenbedingungen profitieren. Standardisierte Cloud-Kapazitäten werden transparent, flexibel und bedarfsgerecht angeboten. Als Kontrollinstanz überwacht der Marktplatz die Einhaltung von Compliance- und Governance-Richtlinien der Provider und bietet Cloud-Nutzern so größere Sicherheit beim Bezug von Cloud-Infrastrukturen.

5 Fazit

Industrie 4.0 benötigt innovative Lösungen, um den gestiegenen Anforderungen an Sicherheit und Datenmanagement zu begegnen. Cloud Computing bildet für diese Herausforderungen die Basistechnologie. Nach wie vor ist beim Cloud Computing die Informationssicherheit ein kritischer Punkt. Die I4.0 Community Cloud bietet hingegen eine ganzheitliche Cloud-Sicherheitsarchitektur und bildet den Kern des cyber-physischen Systems. Dabei übernimmt eine vorausschauende Orchestrierung einen großen Teil der Intelligenz für die CPS-Plattform. Insgesamt gesehen, bergen Community Clouds das Potenzial, innerhalb von Industrie 4.0 für eine Partnerlandschaft verschiedene Prozess- und Sicherheitsstandards zu etablieren und diese langfristig – auch über nationale Grenzen hinweg – durchzusetzen. Dazu muss die Sicherheitsarchitektur auf jedem Layer den jeweiligen Herausforderungen entsprechen. Nur auf diese Weise wird es gelingen, sichere Prozesse auf allen Ebenen der Wertschöpfungsketten zu langfristig realisieren und schützenswerte Daten und Assets abzusichern.

6 Literaturverzeichnis

Glöckl-Frohnholzer, Josef (2013). Mehr Überblick im globalen Durcheinander. Funkschau 09.13. Haar: Weka Fachmedien GmbH.

Glöckl-Frohnholzer, Josef (2014). Die Zukunft der Cloud ist hybrid. Lanline 07.14. Kaufering: ITP Verlag.

Glöckl-Frohnholzer, Josef (2014). Secure Collaboration in der Community Cloud. iX 09.14. Hannover: Heise Zeitschriften Verlag.

Informationstechnik, B. f. (2014). Sichere Nutzung von Cloud-Diensten. Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Kagermann, H. K., Wahlster, W., Helbig, J. (2013). Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Frankfurt: acatech – Deutsche Akademie der Technikwissenschaften e.V.

Smith, M., Brenner, M. (2012). Vertrauliche Datenverarbeitung in der Cloud. In: Web Science: Die Zukunft des Internets. Unimagazin. Hannover: Leibniz Universität Hannover.

Velten, C., S. J. (2013). Cloud Vendor Benchmark 2013. München, Deutschland: Experton Group AG.

Weiss, M., Zilch, A., Schmeiler, F. (2014). Experton Group MC-Studie „Industrie 4.0. München, Deutschland: Experton Group AG.