Bild: iStock

Digitale Transformation

Hype, Chance und Bedrohung?

Peter Kiess

Grundsätzlich bezeichnet eine Transformation einen permanenten Prozess der Veränderung und somit eine stetige Fortentwicklung, sie ist also unser ständiger Wegbegleiter. Bislang verliefen Transformationen eher langsam, manchmal fast unmerklich, und hatten mal weniger, mal mehr Einfluss auf gesellschaftliche, wirtschaftliche und technologische Entwicklungen. Doch die digitale Transformation beschleunigt Veränderungen in einer bisher unvorstellbaren Geschwindigkeit. Was bedeutet diese Entwicklung für den Bereich der physikalischen Sicherheit?

Transformation findet in allen Lebensbereichen statt, auf persönlicher, gesellschaftlicher und politischer Ebene, in wirtschaftlichen Bereichen oder auch im technologischen Umfeld. Grundsätzlich ist sie also „das Normalste“ der Welt mit unterschiedlicher Auswirkung und Bedeutung – wie die Elektrifizierung, das Automobil oder beispielsweise der Wandel von mechanischen zu elektronischen Schließkomponenten. Ob man diese Veränderung nun etwa einem Kondratjew-Zyklus, einer Theorie zur zyklischen Wirtschaftsentwicklung, zuschreibt oder nicht – die digitale Transformation ist real und sie ist wuchtig. Mit allem, was wir bisher erleben und was sich aktuell abzeichnet, wird

es uns schneller, entscheidender, radikaler und nachhaltiger verändern als viele andere der bekannten Veränderungsprozesse. Wer am Ende zu den Gewinnern zählen wird, ist noch lange nicht entschieden. Alle globalen Big Player, Universitäten und tausende von agilen Startups aus allen Branchen investieren Rekordsummen und stellen sich diesem Wettbewerb: die Ideenlosen, Langsamen, Unentschlossenen und Abwartenden werden auf alle Fälle nicht dazu gehören.

Wenn wir retrospektiv die Veränderungen der vergangen sechs bis zehn Jahre in Bezug auf das digitale Zeitalter betrachten, zum Beispiel Online-Einkäufe, soziale Netzwerke oder autonomes Fahren und Car Sharing, wird klar, wie erdrutschartig und unumkehrbar diese das Verhalten und die Geschäftsmodelle verändert haben. Betrachten wir die neueren Technologien und die damit einhergehenden Möglichkeiten, wie beispielsweise Cognitive Computing, Predictive Analytics, Robotik und Sensorik, die Verschmelzung von Mensch und Maschine und mehr, die im Moment weltweit ihren Siegeszug beginnen. Wenn wir uns darüber hinaus des exponentiellen Wachstumspotentials von Technologien bewusst werden, können wir zumindest erahnen, mit welcher Geschwindigkeit, Kraft und Wirkung diese Transformationen große Bereiche unseres Lebens verändern werden.

Kennzeichen der digitalen Transformation

Technologie hat die herausragende Stellung im gesamten Transformationsmodell, denn üblicherweise stellt sie als „Enabler“ die Basis für alles Nachfolgende. Innerhalb dieses Bereiches stellen die softwarebasierten Komponenten die entscheidenden Mechanismen bereit. Der Investor Marc Adreessen prägte den Satz: „Software is eating the world“ – und hat damit die oben genannte Bedeutung treffend beschrieben.

Es handelt sich bei diesen Softwareentwicklungen im Wesentlichen keineswegs um Neuerfindungen – diese Technologien sind seit vielen Jahrzenten im Einsatz. Neu hierbei ist eher, dass sie eben noch leistungsfähiger, noch intelligenter und noch flexibler sind. Darüber hinaus sind sie grenzenlos verfügbar, kombinierbar und mit selbstlernenden Eigenschaften ausgestattet. Damit lassen sich „as a Service“ Anwendungs- und Geschäftsmodelle sehr einfach, nutzenstiftend, hochskalierbar und kostengünstig komponieren. Wer nutzt sie nicht, die Google-Suche, die Dropbox, die Sozialen Netzwerke, Amazon und die Navigationssysteme. Dies ist kein Selbstzweck: die Anbieter prognostizieren ihrerseits mit ausgesprochen cleveren Algorithmen und dem unerschöpflichen Wissen aus ihren Big-Data-Silos, welcher Inhalt zu welchem Zeitpunkt bei welchem Benutzer zu einem Kaufabschluss führt. Dem Anwender ist dies häufig nicht bewusst.

Seitens der Hardware haben sich ebenfalls atemberaubende Entwicklungen ergeben: Sensorik, Werkstoffe, Geräte und Komponenten sind mittlerweile mit eigenständiger (Entscheidungs-) Intelligenz ausgestattet. Software und Hardware verschmelzen beinahe nahtlos im sogenannten Internet of Things (IoT). Auch das ist keine Zukunftsmusik, sondern Realität: der Kühlschrank meldet sich, wenn die Milch alle ist, und die Bohrmaschine kann Informationen über Abnutzung oder potentielle Störungen auf das private Smartphone (oder den Sales Channel) legen. Wir setzen mittlerweile Lautsprecher ein, die mit uns kommunizieren, wie etwa Alexa von Amazon, die Einkäufe tätigen, uns beraten und vieles mehr. Das mögen viele noch als Spielwiese für Technikverliebte halten, die Anbieter solcher Produkte und Services werden uns jedoch schon bald eines Besseren belehren.

Für die Verschmelzung von IoT-Komponenten benötigt es permanent verfügbare Plattformen – hier tobt der Wettbewerb besonders stark. Spätestens seit der Entwicklung des iPhones, mit dem Apple weit mehr als 90 Prozent aller Gewinne im Smartphone-Bereich abschöpft ist klar: wer die Plattform hat, besitzt den Schlüssel zum Geldverdienen.

So ist es nicht wirklich verwunderlich, dass beispielsweise die deutsche Robert Bosch GmbH mit einer klaren Strategie und entsprechender Anstrengung versucht

und auf dem besten Wege ist, eine besonders starke Position im Bereich der führenden IoT Plattform Anbieter weltweit einzunehmen.

Mit den Möglichkeiten neuer Soft- und Hardwaretechnologien gehen natürlich völlig neue Geschäftsmodelle einher. Diese funktionieren weltweit, branchenübergreifend, stark vernetzt und auch mit stark wachsenden Branchenneulingen, beispielsweise Tesla und Airbnb. Die klassischen Marktbarrieren geraten in den Hintergrund – grundsätzlich haben die neuen Modelle eine massiv disruptive Wirkung. Sie können blitzschnell von Kunden produktiv genutzt werden und erfordern oftmals keine eigene IT-Installationen.

Mögliche Auswirkungen auf den Bereich „Physikalische Sicherheit"

#1: Mehr Intelligenz und Autonomie der Komponenten

Analog der bisherigen Entwicklungen im IoT-Bereich werden die eingesetzten Komponenten (Türen, Sensoren und Aktoren) hochgradig intelligenter und entscheiden selbstständig. Die Tür ist eine gesamte Einheit, mit IP-Adresse und direkter Verbindung zu steuernden Entscheidungssystemen. Beliebige Komponenten und Funktionen können je nach Anforderung eigenständig und dynamisch aktiviert und deaktiviert werden. Funktionsprüfungen werden durch die Komponenten selbstständig durchgeführt und Störungen automatisch gemeldet. Sicherheitsrelevante Ereignisse werden eigenständig erkannt, verarbeitet und weitergeleitet.

#2: Mehr Wahlfreiheit und Heterogenität der Komponenten

Proprietäre Systeme sind endgültig Vergangenheit. Hersteller und Anbieter von Schließ- und Sicherheitskomponenten unterstützen offene Standards und sind von unterschiedlichen IoT-Plattformen aus steuerbar. Die Kunden haben die freie Wahl von Komponenten, Anbietern, Funktionen und Steuerbarkeit. Das Management der Einzelkomponenten erfolgt über herstellerunabhängige Standard Device Management Lösungen.

#3: Maximale Prozess-Integration, -Automation und -Sicherheit

Die Bedeutung konkret eingesetzter physikalischer Technik wird abnehmen. Die belastbare und sichere Prozessgestaltung gerät in den Vordergrund. Die Anforderungen sämtlicher betrieblicher Prozesse mit physikalischer Sicherheitsrelevanz werden in die Berechtigungs- und Zutrittsprozesse substanziell integriert. Mitarbeiter, externe Personen wie Besucher, Logistiker, Kunden und Lieferanten werden berücksichtigt. Zudem werden alle Berechtigungen (IT, physikalische, Workflowprozesse) regelbasiert, dynamisch und automatisiert ermittelt und vergeben. Relevante Veränderungen in Funktionsstrukturen, Sicherheitsbereichsstrukturen, Policies, Compliance Vorgaben, BCM, Notfallszenarien, Arbeitsschutz und -Sicherheit sowie Datenschutz werden automatisiert von den Systemen umgesetzt – jede Veränderung ist revisionssicher nachvollziehbar.

Alle manuellen Vorgänge sind elektronisch verfügbar, es existiert kein papierbasierter Vorgang mehr. Die Beteiligten, ob interne oder externe Personen, sind jederzeit über stationäre oder mobile Geräte aktiver Teil der Prozessketten. Alle Systeme sind über Online-Schnittstellen miteinander verbunden. Intelligente Software-Agenten überwachen deren Funktionen, erkennen Unregelmäßigkeiten und reagieren darauf. Das System- und Prozessverhalten passt sich dynamisch den aktuellen Bedrohungslagen und Sicherheitsbedürfnissen an.

#4: Der Mensch ist Maß aller Dinge

Interne und externe Personen sind nicht weiter lediglich verwaltete „Stammsätze" in Systemen – sie sind Schutzziel und Gefahrenpotential gleichermaßen. Ihre Bedürfnisse und Berechtigungen werden durch ihre Aufgaben, Tätigkeiten und Funktionen innerhalb von Organisationen bestimmt. Wo, wann und was sie arbeiten hat unmittelbaren Einfluss auf ihre (Zutritts-) Berechtigungen. Ihre Aufgaben und Arbeitsorte sind oftmals wechselnd und somit auch ihre jeweiligen aktuellen Berechtigungen, die dynamisch ermittelt werden.

Menschen werden zu Usern – inmitten elektronisch abgebildeter Prozesse sind sie aktive Teilnehmer und erhalten entsprechend ihrer Funktion beziehungsweise Position Zugriff auf einfach gestaltete und intuitiv zu bedienende Self-Service-Portale.

#5: (Physikalische) Sicherheit wird IT-Disziplin

Die betrieblichen digitalen Transformationsmaßnahmen werden dazu führen, dass sich der Prozess Ownership in Richtung IT verschiebt. Darüber hinaus sind Sicherheitsstrategien und -prozesse im Bereich der physikalischen Sicherheit in vielen Fällen analog den IT-Sicherheitsprozessen zu behandeln. Das Management von Sicherheitskomponenten wird durch den Einsatz von IoT-Aktoren ebenfalls in zentrale IT-Systeme verlagert. Verantwortliche Sicherheitsexperten im Bereich der Physikalischen Sicherheit werden sich hauptsächlich auf das Design von Vorgaben, Prozessen und Notfallszenarien konzentrieren. Die Verlagerung auch solcher Aufgaben an spezialisierte externe Service Provider wird ebenfalls eine Option sein.

Die Chance: Mut zum Gestalten

Ohne Zweifel: die Zeichen stehen auf Veränderung und erhebliche Risiken, wie Bedrohung von Hackerangriffen und Korrumpierung, sind tägliche Realität und die permanente Herausforderung schlechthin. Gleichzeitig ist das Bewusstsein des aktiven Handelns in den obersten Entscheidungsgremien der Unternehmen angekommen – mit der Bereitschaft, richtungsweisende Veränderungen und die entsprechenden Investitionen auf den Weg zu bringen.

Die Verantwortlichen der Unternehmenssicherheit haben nun eine einmalige Chance. Sie haben die Möglichkeit, aktiver Teil und mutiger Mitgestalter dieser Entwicklung zu sein. Die aktuelle Deloitte-Studie zum Thema Führung in digitalen Transformationsprozessen, „Strategy, not Technology, Drives Digital Transformation", bringt es auf den Punkt: „Today, the costs of inaction almost always exceed the costs of action" (heute übersteigen die Kosten der Untätigkeit fast immer die Kosten des Handelns). Es gibt keinen Grund mehr, auf irgendetwas zu warten. Gehen wir also mit einem klaren, strategisch basierten Ziel voran – besonnen, mutig und entschlossen.

Peter Kiess, Geschäftsführer der Gesellschaft für integrierte Informationssysteme (gis) mbH, www.gis-consulting.de
Co-Gründer der „Cooperative Cognitive Computing" Advisor - Prozess- und Systemdesigner