

CIO-Trends 2018: Technologien und Herausforderungen



In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Unternehmen zahlreicher Branchen befinden sich derzeit in einer Umbruch- und Umbauphase. Neue Technologien verändern bestehende Geschäftsmodelle wie -prozesse und schaffen neue. Das stellt viele Unternehmen vor ganz neue Herausforderungen, nicht zuletzt auch in Fragen der Sicherheit. Datenschutz, DDoS-Angriffe, Ransomware und vernetzte Welten – das Sicherheitsjahr 2018 bringt für IT-Abteilungen vielfältige Aufgaben mit.

Angesichts der Geschwindigkeit der technologischen Neuerungen wird das Jahr 2018 wohl spannend wie nie. So könnte beispielsweise das Internet der Dinge in anderen Technologien, wie etwa dem maschinellen Lernen aufgehen. Dieser E-Guide betrachtet technische Entwicklungen, die 2018 relevant werden. So etwa künstliche Intelligenz, IoT, VR, Robotik und weitere Innovationen.

Sie sind häufig die Grundlage für vernetzte Produkte und Dienste: Die digitalen Zwillinge, bei denen etwas physisch und real existierendes digital abgebildet wird. Wir liefern einen Überblick, wie Digital Twins verschiedenen Branchen helfen können und zeigen wie digitale Zwillinge unterschiedliche Branchen prägen.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

■ Cybersicherheit 2018: Das kommt auf Unternehmen zu

Malte Jeschke, SearchSecurity.de

Das abgelaufene Jahr 2017 war durch einige sehr publikumswirksame Cyberangriffe wie etwa [WannaCry](#) gekennzeichnet. Auch wenn dabei die Anzahl der absolut betroffenen Systeme nicht die Hauptrolle spielte, sondern eher die möglichen wirtschaftlichen Auswirkungen, wenn ein Unternehmen ernsthaft davon betroffen war.

Ob [Ransomware](#) oder [DDoS](#), häufig geht es schlicht ums Geld. Aufgrund der sich verändernden IT-Landschaften bieten viele Unternehmen eine schnell wachsende Angriffsfläche. Und schon ohne neue Bedrohungen durch Angreifer hätten Sicherheitsverantwortliche alle Hände voll zu tun.

So gilt es ganz nebenbei, die eigene Sicherheitsstrategie an neue Gegebenheiten anzupassen, sowie Richtlinien wie die Datenschutz-Grundverordnung ([EU-DSGVO](#)) umzusetzen. Dies sind ja zudem keine Aufgaben, die alleine der IT-Sicherheit obliegen, sondern viele Abteilungen und Abläufe in Unternehmen tangieren oder sehr direkt betreffen. Das gilt insbesondere auch für das Zusammenwachsen von IT und der operativen Technologie - Stichwort Industrie 4.0.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Aber diese Herausforderungen werden durchaus auch bei IT-Abteilungen und Sicherheitsverantwortlichen als Chance verstanden. Sorgen sie doch in einigen Fällen für höhere Budgets und die Möglichkeit, wieder für mehr Transparenz im eigenen Unternehmen zu sorgen.

Alles in allem Grund genug, einen Blick darauf zu werfen, welche Erwartungen renommierte Sicherheitsanbieter für das Jahr 2018 haben.

EU-Datenschutz-Grundverordnung als Herausforderung

Seit 2016 ist die EU-Datenschutz-Grundverordnung (EU-DSGVO) in Kraft. Ende Mai 2018 endet die zweijährige Übergangsfrist, die Unternehmen und Behörden zur Umsetzung der Richtlinien bleibt. Und das ist keine Aufgabe, die auf die leichte Schulter genommen werden sollte. Nicht nur mediale Aufmerksamkeit erfährt das Thema insbesondere im Hinblick auf die möglichen [Bußgelder und Sanktionen](#) bei Verstößen gegen die Richtlinien. Viele Unternehmen werden nicht nur noch im ersten Halbjahr damit beschäftigt sein, die [Compliance](#) in Sachen EU-DSGVO umzusetzen.

Und diese Umsetzung erstreckt sich auf viele Bereiche der IT-Sicherheit. So haben viele Organisationen wohl noch Nachholbedarf bei entsprechenden Maßnahmen. Die Datenschutz-Grundverordnung beinhaltet auch strengere Vorschriften im Hinblick auf das Melden von relevanten Sicherheitsvorfällen.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Nach Ansicht von [IBM](#) wird 2018 daher das Jahr sein, in dem große Unternehmen erstmals in der Lage sein werden, schnell und angemessen auf Datenpannen oder Cyberangriffe zu reagieren.

Es wird wohl allerdings nicht allen Unternehmen gleich leichtfallen, die Verordnung umzusetzen. So geht [G DATA](#) davon aus, dass rund 50 Prozent der Unternehmen bis zum Stichtag 25. Mai 2018 nicht konform zu EU-DSGVO sein werden. Bei [ForgeRock](#) glaubt man, dass sich die EU-DSGVO auch auf Geschäftsmodelle auswirken wird. So würden sich Unternehmen darauf vorbereiten müssen, dass sich das Vertrauen der Kundschaft verringert, wenn nur Compliance-Regeln eingehalten werden. Nur wenn eine Kontrolle über die Daten garantiert wird, würde dies ein Angebot wirklich kundenbindend machen.

Ransomware - das Geschäftsmodell Erpressung

Auch wenn viele Unternehmen inzwischen deutlich besser vor Ransomware geschützt sind als in der Vergangenheit, wird die Bedrohung durch derlei Schadsoftware auch 2018 eine ernsthafte Herausforderung sein. Die Art und Weise der Angriffe wird sich allerdings verfeinern und verändern.

So geht [Trend Micro](#) von einem Zuwachs bei den gezielten Ransomware-Angriffen aus, bei denen Cyberkriminelle einzelne Unternehmen ins Visier

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

nehmen und deren Geschäfte lahmlegen, um entsprechenden Lösegeldforderungen Nachdruck zu verleihen. Bei [Vectra](#) geht man ebenfalls davon aus, dass Angriffe, die den Betriebsablauf in Firmen lahmlegen oder zumindest stören, zunehmen werden. Nach Ansicht von IBM werden zunehmend IoT-Geräte von Ransomware betroffen sein und in ihrer Funktion blockiert werden.

So erwartet [Barracuda Networks](#) eine Entwicklung von der Ransomware zur Protectionware, also von der Lösegelderpressung zur Schutzgelderpressung. Cyberkriminelle werden nicht nur Geld für das Freischalten verschlüsselter Daten verlangen, sondern würden Unternehmen auch immer häufiger mit Schutzgeldforderungen ins Visier nehmen.

[Fortinet](#) rechnet ebenfalls mit einer zunehmenden Anzahl an Ransomware-Attacken und sieht auch Cloud-Anbieter als Angriffsziel. Bei erfolgreichen Attacken betreffen dann die Folgen entsprechend viele Unternehmen. Auch technisch würde sich die [Malware](#) weiterentwickeln. Bitdefender geht von immer ausgefeilterer Ransomware aus, die beispielsweise auch [GPU](#)-Leistung zur [Verschlüsselung](#) nutzen werden, um Sicherheitssoftware zu umgehen.

Der Erfolg der Ransomware erklärt sich häufig durch den erzielbaren monetären Erfolg. Letzteres ist nach Ansicht von Trend Micro auch einer der Gründe für das Zunehmen von Business E-Mail Compromise ([BEC](#)). Bei

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

diesen Angriffen werden bestimmte Mitarbeiter eines Unternehmens nach ausführliche Recherche und [Social Engineering](#) sehr gezielt ins Visier genommen. Diese Mitarbeiter mit entsprechender Verantwortung werden dann dazu verleitet, bestimmte finanzielle Transaktionen vorzunehmen.

So werden laut [Airbus Cybersecurity](#) fehlende Social-Media-Sicherheitsrichtlinien zum ernsthaften Risiko für Unternehmen. Die sozialen Medien lassen sich zum Auspionieren von Informationen nutzen und seien damit ein Einfallstor für hochentwickelte Angriffe auf Unternehmen.

Vernetzte Welten - IoT, Industrie 4.0 und Co.

Die Veränderungen der IT-Landschaft und -Netzwerke sorgt dafür, dass viele Unternehmen ihre Sicherheitsstrategie entsprechend anpassen müssen. Denn mit der zunehmenden Vernetzung vergrößert sich auch die Angriffsfläche, die Unternehmen bieten. Das gilt natürlich für die Cloud-Nutzung, aber auch insbesondere für vernetzte Geräte, die bislang bei Security-Gedanken nur selten Berücksichtigung fanden. IT und Operative Technologie wachsen zunehmend zusammen, damit wächst auch die Angriffsfläche und die Zahl der vernetzten Plattformen, die angegriffen werden können. Und diese stellen gleich in mehrfacher Hinsicht ein besonderes Risiko dar.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Aufmerksamkeit erregten in 2017 insbesondere Botnetze, bei denen missbrauchte IoT-Geräte für DDoS-Angriffe genutzt wurden. Bei [Radware](#) glaubt man, dass sich diese Denial-of-Service-Landschaft auch 2018 kontinuierlich weiterentwickeln. Schon allein aufgrund der zunehmenden Zahl der eingesetzten IoT-Geräte. So könnten Angreifer aufgrund der schlechten Sicherheitsstandards immer mehr anfällige IoT-Geräte finden. [Bitdefender](#) rechnet gleichfalls damit, dass große IoT-Botnets in 2018 zur Normalität werden.

So würde die Verwaltung der Konnektivität von IoT-Geräten Unternehmen vor große Herausforderungen stellen. [Riverbed](#) geht daher davon aus, dass entsprechende Dienstleistungen davon profitieren werden.

Aber vernetzte Geräte können nicht nur missbraucht werden, oder als Einfallstor ins Firmennetzwerk fungieren, sie bieten auch Möglichkeiten für gezielte Angriffe und Erpressungsversuche auf Unternehmen, die verheerende Folgen haben können.

Maschinelles Lernen, KI und Automatisierung

Insbesondere beim Aufspüren von Bedrohungen und Erkennen von sicherheitsrelevanten Ereignissen helfen neue Sicherheitslösungen, die sich Technologien wie maschinellem Lernen oder künstlicher Intelligenz in

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

unterschiedlichen Ausprägungen bedienen. Allerdings nutzen auch Cyberkriminelle die neuen Möglichkeiten.

So berichtet Vectra, dass Cyberkriminelle Machine Learning einsetzen, um den Prozess des Auffindens von Sicherheitslücken in kommerziellen Produkten zu beschleunigen. Zudem werden Angreifer nach Angaben von Trend Micro zunehmend Technologien wie [Blockchain](#) und maschinelles Lernen nutzen, um ihre Aktivitäten besser vor traditionellen Sicherheitsmaßnahmen verstecken zu können.

IBM geht für 2018 von einer Zunahme bei KI-basierten Angriffen aus, da Cyberkriminelle Technologien einsetzen werden, um menschliches Verhalten zu imitieren. Dementsprechend müssten die Sicherheitsanbieter ihre KI-Tools weiterentwickeln.

Schwachstellen- und Patch-Management

Ob Ransomware, IoT-Sicherheit oder auch Datenschutz - das Schließen von Sicherheitslücken und das Patch-Management sind von elementarer Bedeutung für die Gesamtsicherheit eines Unternehmens. Viele der spektakulären Angriffe und Datendiebstähle sind nur aufgrund bekannter und nicht geschlossener Schwachstellen möglich gewesen.

//////
In diesem E-Guide

■ Cybersicherheit 2018: Das
kommt auf Unternehmen zu

■ Technologische Innovationen
2018: AI, IoT, VR und Robotik

■ Industrie wendet sich verstärkt
Digital-Twin-Technologien zu

Und diese Herausforderung wächst mit der sich durch die zunehmende Vernetzung vergrößernden Angriffsfläche. Bei Sicherheitsverantwortlichen sollte daher ein entsprechendes Patch-Management sehr weit oben auf der Agenda stehen.

////////////////////////////////////

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

■ Technologische Innovationen 2018: AI, IoT, VR und Robotik

Chris Matthieu, Citrix

Die rasante Innovationsgeschwindigkeit in der modernen Technikwelt macht die Prognosen, was im jeweils nächsten Jahr Trendthemen sein werden, interessanter und spannender als jemals zuvor. In früheren Generationen mussten Visionen von weltverändernden technologischen Änderungen mindestens mehrere Jahrzehnte in der Zukunft spielen - im Fall der Zeichentrickserie *Die Jetsons* sogar ein ganzes Jahrhundert.

Heute würde ein Zeitreisender, der nur wenige Jahre aus der Vergangenheit zu uns kommt, baff sein angesichts von verbreitet genutzten staatenlosen digitalen Währungen, allgemein verfügbaren selbstparkenden Autos oder Smartphones, die ihren Besitzer per Gesichtserkennung identifizieren.

In diesen Zeiten des raschen Wandels müssen unsere Prognosen für 2018 nicht zurückhaltend ausfallen, damit sie glaubwürdig sind. Während einige der Entwicklungen, die wir vorhersehen, relativ unspektakulär sind und graduelle Fortschritte von 2017 darstellen, gehen andere beträchtlich darüber hinaus - und deuten an, dass die technische Wunderwelt, die *Die Jetsons* skizzieren, womöglich früher Realität wird, als wir gedacht haben.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Machine Learning und AI definieren den Mainstream neu

Wenn Tools und Plattformen für [Machine Learning](#) (maschinelles Lernen) und künstliche Intelligenz (Artificial Intelligence, AI) sich einfacher nutzen lassen, werden sie auch immer mehr Lebensbereiche durchdringen. Indem sie für ihre Trainingsphase die [Skalierbarkeit](#) der Cloud in Anspruch nehmen, werden diese Technologien gewaltige Auswirkungen auf die Zukunft der Arbeit haben. Aufgrund ihrer Fähigkeit zu lernen, was normal ist und was nicht, werden Maschinen eine stetig wachsende Rolle bei der Automatisierung und der vorausschauenden Problemlösung spielen. Sie werden sogar in der Lage sein, potenzielle Täter zu erkennen und auszuschalten, um Sicherheitsverstöße zu verhindern.

Blockchain jenseits von Kryptowährung

[Blockchains](#) und Kryptowährungen mögen fast schon als überholt gelten - doch wir stehen erst am Anfang, was die Auswirkungen dieser miteinander verwandten Technologien angeht. Wir werden im 2018 erleben, wie wichtige neue Anwendungsfälle entstehen. Dezentralisierte und verteilte Unternehmen werden in der Lage sein, mit geringer oder gar keiner eigenen

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Infrastruktur an die Spitze zu gelangen und vielleicht sogar die derzeit dominierenden Cloud-basierten Giganten zu stören.

Edge Computing auf dem Vormarsch

Die Nachfrage nach [Edge Computing](#) wird 2018 spürbar zunehmen. Wenn sich eine größere Anzahl von Geräten mit dem Internet verbinden, wird die [Latenz](#) immer mehr zu einem Problem. Die Cloud wurde für umfangreiche Downloads konzipiert - nicht für Uploads. Anstatt alles zum Zweck von Machine Learning in die Cloud zu verlagern, werden sich Sensoren auf Edge Computing stützen, um zu lernen, was normale Bedingungen sind, und um auf anormale Bedingungen zu reagieren. Dies wird sich enorm auf die Zukunft der Arbeit und Sicherheit auswirken.

Fahrerlose Autos werden noch intelligenter

Autonome Fahrzeuge werden weiterhin die Märkte unter anderem für Personenbeförderung, Landwirtschaft, Logistik und Versand durcheinanderbringen. Da sie als mobile Edge Data Center auf Rädern fungieren, werden diese Fahrzeuge Terabyte oder Petabyte an Sensordaten verarbeiten, um in Echtzeit auf die Verhältnisse in der Umgebung zu reagieren. Autonome Lieferungen und Pendelfahrzeuge gehören in der Nähe meines Wohnortes Tempe (Arizona) bereits zunehmend zum normalen

In diesem E-Guide

■ Cybersicherheit 2018: Das kommt auf Unternehmen zu

■ Technologische Innovationen 2018: AI, IoT, VR und Robotik

■ Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Straßenbild, da fahrerlose Autos von Uber, Waymo und GM auf dem Campus der Arizona State University ihre Runden drehen.

AR, VR und MR definieren die Realität neu

Der Hype um [Augmented Reality](#) (AR), virtuelle Realität (Virtual Reality, VR) und Mixed Reality (MR) wird sich intensivieren, wenn neue Produkte und Funktionen auf den Markt kommen. Magic Leap treibt gerade eine weitere Milliarde Dollar auf, und genauso machen es viele Konkurrenten.

AR wird in der Arbeitswelt der Zukunft schon genutzt, etwa für Anwendungen im Baugewerbe und zur Unterstützung von Vor-Ort-Reparaturen. Citrix führte während der Synergy VR-Workstations vor, die sich mit normalen Brillen betreiben lassen. Da diese Technologie immer kleiner und leistungsfähiger wird und infolgedessen immer weitere Bereiche erobert, wird sie zunehmend mit autonomen Fahrzeugen, Machine Learning und Edge-Computing-Technologien verschmelzen. So wie das iPhone X den Wendepunkt für eine umfassende Gesichtserkennung markiert hat, werden wir 2018 erleben, dass viele AR-Einsatzszenarien den Bereich des Spekultativen verlassen und in der realen Welt ankommen, dicht gefolgt von Durchbrüchen bei VR.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

IoT macht uns gesünder

Wir haben schon gesehen, welche Auswirkungen das **IoT** (Internet of Things) auf Schwerindustrien, etwa die Öl- und Gasbranche, hatte. Dort erfassen Sensoren Echtzeitdaten, um Automatisierung zu ermöglichen, die Betriebssteuerung zu verbessern und Kosten zu senken.

Als Hurrikan Irma Kurs auf Florida nahm, verwendete Tesla IoT-Technologie, um die Reichweite seiner Fahrzeuge in dem Gebiet zu vergrößern, indem die Batterieleistung verbessert wurde und somit die Menschen eine bessere Chance erhielten, dem Sturm auszuweichen.

Nun wird IoT das Gesundheitswesen umkrempeln. Kleinere Innovationen wie das Streamen von Vitalwerten der Patienten direkt in deren elektronische Gesundheitsakte werden Fehler reduzieren und Zeit sparen, so dass die Ärzte mehr Patienten pro Tag behandeln - und, nebenbei bemerkt, mehr Geld verdienen - können. Außerdem lassen sich auf diese Weise die Ergebnisse verbessern, indem die Genauigkeit und Effizienz der medizinischen Betreuung gesteigert wird.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

â€ und wird trotz Omniprâ€senz zum alten Hut

Sie werden den Begriff *Internet of Things* nicht mehr lange hren. Etwa im Laufe des Jahres 2018 wird es zur Selbstverstâ€ndlichkeit, dass Gerâ€te sich automatisch mit dem Internet verbinden, und jedes Unternehmen muss entweder eine IoT-Plattform besitzen oder mieten, um auf dem Markt zu bestehen.

Der Wettbewerb wird zum Motor fr vollstâ€ndig automatisierte IoT-Geschâ€ftsprozesse mit Just-in-Time-Nachschublieferungen und automatisch skalierenden Services. Es wird darber hinaus eine Reihe von IoT-Start-ups geben, die sich auf Technologien konzentrieren, die automatisch Menschen und Profile erkennen und eine Rolle bei der kontextabhâ€ngigen Automatisierung an beliebigen Orten spielen werden - in der Arbeit, zu Hause, im Cafe und so weiter. Diese neuen Lsungen werden in den Technologien, die in autonomen Fahrzeugen, Machine Learning und Edge-Computing-Verfahren stecken, enthalten sein oder mit ihnen verschmelzen.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Die neue Robotikwelle

Während der Hype rund um IoT abnimmt, heißt der nächste logische Entwicklungsschritt für den Brain Trust und Unternehmen, die das Modewort populär gemacht haben, Robotik. Wir dürfen uns darauf gefasst machen, dass mehr Spezialroboter auf den Markt kommen, je weiter wir uns 2019 nähern. Stellen Sie sich ein auf *der Roomba für* alles Mögliche, von Rasenmähern und Grillreinigern bis zu Waschstraßen.

Die neuen Robotikgeräte für den Verbraucher mögen vielleicht nicht so witzig oder stylish sein wie der Haushaltsroboter Rosey aus *Die Jetsons*. Aber zwischen der intelligenten Automatisierung, die sie für den Alltag bringen, den automatischen Technologien, die unsere Umgebung ändern, den selbstfahrenden Autos, die beeinflussen, wie wir über das Transportwesen denken, und so vielen anderen, bereits eingeleiteten Innovationen würden sich George und Jane Jetson in der heutigen Welt zunehmend zu Hause fühlen - fast ein halbes Jahrhundert früher als geplant.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

■ Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Scott Robinson, Analogica

Mit dem Aufblühen des digitalen Zeitalters erschien es fast unvermeidlich, dass ein Teil dessen, was in der physischen Welt existierte, im digitalen Bereich zum Leben erwacht, und dass diese Nachbildung letztendlich auch einen geschäftlichen Wert erhält.

Das Konsumuniversum wird zunehmend digitalisiert - E-Books und digitale Musik sind überall - und der 3D-Druck hat die Digitalisierung zu einer zweispurigen Straße gemacht. Das Stichwort heißt: Digital Twins (digitale Zwillinge).

Verschiedene Definitionen von Digital Twins

Die Nennwertdefinition des Begriffs *Digital Twin* ist eine digitale Instanziierung eines realen physischen Assets. Ein Beispiel hierfür ist das 3D-Druckverfahren: Eine digitale Instanziierung eines Objekts wird verwendet, um das Objekt tatsächlich zu erzeugen. Unter Verwendung

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

älterer Terminologien kann man sich einen Digital Twin als eine Simulation von etwas Realem vorstellen.

In einer Präsentation des GE Global Research Center definiert Colin Parris, Vice President of Software Research bei GE, einen digitalen Zwilling als „ein lebendiges Modell von etwas, das ein Geschäftsergebnis liefert“ und operationalisiert das Konzept in der Praxis.

Gartner definiert einen digitalen Zwilling als „ein dynamisches Softwaremodell eines physischen Dings oder Systems“ - die Schlüsselwörter sind Dynamik und System. Die digitale Zwillingstechnologie ist so wichtig, dass sie einen Platz unter den [Top 10 Strategic Technology Trends for 2017](#) von Gartner eingenommen hat.

Die Ursprünge digitaler Zwillingstechnologie

Digitale Zwillinge sind nicht neu - sie gibt es schon seit mehr als 15 Jahren - und sie sind nicht speziell eine Innovation aus dem Geschäftsleben.

Tatsächlich war die Schaffung digitaler Repräsentationen physischer Objekte der Notwendigkeit der NASA geschuldet, extraterrestrisch Umgebungen zu modellieren, um Hardware hierfür zu bauen. Da ein Roboter auf dem Mars nicht in Echtzeit überwacht werden kann, war es für die NASA

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

wichtig, die Umgebung als digitale Simulation zu modellieren, während sie den Roboter entwarf und baute, um sicherzustellen, dass er beim ersten Mal richtig funktioniert.

Diese Überbrückung der physischen und digitalen Sphären ermöglicht die Modellierung des Verhaltens und der Lebenszyklen von Objekten im physischen Raum. Im Zeitalter des [Internet der Dinge](#) (IoT) und der [Cloud](#) erlaubt es diese Methode, digitale Modelle ständig mit realen Daten aus der physischen Welt zu aktualisieren. Das physische Objekt (oder der Prozess) und sein digitaler Zwilling verbessern sich im Laufe der Zeit deutlich. Und die Anwendungsmöglichkeiten dieses Konzepts sind vielfältig.

Ein geschäftlicher Imperativ für digitale Zwillinge

In einem [Forbes-Artikel](#) beschreibt Thomas Kaiser, Senior Vice President of IoT bei [SAP](#), digitale Zwillinge als eine entscheidende Grundlage für vernetzte Produkte und Services.

„Unternehmen, die nicht reagieren, werden zurückgelassen. Diejenigen, die digitale Zwillinge annehmen, haben die Möglichkeit, Kundenbedürfnisse besser zu verstehen, ihre Produkte und Dienstleistungen kontinuierlich zu verbessern und sogar neue Geschäftsmodelle zu identifizieren, die ihnen Wettbewerbsvorteile verschaffen“, erläutert Kaiser.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Tatsächlich hat IoT die digitale Zwillingstechnologie in den Vordergrund gerückt. Die Fähigkeit von realen Objekten, Informationen aus sich selbst und ihrer Umgebung zu sammeln und diese in Echtzeit über das Internet weiterzugeben, macht Digital Twins zu einem unverzichtbaren Bestandteil der [prädiktiven Analytik](#) für alle Produkte und Prozesse, die die IoT-Technologie nutzen. Mit anderen Worten, das Internet der Dinge und die digitalen Zwillinge sind füreinander bestimmt.

Unzählige Einsatzszenarien für digitale Zwillinge

Während sich das Internet der Dinge innerhalb und über Branchen hinweg ausweitete, werden sich digitale Zwillinge ebenfalls verbreiten - und ihre Nutzung wird sich entsprechend der Nutzung des Internet der Dinge ausbreiten. Hier nur einige Beispiele:

Branchenübergreifende Datenerhebung und -analyse: Der Stand der Technik in der Produkt- und Dienstleistungsentwicklung war vor digitalen Zwillingen reaktiv, nicht proaktiv.

„Wenn ein Asset fehlschlägt oder kurz davor ist, zu versagen, sammeln die meisten Industrieunternehmen Daten, ohne wirklich zu wissen, welche Daten sie sammeln sollen“, erläutert Parris. „Dies sind [unstrukturierte Daten](#). Das Unternehmen konfiguriert das Datenerfassungs- und Analysemodell in der

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Folge so um, dass es Sinn macht, die Daten zu erfassen und den Prozess zu verfeinern, bevor es ihn erneut ändern muss, wenn weitere Probleme auftauchen. Es ist ein statisches Lese- und Reaktionsmodell.“

Digitale Zwillinge beseitigen dieses statische Modell und ersetzen es durch ein dynamisches Modell - ein lebendiges Modell, so Parris. Das Rätselraten wird aus der Datenerhebung entfernt, und die gesammelten Daten werden zur Vorbeugung und nicht zur Diagnose nach einem Ausfall verwendet.

Prototyping: Die Digital-Twin-Technologie ermöglicht virtuelles Prototyping - die digitale Erstellung eines Produkts oder einer Dienstleistung, bevor sie physisch instanziiert wird - sowie die Simulation der beabsichtigten Umgebung und des Betriebs. Diese Art des Prototyping ist nicht nur schneller und billiger, sondern letztlich auch präziser, was zu einer höheren Qualität des Produkts oder der Dienstleistung führt.

Im Außendienst: Die Kombination von IoT und digitalen Zwillingen kann zu Predictive Maintenance führen, das heißt die Fähigkeit zu wissen, dass eine Komponente ausfallen wird, bevor sie tatsächlich ausfällt. Der Außendienst kümmert sich in diesem Fall darum, ein Bauteil vor dem Ausfall auszutauschen, und nicht, um bereits ausgefallene Teile zu ersetzen beziehungsweise das zu reparieren, was infolge des Ausfalls defekt ist.

Im industriellen IoT (IIoT): [Industrial IoT](#) eröffnet neue Möglichkeiten bei komplexitätsbelasteten Produkten und Prozessen. Flugzeugmotoren,

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Fabrikroboter und andere komplexe Maschinen sind schwierig zu modellieren, da sie einzelne Komponenten und Prozesse kombinieren, die unerwartet interagieren können. Es ist schwierig, diese Wechselwirkungen bereits in der Entwurfsphase vorherzusehen.

Durch den Einsatz von Industrial IoT (wobei der Flugzeugmotor oder der Fabrikroboter viele Sensoren enthält) in Kombination mit digitalen Zwillingen lassen sich Interaktionen zwischen Komponenten und Prozessen wesentlich einfacher lokalisieren - und anschließend planen. Und diese Daten sorgen nicht nur für ein besseres Design, sondern fließen auch in den oben erwähnten Predictive-Maintenance-Prozess ein.

Digitale Zwillinge sind sicherlich da, um zu bleiben. [Gartner prognostiziert](#), dass sie innerhalb von drei bis fünf Jahren Milliardenbeträge erreichen werden.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Über die Autoren

MALTE JESCHKE ist Senior Online Editor der deutschen TechTarget-Webseiten SearchDataCenter.de, SearchEnterpriseSoftware.de, SearchNetworking.de, SearchSecurity.de und SearchStorage.de. Er beschäftigt sich unter anderem mit der IT-Sicherheit in all ihren Facetten. Als IT-Journalist ist er seit 1991 tätig, seit 1996 sind seine Inhalte auch online zu lesen. Vor seiner journalistischen Tätigkeit setzte er IT-Projekte für Großunternehmen um.

CHRIS MATTHIEU war Mitbegründer und CTO von Octoblu, einer revolutionären Echtzeit-IoT-Plattform, die von Citrix erworben wurde. Chris ist nun der Direktor des IoT Engineering bei Citrix. Octoblu verbindet Dinge, Systeme, Personen und Clouds zu einem globalen Mesh-Netzwerk, das es Benutzern ermöglicht, Design-Flows, Prozesse und Sensordaten zu automatisieren und zu kontrollieren sowie auf Echtzeit-Ereignisse, Nachrichten, große Datentrends und Anomalien zu reagieren.

SCOTT ROBINSON hat 20 Jahre IT-Erfahrung. Seine Spezialgebiete umfassen vor allem Business Intelligence und System Integration. Er ist ein Enterprise-Architekt und hat einen Abschluss in Sozialpsychologie.

In diesem E-Guide

- Cybersicherheit 2018: Das kommt auf Unternehmen zu
- Technologische Innovationen 2018: AI, IoT, VR und Robotik
- Industrie wendet sich verstärkt Digital-Twin-Technologien zu

Impressum



CIO-Trends 2018: Technologien und Herausforderungen

Ist eine Publikation von SearchSecurity.de

Michael Eckert | *Editorial Director*

Malte Jeschke | *Senior Online Editor*

Tobias Wendehorst | *Online Editor*

Jakob Jung | *Online Editor*

Becky Wrigley | *Production Editor*

Brent Boswell | *Herausgeber*

BBoswell@techtarget.com

TechTarget

275 Grove Street, Newton, MA 02466

www.techtarget.com

© 2018 TechTarget Inc. Kein Teil dieser Veröffentlichung darf ohne vorherige schriftliche Genehmigung des Verlages in irgendeiner Form oder auf irgendeine Weise weitergegeben oder reproduziert werden. Nachdrucke von TechTarget-Publikationen sind verfügbar über The YGS Group.

Über TechTarget: TechTarget publiziert Informationen für Profis im Bereich Informationstechnologie. Mehr als 100 Themen-Websites ermöglichen schnellen Zugriff auf ein reichhaltiges Angebot an Nachrichten, Ratgebern und Analysen über die Technologien, Produkte und Prozesse, die entscheidend sind für beruflichen Erfolg. Unsere Live- und virtuellen Veranstaltungen vermitteln direkten Zugang zu den Einschätzungen und Ratschlägen unabhängiger Experten. IT Knowledge Exchange, unsere soziale Community, bietet die Möglichkeit, um Rat zu fragen und sich mit Kollegen und Experten über Lösungen auszutauschen.

■ Erhalten Sie mehr exklusive Inhalte von PRO+

Als Mitglied erhalten Sie Zugriff auf unser PRO+ – Angebot – eine Auswahl von freien Inhalten, Trainingsmaterialien und exklusiven Möglichkeiten, die speziell von unseren Partnern und unseren Seiten bereitgestellt wurden

PRO+ – Angebote bietet kostenlose Inhalte, die nur für unsere Mitglieder zur Verfügung gestellt werden.

Nutzen Sie die Vorteile Ihrer Mitgliedschaft in vollem Umfang und besuchen Sie
<http://www.searchSecurity.de/ehandbooks>

Titelbild: stock.adobe.com

©2018 TechTarget. Diese Veröffentlichung darf ohne schriftliche Erlaubnis des Herausgebers weder weitergeleitet noch reproduziert werden.