

# Die Zukunft der Sicherheitstechnik

Technologien wie IoT, Edge- und Cloud-Computing, Software Suites und auch Smart-Home werden die Sicherheitstechnik nachhaltig verändern. Ein Ausblick auf 2021 und darüber hinaus.

DR. PETER FEY

Die Produkte der sicherheitstechnischen Industrie waren immer schon „smart“, doch der Trend wird sich in Zukunft weiter beschleunigen. Diese Entwicklung hat seine Ursache in dem Voranschreiten von Themen wie Künstliche Intelligenz (KI) sowie dem massiven Vormarsch von Cloud-Lösungen aller Art. Zwar sind heute noch viele der mit dem Prädikat „KI“ gepriesenen Produkte eher auf dem Level von klassischen Algorithmen angesiedelt, doch zukünftig werden Cloud-basierte Systeme durch ihre schiere Rechenleistung mehr und mehr KI-Anwendungen an der Edge („vor Ort“) unterstützen. Allerdings ist der Umgang mit sicherheitsrelevanten Informationen sehr diffizil. In diesem Zusammenhang sind die Aktivitäten rund um die europäische Gaia-X-Initiative auch für die Sicherheitstechnik von Interesse.

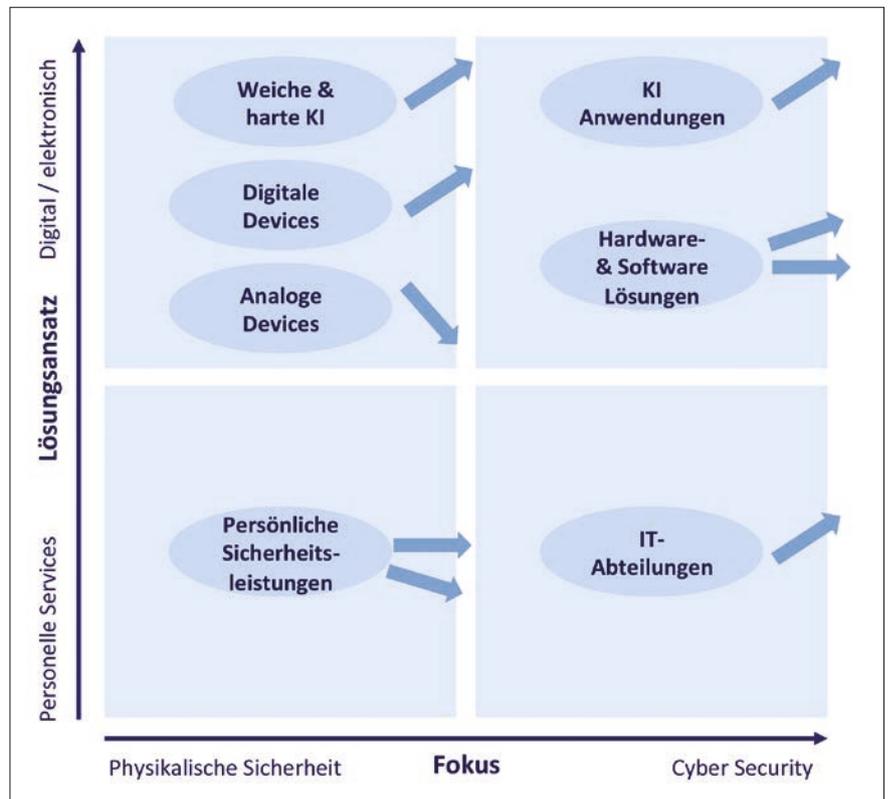
In der Vergangenheit war die Sicherheitstechnik noch sehr stark durch die physische Infrastruktur, das heißt eine Vielzahl an verschiedensten Sensoren, wie zum Beispiel Brand-, Einbruchmeldern und Videokameras sowie eine zentrale Einheit zur Verarbeitung der Daten beziehungsweise eine komplexe Leitstelle, definiert. In den letzten Jahren drängen jedoch immer mehr Begriffe in den Vordergrund, die aus unserer Sicht kurz- bis mittelfristig zu einem Paradigmenwechsel führen werden. Themen, die hierbei eine immer größere Rolle spielen werden sind folgende:

## Internet of Things (IoT)

Der Trend als solcher ist nicht neu, bekommt aber aufgrund der systemimmanenten Her-

„Die Sicherheitstechnik wird immer tiefer in die Logiken und Techniken moderner IT-Systeme eintauchen.“

ausforderungen eine Dynamik, welche die technologische Entwicklung vor sich her treiben wird. Aktuell gehen Schätzungen davon aus, dass 8,4 Milliarden IoT-Devices installiert sind. Dies bringt nicht nur Anforderungen an die IT-Sicherheit mit sich. Die Entwickler dieser Devices, zu denen auch die Anbieter der Sicherheitstechnik zählen, müs-



Spielbrett Sicherheitstechnik mit Entwicklungsperspektiven.

Grafik: Dr. Wieselhuber & Partner



Foto: Pixabay

Das Internet der Dinge (IoT) entfaltet immer mehr Dynamik. 8,4 Milliarden IoT-Devices sind laut Schätzungen aktuell bereits installiert.

sen sich mehr als bisher mit Fragen befassen, die sich auf neue Wege der Konnektivität, wie zum Beispiel Low-Power-Short- und Wide-Range-Networks sowie die hierbei verwendeten Technologien richten.

Energieverbrauch, Reichweite und Bandbreite stellen neben den verwendeten Protokollen hohe technische Ansprüche. Darüber hinaus werden sich die Entwickler mit den Fragen nach dem richtigen IoT-Betriebssystem, den unterschiedlichen IT-Layers von der Gerätesteuerung bis hin zu IoT-Anwendungsentwicklungen sowie zunehmend mit den Aspekten der Echtzeitfähigkeit vor allem beim Event-Streaming beschäftigen müssen. Für die Sicherheitstechnik bedeutet das ein immer tieferes Eintauchen in die Logiken und Techniken moderner IT-Systeme. Nicht vergessen sollte man hierbei die folgenden zentralen Fragestellungen: Was fangen die Unternehmen mit all den Daten an? Welchen Nutzen können sie ihren Kunden konkret bieten? Und wie kann daraus ein wirtschaftlicher Nutzen für das eigene Unternehmen generiert werden? Digitale Geschäftsmodelle sind zwar in aller Munde, viele Unternehmen scheitern aber an ihrer Konkretisie-



„Zukünftig werden Cloud-basierte Systeme durch ihre schiere Rechenleistung mehr und mehr KI-Anwendungen an der Edge unterstützen.“

**Dr. Peter Fey**, Mitglied der Geschäftsleitung bei Dr. Wieselhuber & Partner, München, und Branchenexperte für die Sicherheitstechnik.

rung getreu dem Satz „Von der Analyse zur Paralyse“.

### Edge versus Cloud-Computing

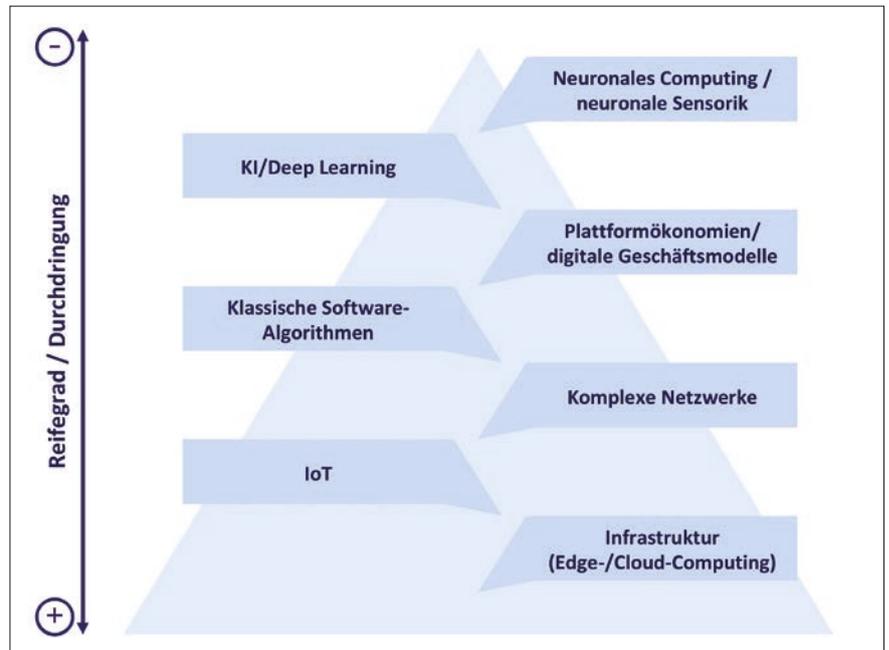
Anbieter von Software-Lösungen, wozu auch Security-as-a-Service zählt, haben sich von lange Zeit dominierenden Verkaufsmodellen abgewendet und stellen ihre Produkte auf Subscriptions- beziehungsweise Abo-Basis zur Verfügung. Die Software läuft zunehmend nicht mehr auf eigenen Rechenzentren/Servern, sondern in der Cloud – ein Trend, den jeder nicht nur im privaten, sondern zunehmend auch im geschäftlichen Umfeld beobachtet haben konnte. Dabei hat sich auch im Cloudgeschäft ein struktureller Wandel ergeben: Herrschten anfangs noch die sogenannten Privat Clouds vor, bei denen die Software in einer nur für den jeweiligen Kunden zugänglichen Cloud verwaltet wurde, hat sich in den letzten Jahren mit zunehmendem Tempo ein Schwenk hin zu den sogenannten Public- beziehungsweise Hybrid-Clouds vollzogen. Anbieter wie AWS, Microsoft Azure, Google und auch das chinesische Unternehmen Tencent verzeichnen Wachstumsraten, von denen andere Branchen nur träumen können. ▶

Foto: Dr. Wieselhuber & Partner

Schätzungen gehen auch weiterhin von glänzenden Geschäften aus: 2020 beträgt der weltweite Markt circa 370 Milliarden US-Dollar. Für 2025 wird dieser auf circa 830 Milliarden US-Dollar geschätzt, was einer Wachstumsrate von jährlich 17,5 Prozent entspräche.

Auf der anderen Seite steht ein Trend, der nicht gegenläufig, aber komplementär zu den Cloud-Lösungen steht, das sogenannte Edge-Computing. Hierbei kann es sich um Edge Devices, wie zum Beispiel Industrie-PCs als auch um leistungsfähige Micro-Rechenzentren wie die AWS Outpost oder die Oncite Edge handeln. Edge-Computing bietet sich an, wenn es um Datenhoheit, Leistungsfähigkeit und Near-Realtime-Prozesse geht, bei denen die Latenzen der klassischen Cloudlösungen zu Problemen führen. Gerade für größere sicherheitstechnische Lösungen mit komplexen Algorithmen und leichten KI-Anwendungen können diese Systeme Lösungen bereitstellen.

Da der deutsche Mittelstand traditionell starke Bedenken hinsichtlich der Sicherheit seiner Daten hat, werden häufig hybride Modelle angestrebt. Zwar bieten inzwischen alle Anbieter Cloud-Rechenzentren auf europäischen Boden an, doch sind immer noch sehr starke Bedenken vorhanden. Gerade sicherheitstechnische Anbieter, die mit äußerst vertraulichen Daten umgehen, sind häufig mit gekapselten Server-Lösungen unterwegs. Um den europäischen Unternehmen den Nutzen Cloud-basierter



Themenpyramide Sicherheitstechnik: Technologische Trends

Grafik: Dr. Wieselhuber & Partner

Systeme auf breiter Front zur Verfügung zu stellen, da sich diese sehr viel besser skalieren und warten lassen, arbeiten Deutschland, Frankreich und weitere Vertreter der EU eine Basis für die nächste Generation einer europäischen Dateninfrastruktur und -kommunikation aus. Im Mittelpunkt steht unter anderem Datensouveränität und Innovation auf höchstem Niveau, was vor allem auch den Bedürfnissen der Sicherheitstechnik

entgegenkommen wird. Es wird spannend für die Sicherheitstechnik, die weiteren Entwicklungen der Initiative zu beobachten.

### Software Suiten auf Micro-Services-Basis

Ein weiterer Grund, weshalb Cloud- beziehungsweise moderne Edge-Lösungen für die Sicherheitstechnik interessant sind, hat mit veränderten Software-Architekturen zu tun. Software Suiten, das heißt ganze Bündel an Funktionen/Anwendungen/Apps lassen sich in einer Cloud-Architektur sehr viel besser verwalten, betreiben und updaten. Hinzu kommt, dass der Trend in Richtung sogenannter Micro-Services geht, die getrennt voneinander sehr flexibel und schnell entwickelt werden können. Sie konzentrieren sich in der Regel auf spezifische Aufgabenstellungen und Funktionen. Software-Architekturen basierend auf Microservices bieten sich vor allem an, um die Bestands-Software schnell und flexibel um neue Funktionen zu erweitern, ohne dass hierbei große Eingriffe in der bestehenden Code-Struktur vorgenommen werden müssen. Diese Entwicklungen aus dem IT-Umfeld werden sich daher auch in den Security-as-a-Service-Angeboten ausbreiten. Denn erst durch den Datentopf-übergreifenden Zugriff kann Mehrwert für die Kunden gewährleistet werden.



IKT-Unternehmen wie Apple, Google und Co. konzentrieren sich immerr mehr auf das hypersichere, voll vernetzte Haus der Zukunft.

### Hyper-Secure Smart Home

Es gibt wenig, worüber man im professionellen Umfeld der Sicherheitstechnik mehr lächelt als über den Begriff Smart Home. Doch der technische Fortschritt bringt es mit sich, dass hierin gerade für die kleineren Unternehmen der Branchen nicht zu unterschätzende Gefahren lauern. Denn die großen, ressourcenstarken IKT-Unternehmen wie Apple, Google und Co. konzentrieren sich mehr und mehr auf das hypersichere, voll vernetzte Haus der Zukunft. Zukünftige hochsichere Devices werden über Apple HomeKit beziehungsweise Google Home mit Fenster- und Türsensoren etc. interagieren. Diese Transformation wird das Angebot von klassischen Sicherheitslösungen zumindest im privaten Umfeld verändern und dadurch gleichzeitig einen viel breiteren Markt für Sicherheitstechnologie schaffen. Negative Folgen könnten jedoch die Infragestellung monatlicher Gebühren der traditionellen Anbieter, die Senkung der Preise für High-tech-Überwachungsgeräte sowie mehr Do-it-Yourself-Implementierungen sein. Auf der anderen Seite liegen hierin auch Chancen für die Errichter: Selbst wenn die Geräte für private Applikationen zukünftig von den großen IKT-Konzernen kommen, wird die Projektierung und die Errichtung von größeren Projekten weiterhin vom Fachbetrieb übernommen werden. Denn: die großen IKT-ler konzentrieren sich ausschließlich auf skalierbares Geschäft. Die Software-Plattformen könnten jedoch zukünftig zu einem nicht unwesentlichen Teil in die Clouds der Hyperscaler beziehungsweise IKT-Riesen wie Google und Co. abwandern.

### Fazit

Die geschilderten Technologietrends werden auf jeden Fall eines zur Folge haben: Die verschiedenen Geschäftsfelder der Branche werden mit zunehmendem Tempo weiter konvergieren. Persönliche Sicherheitsdienstleister sind zunehmend auf IT-Support angewiesen, IoT-Devices und vernetzte Systeme stellen hohe Anforderungen an die Cyber Security, sicherheitstechnische Leitstände sollen zunehmend intelligenter werden und benötigen daher verstärkt IT-Know-how, um KI-fähige Systeme bereit zu stellen und so weiter. Eine Folge dieser Entwicklung wird sein, dass sich die Bran-

370

**MILLIARDEN** US-Dollar beträgt der weltweite Markt für Public- beziehungsweise Hybrid-Clouds momentan. Für 2025 wird dieser auf ungefähr 830 Milliarden US-Dollar geschätzt. Das entspräche einer Wachstumsrate von jährlich 17,5 Prozent.

che weiter konsolidieren wird. Schätzungen gehen davon aus, dass sich bis 2030 die Anzahl der Anbieter in der Branche um bis zu 50 Prozent reduzieren wird. Was für die Unternehmen der Branche aber nicht Marktberreinigung im klassischen Sinne bedeutet, sondern vielmehr das Aufgehen in einem größeren, leistungsfähigeren unternehmerischen Verbund. ■

» **Dr. Wieselhuber & Partner GmbH:**  
[www.wieselhuber.de](http://www.wieselhuber.de)



## SCHILLE Informationssysteme ist das jüngste Mitglied in der PKE-Familie

**Am 15. November 2019 hat die PKE Deutschland GmbH, mit Hauptsitz in München, den Geschäftsbetrieb der Firma Schille Informationssysteme GmbH in Hannover übernommen.**

PKE steht seit über drei Jahrzehnten für erstklassige Lösungen im Bereich Sicherheitstechnik. Mit dem Erwerb der SCHILLE Informationssysteme GmbH baut PKE die Kompetenz im Bereich integrierte und bedienoptimierte Video- bzw. Sicherheitsmanagementsysteme weiter aus. Zur Sicherstellung der hochqualitativen Betreuung des bestehenden Kundenstamms wurde bei PKE das komplette Entwicklungs- und Support- Team der ehemaligen SCHILLE Informationssysteme in Hannover übernommen und in den letzten Wochen das „Schille Competence Center“, kurz „SICC“ genannt, etabliert. Die PKE kann somit die Softwareansprüche der im Feld befindlichen Systeme bedienen – darunter selbstverständlich auch die langjährig als OEM Versionen im Markt von SIEMENS Schweiz und SIEMENS Deutschland unter dem Namen „SINVR“ installierten Videomanagementsysteme, sowie die weiteren OEM Versionen „DiViCro“ von Dekom und „Zelaris“ aus dem Errichter-Geschäft. In den letzten Monaten wurde mit Hochdruck weiterentwickelt, da-

durch sind bei PKE bereits neue Servicereleases verfügbar. Ihr PKE Kundenbetreuer informiert Sie dazu gerne über Details:

» **Kontakt:**  
**Andreas Rohde**  
Leiter Schille Competence Center  
PKE Deutschland GmbH  
Goseriede 4  
30159 Hannover  
T: +49 511 545272 1090  
Mail: [sicc@pke-de.com](mailto:sicc@pke-de.com)

» **Weitere Informationen unter:**  
[www.pke-de.com](http://www.pke-de.com) und  
[www.sivms.cloud](http://www.sivms.cloud)

