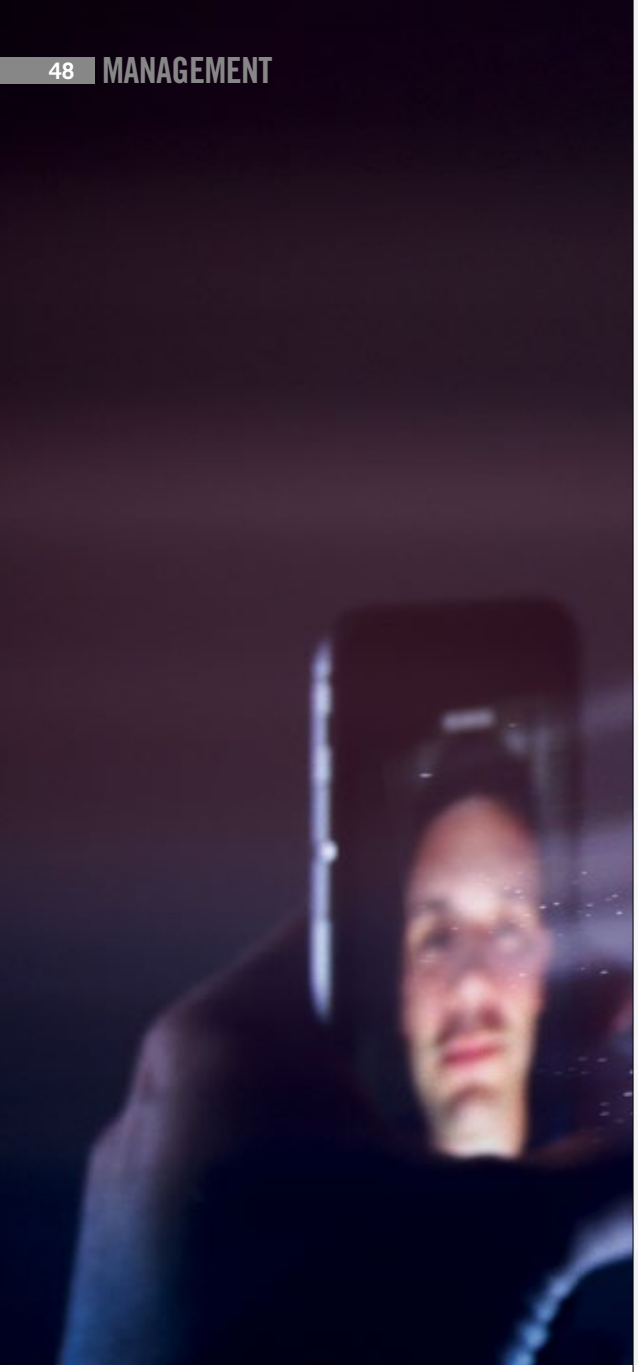


SMART ACCESS

Datenschutz und der Schlüssel von morgen

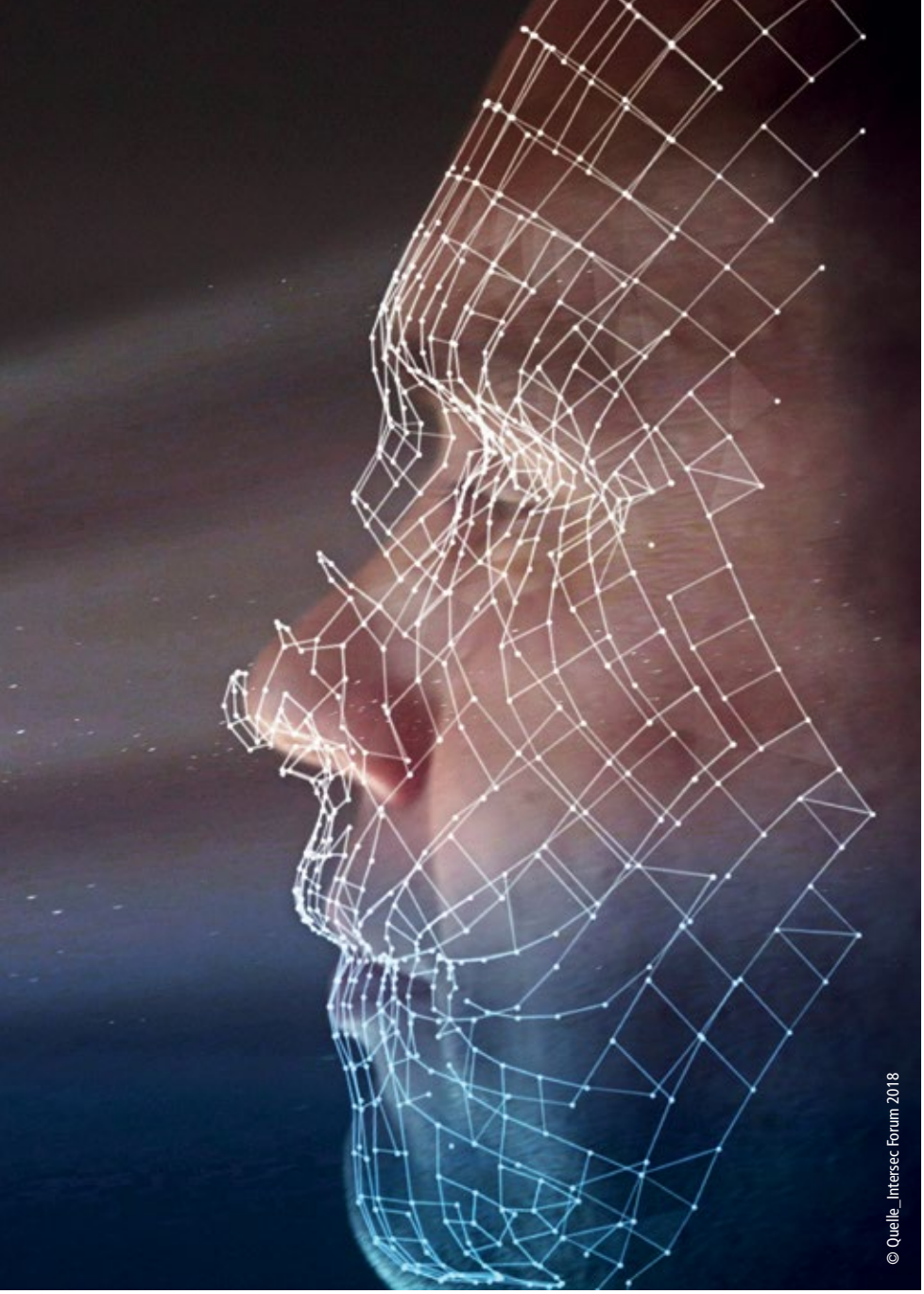
Zukunftsdialog Smart Access auf dem Intersec Forum: „Smart Services und Datenschutz – ändert die neue DSGVO die Spielregeln?“

Sichere und komfortable Zutrittslösungen, die das Internet of Things (IoT) mit der bewährten Welt der Mechatronik verbinden: Darüber diskutierten im „Zukunftsdialog Smart Access“ anlässlich des Intersec Forums im März 2018 Experten aus Wissenschaft und „Technologieschmieden“ – moderiert von Professor Dr.-Ing. Kai-Dietrich Wolf, Leiter des Instituts für Sicherungssysteme der Bergischen Universität Wuppertal. Im Mittelpunkt standen die Innovationen digitaler und IoT-Anwendungen für elektronische Zutrittskontrolle und moderne Schließsysteme unter der Maßgabe von Datensicherheit (Cyber Security) und Datenschutz (Privacy). Und: Die Vereinbarkeit moderner Technologien mit der DSGVO.

intersec
forum
CONFERENCE REVIEW
Artikel zum Intersec Forum 2018

Der Zutritt von morgen heißt „Smart Access Management“. Denn die Verschmelzung elektronischer Komponenten mit mechatronischen Schließsystemen eröffnet ganz neue Horizonte für moderne Zutrittslösungen. So benötigen Gebäudenutzer mit dem Smartphone als „Ausweis“ selbst für unterschiedliche Gebäude keine separaten Chipcards oder Schlüsselanhänger mehr, sondern verwenden zum Öffnen von Türen eine entsprechende App. Ermöglicht wird das durch Übertragungstechnologien wie beispielsweise Near Field Communication (NFC) und Bluetooth Low Energy (BLE).

Die einheitliche Bedienung über das Smartphone beschert den Nutzern einen erheblichen Komfortgewinn und senkt den Verwaltungsaufwand für die Betreiber. Das gilt besonders für Dienste, die mit herkömmlichen Schlüsseln oder Smartcards nur schwer oder mit großem Aufwand umgesetzt werden können. So wird die kurzfristige Vergabe von Berechtigungen auch mit zeitlich begrenzter Gültigkeit in Hotels oder bei der Wartung von Industrieanlagen deutlich erleichtert, ebenso für den temporären Zugang von Liefer-, Reinigungs- und Pflegekräften im Rahmen des Assisted Living im häuslichen Bereich. Neue Möglichkeiten ergeben sich auch beim Zugang zu gemeinsam genutzten Ressourcen, etwa im Car Sharing.



© Quelle_Intersec Forum 2018

Zukunftsdialog mit Experten

So stand denn auch der letzte Tag des Intersec Forum ganz im Zeichen des Zukunftsdialogs Smart Access: Moderiert und gestaltet von Professor Dr.-Ing. Kai-Dietrich Wolf, Leiter des Instituts für Sicherungssysteme der Bergischen Universität Wuppertal, diskutierten Experten die Innovationen digitaler und IoT-Anwendungen für elektronische Zutrittskontrolle und moderne Schließsysteme unter der Maßgabe von Datensicherheit (Cyber Security) und Datenschutz (Privacy). Redner waren Ho Chang, Geschäftsführer des in Nürnberg ansässigen Softwareentwicklers für biometrische Gesichtserkennung BioID, Antoine Huber, Director IoT for Building – Mobile Services & IoT beim internationalen Anbieter digitaler Sicherheitstechnik Gemalto France, Karsten Nölling, Vorsitzender der Geschäftsführung beim digitalen Schließsystem-Entwickler Kiwi. KI GmbH, Dr. Christian Zenger, Geschäftsführer des Start-ups Physec. Jürgen Schneider, Prokurist nedap Technology partner nTp for Security Management GmbH sowie Prof. Dr.-Ing. Tibor Jager, Universität Paderborn. Die Keynote mit dem Titel „Aus Access Control wird Smart Access Management" wurde von Christoph Zwahlen, Global Marketing Manager von NXP Semiconductors, gehalten.

In der abschließenden Podiumsdiskussion beschäftigten sich Ann-Kathrin Schmitt, BioID, Dr. Thomas Engelke, Verbraucherzentrale-Bundesverband, Thomas Kahl, Fachanwalt bei Taylor Wessing, und Karsten Nölling von Kiwi. KI mit der aktuellen Frage: „Smart Services und Datenschutz – ändert die neue DSGVO die Spielregeln?" Die wesentlichen Aussagen und Statements der Fachleute stellen wir Ihnen hier vor.

Bitte umblättern ►

Diskutanten Thomas Kahl (l.) von Taylor Wessing und Karsten Nölling (Mitte) von Kiwi.Ki

Moderierte eine spannende Diskussion: Prof. Dr.-Ing. Kai-Dietrich Wolf vom Institut für Sicherungssysteme, Bergische Universität Wuppertal

Thomas Kahl, Fachanwalt für IT-Recht, Kanzlei Taylor Wessing: Die Datenschutzgrundverordnung (DSGVO) ist ein extrem umfassendes Gesamtwerk. Mit Inkrafttreten der neuen Verordnung erhält die „Datenschutz-Awareness" einen großen Stellenwert, und zwar in dreierlei Hinsicht: Kunden werden sich als „Betroffene" in steigender Anzahl mit Auskunftsansprüchen an Unternehmen wenden, Unternehmenskunden werden einen höheren Auskunftsbedarf gegenüber ihren Dienstleistern geltend machen und letztlich müssen auch öffentliche Stellen – sprich Behörden – die neuen Regularien umsetzen.

> „Vertrauen in die Einhaltung datenschutzrechtlicher Standards ist bei den Endverbrauchern nicht ausreichend vorhanden."

Die behördlichen Stellen, die für die Datenschutzaufsicht zuständig sind, wählen zwar erfahrungsgemäß eher große Unternehmen für eine Überprüfung der Einhaltung der gesetzlichen Vorgaben zum Datenschutz aus. Die DSGVO sieht aber grundsätzlich keine Ausnahmen nach Unternehmensgröße für die Sanktionierungen bei Nichteinhaltung der Regularien vor. So geraten nun auch kleinere Unternehmen mit in den Fokus der Behörden. Hier drohen neben Anordnungen ggf. hohe Bußgelder. In Deutschland ist hier noch vieles im Fluss, während andere EU-Länder wie z.B. Frankreich hier schon deutlich sichtbare Zeichen setzen, was die Absicht der Sanktionierung von Verstößen betrifft.

Ein weiterer wichtiger Aspekt sind aus Sicht der Aufsichtsbehörden die mit der neuen DSGVO eingeführten Dokumentationspflichten. Diese erfordern u.a. die Erstellung und die Pflege von Verfahrensverzeichnissen, in denen die datenschutzrelevanten Prozesse des Unternehmens darzustellen sind und deren Erstellung oftmals sehr umfangreich, ressourcen- und kostenintensiv sein wird. Viele Unternehmen haben ihre Prozesse noch nicht ausreichend dokumentiert, so dass hier noch viel Nachholarbeit zu leisten ist. Unternehmensintern bedarf es zudem der stärkeren „Awareness" der Mitarbeiter, um der Bedeutung dieser neuen Vorgaben auch gerecht zu werden.

Ein weiterer wichtiger Punkt ist das Thema Privacy by Design, wonach schon bei der Entwicklung eines Produkts datenschutzrechtliche Aspekte einbezogen werden müssen. Dies erfordert einerseits die Implementierung und Dokumentation entsprechend transparenter Prozesse. Aber auch das Thema Datenportabilität wird eine größere Rolle spielen. Dies gilt insbesondere für große Unternehmen, die einschlägige Kundendaten verarbeiten. Hintergrund ist, dass betroffene Kunden ihre Daten zukünftig ggf. zu einem neuen Provider bzw. Anbieter „umziehen" können. So werden zukünftig zwischen den betroffenen Unternehmen Datenflüsse entstehen, die Unternehmen vor große technische Herausforderungen stellen werden. Insoweit dürfte die baldige Etablierung neuer Standards wichtig werden.

Dr. Thomas Engelke, Leiter Team Energie und Bauen, Verbraucherzentrale Bundesverband: Aus Sicht der Endverbraucher und Nutzer stellt sich die Frage, wie wir von der zunehmenden Digitalisierung und Nutzung erhobener persönlicher Daten betroffen sind. Ein wichtiger Aspekt ist das Thema Vertrauen in die Einhaltung datenschutzrechtlicher Standards. Dieses Vertrauen ist bei den Nutzern und Endverbrauchern nicht ausreichend vorhanden. Es bedarf besserer Standards, die rechtlich abgesichert sind. Das würde auch einen ökonomischen Vorteil für den Wirtschaftsstandort Deutschland darstellen. Am Beispiel Energiewende lässt sich klar zeigen, dass ohne erfolgte Digitalisierung der Status quo nicht hätte erreicht werden können. Grund dafür ist die in den letzten zwanzig Jahren massiv gestiegene Anzahl von Energieerzeugern in Deutschland im Bereich der regenerativen Energien, insbesondere auch im Bereich der Prosumenten (Anm. d. Red.: Verbraucher mit professionelleren Ansprüche an ein Produkt als ein durchschnittlicher Endverbraucher), die zu

Im Gespräch mit Moderator Prof. Kai-Dietrich Wolf (l.): Ann-Kathrin Schmitt, BioID GmbH Nürnberg und Dr. Thomas Engelke von der Verbraucherzentrale Bundesverband e.V. (VZBV)

mehr Wettbewerb im Strommarkt geführt hat. Für die in nächster Zeit auslaufenden Verträge müssen neue Geschäftsmodelle gefunden werden, um das vorhandene Energieangebot sinnvoll zu vermarkten. Um „private" von „geschäftlichen" Daten zu trennen, bedarf es neuer und sicherer Standards bzw. einer klaren Datentrennung.

Bei Smart-Home-Anwendungen müssen Fragen der Produkthaftung und des Vertragsrechts gelöst werden. Zum Beispiel müssen Geräte-Updates für sicherheitsrelevante Software über die verpflichtende Gewährleistungsdauer hinaus für die gesamte Produktlebensdauer verfügbar sein. Die Information über diese begleitend zur Verfügung zu stellende Software sollte den Verbrauchern zugänglich gemacht werden.

Wichtig ist aber dabei, dass dem Verbraucher eine Wahlfreiheit eingeräumt wird. Geräte müssen sowohl „analog" als auch im Verbund mit smarten Lösungen betrieben werden können.

Die neue DSGVO ist aus Verbrauchersicht zu begrüßen. Essentieller Punkt ist das darin enthaltene Kopplungsverbot sowie die Einbettung in EU-Recht. Das bedeutet, dass auch Unternehmen, die ihren Sitz nicht in Deutschland und der EU haben, wirtschaftlich aber in diesem Raum aktiv sind, ebenfalls den Regularien der DSGVO unterliegen. Durch das Kopplungsverbot darf ein Vertrag oder ein Dienstangebot nicht mehr an die Einwilligung in Verarbeitungen der Daten gekoppelt werden, die für die Erfüllung des Vertrags nicht notwendig sind.

Ann-Kathrin Schmitt, Marketingleiterin BioID GmbH: Die Einführung der DSGVO ist für Unternehmen wie BioID als Biometrie-Anbieter eine Herausforderung - aber vor allem eine Chance. Datenschutz und Datensicherheit sind schon immer die Grundprinzipien, auf denen die Gesichtserkennung von BioID aufbaut. Die Erhebung und Speicherung personenbezogener Daten findet auch jetzt schon datensparsam und pseudoanonymisiert statt. Ziel ist es, Personen durch ihre expliziten Merkmale zu erkennen und ihnen so Zugang zu Gebäuden oder Konten zu gewähren. Dafür brauchen wir als Serviceanbieter aber neben den biometrischen Merkmalen keine Daten der Person.

Datenschutz impliziert die Option der selbstbestimmten Datenfreigabe und Verwendung. Biometrische Anwendungen können diesen Aspekt unterstützen: Eine Freigabe der Datennutzung ist über die biometrische Authentifizierung klar nachvollziehbar; das Verfahren ist sicher und zuverlässig. Der Fingerabdruck oder die Gesichtserkennung mit Lebenderkennung dient als Authentifizierung, bei der die Anwesenheit des Nutzers sichergestellt ist. Man braucht kein Passwort oder Token etwa in Form eines Transponders mehr. Das macht es für den Nutzer besonders einfach.

Biometrische Schlüssel können nicht weitergegeben, gestohlen oder vergessen wer-

Bitte umblättern ▶

den, was ein starkes Sicherheitsmerkmal ist. Je nach Anwendung können aber zusätzliche Personen in bestehende biometrische Authentifizierungen eingelernt, also aufgenommen werden, so dass Berechtigungen zum Öffnen von Türen oder ähnlichem durch den Besitzer bzw. den Erstnutzer vergeben werden können. Denkbar sind auch Lösungen, die eine Benachrichtigung per App einschließen, dass eine Person vor der Haustür steht und Zugang zum Haus haben möchte. Per Gesichtserkennung kann diesem Wunsch bei Bedarf dann stattgegeben werden.

Karsten Nölling, Geschäftsführer Kiwi.KI GmbH: Die Entwicklung und Einführung einer Plattform zur digitalen Bewirtschaftung großer Wohneinheiten ist der Grundgedanke der Geschäftsidee von Kiwi.KI. Sicherheitslücken, die durch die Anwendung physischer Schlüssel entstehen können, sollen so der Vergangenheit angehören. Basis der Anwendungen sind entweder ein RFID-basierter Transponder oder eine App-basierte Lösung; die Zugriffsrechte werden an reale physische Personen vergeben. Gleichzeitig besteht die Möglichkeit, per Mail eine Zutrittsberechtigung an eine Person zu übertragen, die diese dann entsprechend nutzen kann. Auch biometrische Gesichtserkennung könnte diese Anwendung ergänzen. Fazit ist aber, dass der Kunde entscheidet, in welcher Form und in welchem Umfang die Plattform zu nutzen ist.

Kiwi.KI vertritt das Prinzip, generell keinerlei personenbezogene Daten von Mietern zu erheben. Insbesondere aufgrund der Tatsache, dass große Kunden betreut werden, die auch über entsprechende Betriebsratspräsenz verfügen, ist dies geboten. Fragwürdige sogenannte „Tracking-Funktionen" sind nicht aktivierbar. Wir sind der Auffassung, dass diese Art der Datennutzung nicht zu unserem Unternehmen passt.

In speziellen Fällen, beispielsweise bei Nutzung durch Dienstleister, ist die Nachverfolgbarkeit von Ereignissen wiederum sinnvoll. Der Kiwi Safe wird mittels Kiwi App geöffnet und verschlossen, wobei diese Aktivierungen festgehalten werden können. Es wird demnach möglich sein, Daten der Zugangskontrolle zu dokumentieren, ohne die Datenschutzrichtlinien zu verletzen. Mieter bleiben natürlich weiterhin anonym.

Prof. Dr.-Ing. Kai-Dietrich Wolf, Institut für Sicherungssysteme, Bergische Universität Wuppertal: Alle Unternehmen, mit denen ich spreche, haben sich intensiv auf das Inkrafttreten der DSGVO vorbereitet. Neue Dokumentationspflichten bringen dabei deutlich spürbare Belastungen mit sich; auch Sorgen angesichts der drakonischen Strafen wurden geäußert. In puncto Awareness sind diese Unternehmen

Ann-Kathrin Schmitt (BioID) und Dr. Thomas Engelke (VZBV)

auf dem richtigen Weg. Die Prinzipien ‚Privacy by Design' und z. B. das Kopplungsverbot in die Prozesse der Produktentwicklung einzubauen, wird aus meiner Sicht insbesondere Schließsystemherstellern nicht schwerfallen, da die Datenerhebung noch nie im Vordergrund stand. Wir haben in der Diskussion gesehen, dass Unternehmen wie Kiwi.KI oder BioID mit ihren Geschäftsmodellen von der neuen Gesetzgebung profitieren könnten.

Ich meine, es ist Zeit für große sowie kleine Unternehmen, sich Gedanken über eine einvernehmliche, nutzerzentrierte Erhebung von Daten zu machen und sich von der Goldgräberstimmung des Big-Data-Hypes zu verabschieden. Meine Vision von einer gemeinsamen Plattform zur sicheren Datenverarbeitung, an die insbesondere kleine Unternehmen andocken können, wurde nicht durchgängig zustimmend geteilt, auch darüber sprachen wir auf dem Podium. Von allen Teilnehmern befürwortet wurden Bemühungen zur Schaffung gemeinsamer sicherer und DSGVO-konformer Standards; damit sollten sich die Branchenunternehmen beschäftigen. Dies könnte Kompatibilitäten der Produkte befördern sowie Kooperationen erleichtern und nicht zuletzt auch die Position kleinerer Unternehmen gegenüber großen Akteuren stärken.

Fazit: Authentifizierung ist „Key"

Die Nutzung einer vertrauenswürdigen Identität und eine einheitliche Bedienung für die verschiedensten Dienste erhöht auch die Nutzerakzeptanz eines vernetzten Gebäudes. Nach der Studie eines britischen Marktforschungsunternehmens in mehr als 50 Ländern wollen 85 Prozent der Befragten eine Identität für mehrere Systeme und Dienste verwenden. Z.B. meinen 60 Prozent der Teilnehmer, dass die Benutzung eines mobilen Gerätes die betriebliche Effizienz deutlich steigert.

Eine Voraussetzung bei der Einführung von vernetzten Smart-Access-Technologien ist allerdings nach Meinung der Experten ein optimaler Schutz vor Missbrauch von Nutzerdaten und Cyber-Angriffen im Hinblick auf Datensicherheit und Datenschutz. Hierzu wird intensiv an sicheren Verschlüsselungstechnologien und „Secure End-to-End Solutions" gearbeitet, aber auch an der Auswertung biometrischer Daten, ohne auf die Person des Trägers zurückschließen zu können. Entscheidend ist ebenso die Speicherung sensibler Daten in einem besonders geschützten Bereich. Letztendlich handelt es sich hier um Komfortlösungen, die bei intelligenter und sicherer Implementierung durchaus das Potential haben, zur Verbesserung der Sicherheit beizutragen. „Intelligente" – smarte – Häuser könnten z. B. auf unterschiedliche Sicherheitsanforderungen, die durch Ereignisse wie Feuer oder bei Einbruch manifest werden, mit adäquaten Maßnahmen reagieren. Die zunehmende Vernetzung erlaubt die intelligente Nutzung von immer mehr Informationen. Das größte Hemmnis dieser Entwicklung sind derzeit wohl im Wesentlichen Software-basierte Inkompatibilitäten, die von einigen Herstellern durchaus gewollt sind. Manche der großen Akteure scheinen zu glauben, dass sie von den Entwicklungen am besten im Alleingang profitieren können; dabei steht vermutlich der exklusive Zugang zu Nutzerdaten im Fokus.

Weitere Technologien werden kommen – und das Thema bleibt spannend. Sowohl hier im Fachmagazin GIT SICHERHEIT – und bestimmt auch wieder beim nächsten Intersec Forum in Frankfurt.. ■

Kontakt

Institut für Sicherungssysteme
Velbert; Bergische Universität Wuppertal
Univ.-Prof. Dr.-Ing. Kai-Dietrich Wolf
Tel.: +49 2051 93322 15
wolf@iss.uni-wuppertal.de,
www.iss.uni-wuppertal.de