



Teilnehmer des ersten Tages des PROTECTOR Forums Zutrittskontrolle (von links): Herausgeber Lothar Zobel, Jürgen Schneider, Sven Däberitz, Hartmut Beckmann, Volker Kraiss, Kester Peter Brands, Dietmar Vetten, Jürgen Alz, Robert Karolus, Polichronis Sidiropoulos, Wilfried Joswig, Rainer K. Füess, Boris Stamm, Michael Wanka, Michael Wienke, Chefredakteur Bernhard Frey, Christoph Tegelkamp.

Bilder: MG

Vernetzt und mobil: zwischen smart und sicherheitsrelevant

Alles, immer und von überall?

Dank intelligenter und ständig vernetzter Kommunikationsgeräte sind auch komplexe technische Systeme heute portabler und flexibler denn je. In der Zutrittskontrolle bringt dies Vorteile, kann jedoch auch Risiken schaffen.

Zu Beginn des diesjährigen Forums Zutrittskontrolle steht zunächst einmal eine Bestandsaufnahme in Sachen Mobilität und Apps an. Moderator Boris Stamm fühlt den Teilnehmern auf den Zahn: „Wie ist der aktuelle Stand hinsichtlich mobiler Zutrittskontrolle? Lohnt es sich, Lösungen für Smartphones und Tablets anzubieten? Oder werden solche Apps sogar schon vorausgesetzt und von Anwenderseite eingefordert?“

Rainer Füess von Tisoware stimmt zu, dass dies ein Trend ist: „Das Thema Mobile Computing ist in aller Munde, und bezogen auf unser Angebot ist es so, dass wir bereits mobile Lösungen im Sicherheitsbereich anbieten, genauso auch für Human Resources und den Industriebereich. Es ist festzustellen, dass diese im Mittelstand tatsächlich noch weniger nachgefragt werden, wobei es auch hier einige Anwendungsbeispiele gibt, bei denen sie sehr nützlich sind

– zum Beispiel Alarmmeldungen oder Live-Bilder für den Manager unterwegs. Das sind Dinge, die in der Praxis bereits genutzt werden. Dennoch entwickeln wir unsere Anwendungen im mobilen Bereich stets weiter, um dem Trend gerecht zu werden.“

Vielseitig nutzbar

Jürgen Alz von Bosch Sicherheitssysteme sieht gleich zwei Anwendungsfelder für mobile Apps: „Wir nutzen das Mobile Computing in zweierlei Hinsicht: Wir bieten es einerseits für den Servicebereich an, um damit Projektierung und andere Service-Aufgaben zu erleichtern. Andererseits bieten wir Anwendern darüber auch zahlreiche Funktionen des Alarm-Managements an. Die sind heute schon in Form einer App für unseren Kunden verfügbar und werden von diesen genutzt.“

Sven Däberitz von Intrakey bestätigt den Trend ebenfalls: „Wir haben seit einem Jahr Apps für Zeiterfassung, Zutritt und den Fuhrparksektor. Hier gibt es ein sehr differenziertes Bild der Nachfrage. Manche interessieren sich kaum dafür, andere setzen das als selbstverständlich voraus, letztere sind meistens kleine, innovative Mittelständler, die solche Apps verlangen.“

Und Michael Wienke von Honeywell ergänzt: „Wir bieten unseren Kunden heute ebenfalls die Möglichkeit, die Sicherheitssysteme auf dem Tablet, beziehungsweise mit einer App, zu verwalten. Das hängt auch mit einem weiteren Bereich zusammen, bei dem ich Chancen und auch konkrete Nachfragen sehe. Das betrifft den Ansatz, komplette Datenbanken in die Cloud auszulagern. Das sorgt für weitere Flexibilität und schafft die Möglichkeit, die Daten dort auch von einem Dienstleister verwalten zu lassen.“

Nutzen differenzieren

Dass alle diese Anwendungen Potenzial haben, glaubt Hartmut Beckmann von Uhlmann und Zacher: „Für den Anwender



„Man muss nur zehn Jahre zurückschauen, damals haben die mobilen Anwendungen schon langsam in die Zeitwirtschaft Einzug gehalten. Das hat Urlaubsanträge und Zeitkorrekturen vereinfacht und ist mittlerweile Standard in diesem Umfeld. In der Sicherheitstechnik braucht es wohl auch deshalb noch etwas länger, um sich durchzusetzen, weil man immer auch an die Sicherheit der Systeme denken muss. Aber ich denke, auch das wird man in den nächsten Jahren lösen, so dass die Verbreitung steigt.“
Robert Karolus, Produktmanager Interflex Datensysteme GmbH & Co. KG

„Ich habe auch das Gefühl, dass wenn wir uns den Sektor Sicherheit anschauen, viele noch recht konservativ eingestellt sind. Es geht nicht nur um Geräte und smarte Applikationen, sondern auch darum, dass die Menschen und die Unternehmen mitziehen müssen. Ich denke, dass sich die Technik schneller weiterentwickelt, als wir in der Lage sind, es organisatorisch abzubilden.“

Wilfried Joswig, Geschäftsführer, VfS – Verband für Sicherheitstechnik e.V.



bringt das deutliche Vorteile, vor allem hinsichtlich der Zeitersparnis. Der Anspruch hat sich in den letzten Jahren massiv geändert: Es geht in der praktischen Anwendung von Sicherheitssystemen immer darum, möglichst schnell Informationen zu bekommen, um angemessen entscheiden zu können. Das findet auch in der Sicherheitsbranche immer stärker auf Basis mobiler Lösungen statt.“

Damit wird bereits deutlich, dass sowohl das Bild der Nachfrage auf Kundenseite, als auch die Nutzungsszenarien von mobilen Zutrittskontroll-Apps differenziert zu betrachten sind. Volker Kraiss von Kraiss Consult versucht, dies zu veranschaulichen: „Bezogen auf die Sicherheitstechnik und auf die Zutrittskontrolle sind die Möglichkeiten relativ klar einzugrenzen. Die eine Möglichkeit ist das Informationsmanagement, bei dem aus dem System heraus Informationen und Alarmer auf mobile Geräte gesendet werden. Die zweite Möglichkeit ist die Pflege und Datenaktualisierung, bei der Anwender von mobilen Geräten aus Daten in die Systeme eingeben oder anpassen können. Darüber hinaus können Systemlieferanten im Bereich

Ich sage dir, wer du bist.



Im kabellosen Zutrittssystem eAccess von Glutz identifizieren die Beschläge zutrittsberechtigte Personen auf Anhieb. Und lassen diese freundlich eintreten. Eine Annäherung mit einem Clip oder einer Card genügt – und schon entriegelt sich das Schloss automatisch. Einfach, komfortabel und sicher. Entdecken Sie die Zukunft des Zutritts!
www.glutz.com

Glutz

since 1863



„Ich bin der Meinung, dass die Welten immer mehr verschmelzen werden – der mobile Teil mit dem der klassischen Anwendung. Wir haben deshalb schon eine Lösung entwickelt, die auf allen Endgeräten die gleiche Oberfläche hat, am PC, am Tablet und am Smartphone. Mit einem solchen responsive Design

hat der Anwender nur noch eine Oberfläche, in der er sich immer sofort zurecht finden. In Zukunft wird hier kaum noch eine klassische Trennung stattfinden, weil es um die Funktion geht und nicht um das Gerät, auf der man sie zur Verfügung stellt.“

Rainer K. Füess, Prokurist – Leiter Partnervertrieb und Marketing, Tisoware GmbH

„Wenn die Applikationen generalisiert werden, so dass man sie auf verschiedenen Geräten nutzen kann, muss man sich dennoch Gedanken machen, wie hat man den Zugang zu den jeweiligen Geräten sichert. Dabei spielt es keine Rolle, ob es nun ein PC oder ein Tablet ist, die Unternehmen müssen sich Maßnahmen überlegen, wie man auch mobile Technik sicher nutzt. Dazu fehlt es momentan aber auch etwas an den nötigen Investitionen in die Infrastruktur.“

Michael Wanka, Regional Sales Manager D-A-CH Region, HID Global GmbH



„Die Kunden, die uns eine Fernwartung erlauben, haben sich nicht nur um die Sicherheitsvorkehrungen Gedanken gemacht, sie haben auch das Vertrauen zu uns, dass wir sorgsam mit den Daten umgehen. Andererseits gibt es natürlich Kunden, die sehr konservativ sind oder ein sehr hohes Schutzbedürfnis haben, die erlauben einen Fernzugriff über das Internet schlichtweg überhaupt nicht.“

Sven Däberitz, Geschäftsführer, Intrakey Technologies GmbH

Service und Fernwartung von mobilen Geräten aus, egal wo man sich gerade befindet, in ein System einloggen, Service betreiben und in gewissem Umfang auch reparieren. Kürzere Wiederherstellungszeiten des Sollzustands sind die Folge beziehungsweise der Nutzen.“

Wartung aus der Ferne

Gerade der letzte Punkt birgt gleich doppelt Potenzial: nämlich für Anwender und Errichter. Jürgen Schneider von Nedap Technology Partner erklärt: „Die Vorteile des Fernservices und des Supports über das Netz sind nicht von der Hand zu weisen – vorausgesetzt, dass es für den Kunden ausreichend sicher umgesetzt wird, etwa über VPN-Zugänge. Dann bringt es für beide Seiten Vorteile. Derjenige, der den Service erbringen muss, kann schneller arbeiten und auch direkter eingreifen. Und demjenigen, der den



Service benötigt, wird schneller geholfen. Man muss auch realistisch sein, denn Reaktionszeiten von unter vier Stunden kann man sonst kaum bezahlbar einhalten. Somit ist die Fernwartung als Bestandteil der mobilen Welt durchaus etwas, wo Potenzial und auch Interesse vorhanden ist.“

Hier ergeben sich weitere Vorteile, wie Sven Däberitz anmerkt: „Wenn es um die Diskussion geht, ob man – auch aus Sicherheitsgründen – eine Fernwartung zulässt, sollte man auch die Kostenseite betrachten. Denn es macht schon einen großen Unterschied, ob man immer einen teuren Techniker vor Ort einsetzen muss oder ob dieser einfach eine Stunde online an dem Problem arbeitet, was wesentlich effizienter und günstiger zu haben ist.“

Rainer Füess ergänzt: „Es betrifft einerseits die Kosten, aber auch den Faktor Zeit. Man muss immer sehen, ob denn ein Techniker gerade verfügbar ist. Die Online-Sitzung könnte er vielleicht schnell einschieben, wohingegen eine lange Anfahrt eventuell nicht sofort eingeplant werden kann. Das Problem ist also meist online schneller gelöst, als wenn Servicepersonal erst zum Kunden fahren muss.“

Cui bono, App?

Trotz dieser einerseits nachvollziehbaren Vorzüge vernetzter und mobiler Systeme gibt es auch fragwürdige Ansätze und Ideen, wie Moderator Boris Stamm anmerkt: „Für mich stellt sich immer wieder die Frage, für welche Anwender die mobile Welt wirklich einen entscheidenden Mehrwert bietet. Schließlich ist nicht alles, was technisch möglich ist, auch praktisch sinnvoll. Nehmen wir einmal den Administrator, der auch noch wenn er im Urlaub unter Palmen liegt das System administrieren soll. Wie sieht es mit der Nachfrage aus?“

Auch wenn dies ein wenig überzeichnet sein mag, so ist es Ausdruck einer gewissen

Unsicherheit aufseiten der Anwender, wie mit den Möglichkeiten der mobilen Welt umgegangen werden soll und was sinnvoll und sicher eingesetzt werden kann. Dietmar Veten von GST möchte das Thema praxisnah skizzieren: „Wir konnten in den letzten einhalb Jahren feststellen, dass die Nachfrage nach mobiler Information steigt. Es geht gar nicht darum, aus dem Karibikurlaub heraus die Zutrittskontrolle zu administrieren, es geht um den Einsatz übergeordnete Systeme, die in der Lage sind, Informationen mobil weiterzugeben. Solche Nachfragen haben wir zum Beispiel verstärkt aus Krankenhäusern. Die Verantwortlichen sind ständig mobil im Haus unterwegs und haben gleichzeitig immer weniger Personal. Sie müssen also bestimmte Meldungen stets sofort mobil geliefert bekommen und entsprechend handeln können. Auch große Konzerne, die nicht unbedingt immer jemanden an einem bestimmten Platz sitzen haben, profitieren, wenn die Mitarbeiter das System quasi immer unter'm Arm dabei haben.“

Hier sieht auch Volker Kraiss deutliche Anwendungsvorteile: „Das ist für größere Unternehmen interessant, vor allem wenn wir in Richtung Berechtigungsmanagement und User-Selfservice in einem standortübergreifenden System denken. Man meldet sich mobil selbst an und möchte ein Zutrittsrecht beantragen, welches dann über das Ausweis- und Berechtigungsmanagement vergeben werden kann. Hier spielt es im Endeffekt keine Rolle, ob man als Antragsteller an einem Arbeitsplatz sitzt, oder ob man ein mobiles Gerät nutzt. Wenn man sich Web-basiert einloggt, kann man dies von jedem Smartphone aus machen.“

Dabei gilt es aber auch zu bedenken, wie man die Vertrauenswürdigkeit von Apps einschätzt, merkt Wilfried Joswig vom Verband für Sicherheitstechnik (VfS) an: „Eine Ebene, die man dabei sicherheitstechnisch betrachten muss, ist: Woher stammen die Apps, die dann jeder runterladen soll? Man



muss auch prüfen, ob dort im Hintergrund noch etwas anderes passiert, etwa heimlich Daten abgegriffen werden. Man muss in jedem Fall sicherstellen, dass man die richtige App zur richtigen Anwendung bekommt.“

Genau abwägen

Bei aller Euphorie bezüglich smarter Technik und ständiger Vernetzung, darf man also Sicherheitsbedenken und andere Hinderungsgründe nicht außer Acht lassen. Häufig lässt sich deshalb noch nicht das ganze Potenzial mobiler Systeme abzurufen. Wilfried Joswig erläutert seine persönliche

Sicht: „Ich bin absoluter Fan von neuer Technik, aber ich habe auch das Gefühl, dass wenn wir uns den Sektor Sicherheit anschauen, viele noch recht konservativ eingestellt sind. Es geht nicht nur um Geräte und smarte Applikationen, sondern auch darum, dass die Menschen und die Unternehmen mitziehen müssen. Ich denke, dass sich die Technik schneller weiterentwickelt, als wir in der Lage sind, es organisatorisch abzubilden. Die technischen Möglichkeiten, die heute vorhanden sind, werden teilweise gar nicht genutzt, weil das Verständnis oder das Wissen um die Möglich-

keiten fehlt. Technische Entwicklung und Qualifizierung der Menschen und der Organisationen müssten enger aufeinander abgestimmt werden.“

Dem pflichtet auch Polichronis Sidiropoulos von Assa Abloy bei: „Ich würde sagen, dass es sich beim Mobile Computing im Bereich der Sicherheitstechnik noch um einen schleichenden Prozess handelt. Einzelne Funktionalitäten sind zwar bereits vorhanden, da sie von Seiten der Anwender gefordert werden, doch nun gilt es, hieraus klare ‚Workflows‘ für die Handhabung zu definieren, um die Brücke zwischen



Xesar und AirKey

Ob mit der mobilen NFC-Sicherheitslösung AirKey oder dem standortbasierten Zutrittskontrollsystem Xesar – EVVA setzt neue Maßstäbe.

**Werden Sie EVVA-Elektronik-Partner –
Kommen Sie zur Schulung.**

Aktuelle Schulungstermine in Ihrer Nähe unter
www.evva.de/anmeldung

www.evva.com

Sicherheit und Komfort zu schlagen. Es steht jedoch außer Frage, dass auch die Sicherheitstechnik immer mobiler wird.“

Aber es gibt noch andere Hinderungsgründe, wie Kester Brands von Tyco zu bedenken gibt: „Meist ist es so, dass je größer ein Unternehmen wird, umso größer auch die Hemmschwellen werden, mobile Geräte einzusetzen. Hierzulande wagt kaum einer den Schritt, sie aktiv im Bereich der Zutrittskontrolle einzusetzen. Oder wenn man sich dagegen England oder die USA ansieht, dort ist Zutritt on Demand gefordert. Man hat nur noch einen Controller vor Ort und eine mobil verfügbare App, um die Zutrittskontrolle zu verwalten. Davon sind wir noch relativ weit weg, was vielleicht auch an der konservativen Struktur in Deutschland beziehungsweise im deutschsprachigen Raum liegt.“

Auch Sven Däberitz erlebt teilweise Bedenken bei Kunden: „Bei Konzernen oder im größeren Mittelstand stößt mobile Zutrittskontrolle meist auf Ablehnung – einerseits aus Sicherheitsgründen, andererseits weil das Verständnis fehlt. Bei der Zutrittskontrolle ist es so, dass die Nachfrage ganz klar nur in Richtung Kontrollfunktion und Alarmmeldung geht. Es gibt kaum Kunden, die die Türen wirklich per App öffnen wollen, weil dort oft ein Sicherheitsproblem gesehen wird.“

IP bis zum Ende

Auch technisch ist noch nicht alles ausgeschöpft und bis zum Ende hin vernetzt, wie Kester Brands ergänzt: „Erstaunlich ist, dass wir zwar über mobile Welten und smarte Geräte sprechen, aber mit den Zutrittssystemen in den allerwenigsten Fällen bis an die Tür per IP vernetzt sind. Wir benutzen zwar die IT-Welt bis zu einem gewissen Punkt, nämlich vom Rechner bis zum Controller, aber bis zum Leser an der Tür reicht die IP-Technik nur in Ausnahmen. Ganz anders ist es in der Videotechnik, dort geht der IP-Anschluss bis an die Kamera. Auch die Intercom hängt heute an der Außenfassade und ist IP-gestützt. Nur die Zutrittsleser sind in der Regel noch proprietär angebunden. Dabei könnte man, wenn man diese Geräte auch IP-fähig machen würde, viel mehr Funktionalität an der Tür bereitstellen und auch den Support aus der Ferne wesentlich tiefer ins System bringen.“

Für Michael Wanka von HID wäre ein solches Unterfangen keine unlösbare Aufgabe, es müsse aber genau abgewogen werden: „Diese Frage stellt sich zunächst ein-



„Ich würde den Trend zu mobilen Anwendungen nicht davon abhängig machen, ob es sich nun um große, kleine oder mittelgroße Firmen handelt. Es hat viel mehr mit der Firmenphilosophie zu tun. Wir haben schon vor zehn Jahren mobile Lösungen bei amerikanischen Unternehmen umgesetzt, für die es absolut zweitrangig war, ob das System in Frankfurt oder in Hamburg administriert wurde. Es gibt aber gerade hierzulande wesentlich konservativere Ansichten bei Firmen, die sagen: Um Gottes Willen, kein Tablet in meinem Haus. Oft auch mit der Sicherheit als Begründung, obwohl es eigentlich eher Unwissenheit ist, die den Einsatz verhindert.“
Dietmar Vetten, Vertrieb, GST Gesellschaft für Sicherheitstechnik mbH

„Ich denke, für Sicherheitsverantwortliche ist der Zugriff über das Internet ein zweischneidiges Schwert. Sie dürften natürlich froh sein, wenn sie per Fernwartung eine schnelle Störfallbehebung bekommen, aber die Gefahr, die sie immer dahinter vermuten, ist, dass womöglich auch der Falsche bis in die Tiefe in das System hinein zugreifen kann. Hier muss man Vorkehrungen treffen und das auch kommunizieren, um solche Anwendungen sicher zu machen.“
Boris Stamm, Moderator des Forums Zutrittskontrolle



„Meist ist es so, dass je größer ein Unternehmen wird, umso größer auch die Hemmschwellen werden, mobile Geräte einzusetzen. Hierzulande wagt kaum einer den Schritt, sie aktiv im Bereich der Zutrittskontrolle einzusetzen. Oder wenn man sich dagegen England oder die USA ansieht, dort ist Zutritt on Demand gefordert. Man hat nur noch einen Controller vor Ort und eine mobil verfügbare App, um die Zutrittskontrolle zu verwalten. Davon sind wir noch relativ weit weg, was vielleicht auch an der konservativen Struktur in Deutschland beziehungsweise im deutschsprachigen Raum liegt.“
Kester Peter Brands, Regional Sales Manager Western Europe – D-A-CH, Tyco Security Products

mal auf der technischen Seite. Hier kann man sagen: Ein IP-Leser ließe sich relativ leicht und auch vergleichsweise schnell umsetzen. Aber man muss auch die Kosten und das Kompetenz-Gerangel bezüglich IP-Technik in den Unternehmen bedenken. Es ist daher auch eine Frage, wer die IP-Technik verwaltet, und wie es sich eine Umstellung kostenmäßig niederschlagen würde.“

Knackpunkt Sicherheit

Ein weiterer Knackpunkt bei der Nutzung von Internet und mobilen Apps für die Zutrittskontrolle ist die Sicherheit der Daten. Dass dies auch in der Praxis immer wieder diskutiert wird, kann Rainer Füess bestätigen: „Datenschutz und Datensicherheit sind täglich Themen in der Beratung und Projektierung. Man muss hier Vorsichtsmaßnahmen treffen und Vereinbarungen mit den Kunden eingehen. Das ergibt sich

schon allein aus gesetzlichen Vorgaben, die uns verpflichten, unsere Systeme hinsichtlich Datenschutzerfordernissen zu prüfen.“

Und Volker Kraiss ergänzt: „Datensicherheit hängt sehr eng mit der Verschlüsselung zusammen, die gewährleistet sein muss. Das ist in unserer Branche natürlich immer ein Thema. Wir fragen bei unseren Ausschreibungen immer bei den Systemlieferanten genau nach, wie der sichere Datenverkehr bis hinunter zu den Ausweislesern konzipiert ist. Bei fast allen Anwendungen ist aber auch die Nutzung des Internets vorgesehen, und da könnte theoretisch abgehört werden, sofern nicht gesicherte Verbindungen mit entsprechenden Verschlüsselungsmechanismen genutzt werden.“

Davon unabhängig kann man natürlich weitere Maßnahmen ergreifen, wie Dietmar Vetten skizziert: „Ziehen wir noch einmal das Beispiel Fernwartung heran: Die Unternehmen, die uns erlauben, auf ihre Systeme

zuzugreifen, haben unterschiedlichste Wege, das abzusichern. Sie haben ihre Netzwerksicherheit im Griff und stellen teilweise einen eigenen Laptop zur Verfügung, mit dem man Zugriff auf das Netzwerk hat. Es gibt auch Kunden, die extra ein bestimmtes Netzwerkkabel einstecken, um temporär von außen Zugriff auf den Zutrittsserver zu gewähren.“

Dass sich die mobile Technik am Ende deshalb doch langsam durchsetzen wird, glaubt Robert Karolus: „Man muss nur zehn Jahre zurückschauen, damals haben die mobilen Anwendungen schon langsam in die Zeitwirtschaft Einzug gehalten. Das hat Urlaubsanträge und Zeitkorrekturen vereinfacht und ist mittlerweile Standard in diesem Umfeld. In der Sicherheitstechnik braucht es wohl auch deshalb noch etwas länger, um sich durchzusetzen, weil man immer auch an die Sicherheit der Systeme denken muss. Aber ich denke, auch das wird man in den nächsten Jahren lösen, so dass die Verbreitung steigt.“

Hoch in den Wolken

Genau diesen Bedenken scheint ein anderer Trend zu widersprechen, bei dem man viel Kontrolle aus der Hand geben kann. Die Rede ist von Cloud-basierender Zutrittskontrolle beziehungsweise Auslagerung von Datenbanken und Administrationsaufgaben auf verteilte Server. Diese Schlagworte liest man immer wieder, wiewohl die Resonanz aus der Praxis noch verhalten ist, weiß Christoph Tegelkamp von Dorma: „Das Verlagern von Softwareapplikationen und die Administration von Zutrittskontrolle aus der Cloud klingt vielversprechend und bietet Vorteile für den Nutzer. Die Erfahrung bei mittleren und größeren Kunden hat aber auch gezeigt, dass sie größten Wert auf ihre Sicherheitsprozesse legen und den Nutzen höheren Komforts gegenüber möglichen Risiken einer externen Speicherung der Daten abwägen. Von daher wird es noch spannend werden, in welchen Bereichen sich Cloud- und

Mobil-Lösungen wirklich durchsetzen können.“ Das Potenzial dafür sieht Hartmut Beckmann eher in den kleineren Anwendungen: „Wenn man kleine und mittlerer Unternehmen mit einer modernen Zutrittskontrolle ausstatten will, dann muss man Lösungen bringen, die günstig und effizient sind. Das geht mit Cloud- und App-basierten Systemen sehr gut, weil die Infrastruktur schlank und kostengünstig ist. Damit kann man Anlagen mit fünf oder sechs Türen auch gut handhaben.“

Es zeigt sich: die Zutrittskontrolltechnik steckt mitten in einem Wandel der Systeme

und der Bedienphilosophien. Noch ist nur schemenhaft absehbar, in welche Richtung sich die mobile Zutrittskontrolle entwickelt und wie es künftig die Akzeptanz der Nutzer bestellt sein wird. Potenziale sind vorhanden, genauso wie einige Ungereimtheiten. Auch deshalb bleibt es ein spannendes Feld, das man aufmerksam weiter beobachten sollte. MG



Artikel als PDF

www.sicherheit.info
Webcode: 1134057

**IFSEC
stand E1450**



GESUCHT:

**Stressfreier
Errichter m/w**

Sie haben pünktlich um 17 Uhr Feierabend und die Wochenenden sind entspannt. Die Implementierung des Sicherheitssystems, welches Sie betreuen, ist flexibel und kosteneffektiv.

Ist das Ihr persönliches Profil?

Dann arbeiten Sie vermutlich schon mit der Sicherheitsplattform AEOS. Wenn nicht, schauen Sie es sich an:
www.nedapsecurity.com/de/gesucht