



Bilder: MG

Die Teilnehmer am zweiten Tag des PROTECTOR Forums Zutrittskontrolle (von links): Bernd Lesemann, Hartmut Beckmann, Volker Kraiss, Dietmar Vetten, Marco Pompili, Chefredakteur Andreas Albrecht, Moderator Boris Stamm, Polichronis Sidiropoulos, Harald Gilleßen.

Offline- und Online-Systeme

Das Kind beim Namen nennen

Die Zutrittstechnik ist stetig im Wandel, die Bandbreite an Systemen und Funktionen wächst. An vielen Stellen verschwimmen zudem die Grenzen, was eigentlich Zutrittskontrolle ist und wie man sie aktuell definieren kann. Offline- und Online-Systeme nähern sich derart an, dass eine klare Abgrenzung schwer fällt. Dennoch bot das PROTECTOR Forum Zutrittskontrolle 2015 den idealen Rahmen, es zu versuchen.

Definition: „Für mich kann auch eine mechanische Schließanlage eine Form von Zutrittskontrolle sein, eben eine mechanisch organisierte Zutrittskontrolle. Aber ich weiß natürlich, dass man die Diskussion häufiger führt, wie genau Zutrittskontrolle zu definieren ist.“

Zwischen den Extremen

Genau in diesem recht weiten Spannungsfeld bewegen sich auch die Anwender, die entscheiden müssen, welche Aussagen von Herstellern der Kategorie Vermarktung oder der Kategorie Technik zuzuordnen sind. Die Gemengelage am Markt ist manchmal verwirrend, wie auch die Schilderung von Bernd Lesemann von Opertis zeigt: „Wenn wir über elektronische Zylinder reden, finden sich hier auch mehrere Begriffe wieder: Mechatronik, Digitalzy-

Schon die erste Frage zum Thema durch Moderator Boris Stamm löst eine Grundsatzdebatte aus: „Ich möchte vorneweg eine Frage zur Begriffsklärung stellen: Nehmen wir einmal an, ich ersetze als Betreiber meine alte mechanische Schließanlage und verwende stattdessen in Zukunft nicht mehr das Medium Schlüssel, sondern einen Transponder. Habe ich dann automatisch Zutrittskontrolle?“

Volker Kraiss von Kraiss Consult winkt ab: „Durch den Einsatz von elektronischen Zylindern und Beschlägen hat man noch keine klassische Zutrittskontrolle. Wenn man mechanische Zylinder durch elektronische Zylinder oder Beschläge ersetzt, hat man in erster Linie nur ein elektronisches und relativ komfortables Schließsystem und nicht mehr.“ Doch für Harald Gilleßen von Gretsch-Unitas ist auch das eine Frage der

linder, Offline-Zutrittskontrolle und so weiter. Außerdem kommt es auf die konkrete Ausgestaltung der jeweiligen Anlage an. Die vollen Funktionalitäten einer Zutrittskontrollanlage können auch mit elektronischen Schließzylindern und der zugehörigen Verwaltungssoftware offline wie online gegeben sein. Eine vernetzte elektronische Schließanlage ist deshalb auch ein Zutrittskontrollsystem, das man von ganz geringen Anforderungen bis hin zu höchsten Ansprüchen skalieren kann – inklusive Forensik und Hochsicherheit sowie Einbindung von Brandmeldeanlagen oder Videoüberwachung.“

Volker Kraiss betont, dass es dennoch Möglichkeiten zur Differenzierung gibt: „Die Leistungsmerkmale einer klassischen Online-Zutrittskontrollanlage unterscheiden sich schon wesentlich von den Leistungsmerkmalen eines elektronischen Schließsystems. Bei klassischen Online-Zutrittskontrollanlagen verfügen wir über deutlich erweiterte Funktionalitäten, allen voran die Türüberwachung, die Kombination mit zusätzlichen Stellgliedern und die Integration in ein übergeordnetes Gefah-



renmanagement. Diese Dinge kommen in der Welt der elektronischen Zylinder und Beschläge nicht vor, und das markiert für mich den Punkt, an dem zumindest im Bereich sicherheitsrelevanter Geschäftsprozesse und damit verbundener Sicherheitsstandards elektronische Schließkomponenten beziehungsweise Schließsysteme nicht eingesetzt werden können.“

Ergänzen und zusammenwachsen

Doch es gibt auch Szenarien, wo die Mechatronik erweiterte Funktionen ermöglicht oder gewisse Installationen vereinfacht, wie Harald Gilleßen anmerkt: „Die problemlose Verfügbarkeit von leistungsfähigen mechatronischen Komponenten hat auch klare Vorteile für manche

Offen und flexibel.

AXIS A1001 Netzwerk-Tür-Controller

AXIS A1001 ist ein einfach zu installierender Tür-Controller mit integrierter Management-Software sowie offenen Schnittstellen zur Integration in andere Systeme.

Mit AXIS A1001 erhalten Sie endlich eine offene und flexible Alternative für die Zutrittskontrolle – egal ob Sie eine, oder 1.000 Türen installieren.

www.axis.com/products/access_control

AXIS[®]
COMMUNICATIONS

Security
Distribution
Partner:



Tel.: +49 6074 888-300
E-Mail: security@videor.com
videor.com



„Wenn wir über elektronische Zylinder reden, finden sich hier auch mehrere Begriffe wieder: Mechatronik, Digitalzylinder, Offline-Zutrittskontrolle und so weiter. Außerdem kommt es auf die konkrete Ausgestaltung der jeweiligen Anlage an. Die vollen Funktionalitäten einer Zutrittskontrollanlage können auch mit elektronischen Schließzylindern und der zugehörigen Verwaltungssoftware offline wie online gegeben sein.“

Bernd Lesemann, Product Manager, Opertis GmbH

„Die problemlose Verfügbarkeit von leistungsfähigen mechatronischen Komponenten hat auch klare Vorteile für manche Anwendung. Nehmen wir zum Beispiel eine Brandschutztür, die man in ein Zutrittssystem einbinden möchte. Das geht mit einem elektronischen Zylinder ohne die teuren und aufwendigen baulichen Veränderungen, vor denen man sonst wohl zurückschrecken würde.“



Harald Gilleßen, Produktmanagement Elektronik, BKS GmbH



„Es geht in der Praxis darum, ein gewisses Anforderungsszenario an der Tür zu bedienen. Dabei kann man heute je nach Türsituation frei wählen zwischen einer klassischen drahtgebundenen Online-Zutrittskontrolle und mechatronischen Komponenten, die wiederum entweder über die offline-Berechtigungen auf der Karte oder mittels Funk vernetzt werden.“

Polichronis Sidiropoulos, Vertriebsleiter Zutrittskontrolle, Assa Abloy Sicherheitstechnik GmbH

„Ich sehe auf jeden Fall eine Tendenz, dass Offline-Hersteller immer komplexere Systeme anbieten, mit denen sie teilweise sogar die Online-Zutrittskontrolle ersetzen könnten. Doch entscheidend bei der Wahl der Technik sollten die Anforderungen der Anwender sein. Nach der Konzepterstellung, kann die Auswahl der Produkte und Technologien erfolgen.“



Hartmut Beckmann, Leiter Vertrieb, Uhlmann & Zacher GmbH

Anwendung. Nehmen wir zum Beispiel eine Brandschutztür, die man in ein Zutrittssystem einbinden möchte. Das geht mit einem elektronischen Zylinder ohne die teuren und aufwendigen baulichen Veränderungen, vor denen man sonst wohl zurückschrecken würde. Mit einem verdrahteten Online-System wäre das sehr schwierig. Aber dank der Mechatronik kann man diese Türen mühelos integrieren und absichern.“

Das angesprochene Szenario sowie die erwähnten Funktionalitäten auf beiden Seiten verdeutlichen schon, dass es in der Praxis – und vor allem aus Anwendersicht – diese klare Trennung der Systeme gar nicht gibt. Und auch die Hersteller bieten zunehmend beide Varianten an, um die Ansprüche des Kunden bestmöglich bedienen zu können. Vielmehr wachsen die einstigen Offline-Systeme nach oben in die Richtung Zutrittskontrollanlage und zum anderen runden die klassischen Online-Anbieter ihre Portfolios nach unten hin durch vernetzte Digital-Zylinder ab.

Polichronis Sidiropoulos von Assa Abloy erläutert: „Insgesamt lassen sich hier zwei Ansätze erkennen. Einmal der ursprüngliche Top-down-Ansatz, bei dem die klassische Online-Zutrittskontrolle über die Mechatronik erweitert wird und dadurch in den Objekten zusätzliche Türen mit Zutrittskontrolle in Form von mechatronischen Komponenten ausgestattet und innerhalb eines Systems verwaltet werden. Und einmal der Bottom-up-Ansatz, bei dem die mechatronischen Komponenten aus der digitalen Schließanlage vernetzt und nach und nach mehr Funktionen aus der klassischen Online-Zutrittskontrolle integriert werden.“

Hartmut Beckmann von Uhlmann & Zacher ergänzt: „Viele klassische Online-Hersteller, die nun in Richtung Offline gegangen sind, müssen sich vorab überlegen, ob sie die Produkte selbst entwickeln wollen oder per OEM zukaufen, um das eigene System sinnvoll zu ergänzen.“

Anforderungen entscheiden

Dieses Zusammenwachsen vor allem auf administrativer Ebene kommt den Bedürfnissen der Anwender entgegen, wie Dietmar Vetten von GST betont: „Der Kunde möchte aus einer Software heraus alle Komponenten seines Zutrittssystems verwalten können und nicht zwei Systeme parallel laufen lassen. Alle Funktionen, die das Offline-Produkt bietet, sollen mit einer Online-Software abgebildet werden können. Natürlich gibt es Hersteller, die beides anbieten oder zumindest eng kooperieren, aber meistens sitzen wir als Systemintegrator zwischen den Herstellern und müssen dafür sorgen, dass es reibungslos läuft. Bei der Kombination von Offline und Online kommt es stark darauf an, dass im Pflichten- und Lastenheft genau geregelt ist, wer was zu leisten hat.“

Polichronis Sidiropoulos ist der Meinung: „Es geht in der Praxis darum, ein gewisses Anforderungsszenario an der Tür zu bedienen. Dabei kann man heute je nach Türsituation frei wählen zwischen einer klassischen drahtgebundenen Online-Zutrittskontrolle und mechatronischen Komponenten, die wiederum entweder über die offline-Berechtigungen auf der Karte oder mittels Funk vernetzt werden.“

Hartmut Beckmann sieht dafür gute Voraussetzungen: „Ich sehe auf jeden Fall eine





Marco Poimpili von Axis Communications verdeutlicht: „Die klassische Online-Zutrittskontrolle wird trotz des Erfolgs von Mechatronik immer noch gebraucht, und zwar immer da, wo ein Wachmann in der Leitstelle sitzt und das System im Auge behält. Die Offline-Systeme sehe ich nach wie vor stark in der Zutrittsorganisation, wo es weniger um Hochsicherheit geht.“

Es bleibt also auch künftig genug Raum für beide Systemdesigns, während gleichzeitig die Schnittmengen zur Integration wachsen. Dass die Nutzeranforderungen verstärkt in den Fokus rücken, ist zweifels- ohne zu begrüßen, denn die genaueste Begriffsdefinition nützt wenig, wenn sie an den Bedürfnissen der Kunden und an den in der Praxis geltenden Gewohnheiten vorbeigeht. MG

Tendenz, dass Offline-Hersteller immer komplexere Systeme anbieten, mit denen sie teilweise sogar die Online-Zutrittskontrolle ersetzen könnten. Doch entscheidend bei der Wahl der Technik sollten die Anforderungen der Anwender sein. Nach der Konzepterstellung kann die Auswahl der Produkte und Technologien erfolgen.“

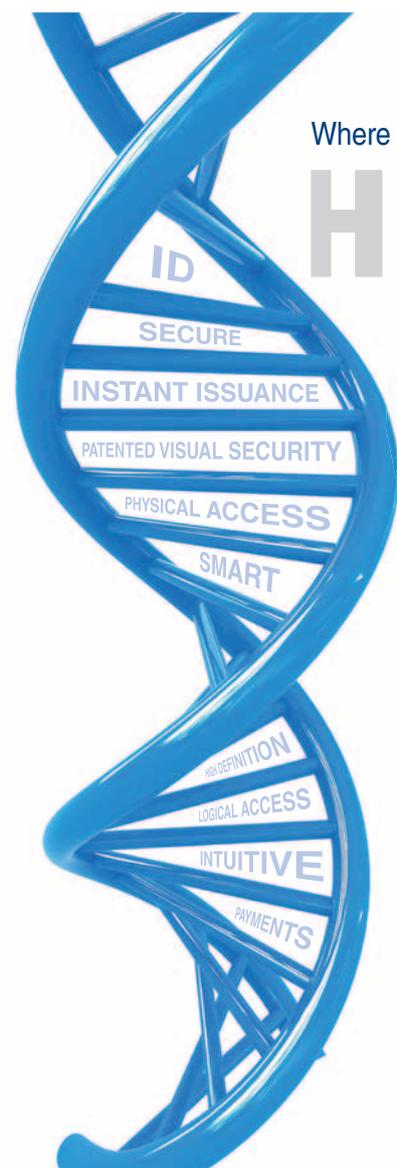
Und Volker Kraiss ergänzt: „Bei vielen Anwendern – gerade in der Industrie –

wird aus Offlinekomponenten und den Onlinekomponenten ein sinnvoll abgestuftes Gesamtsystem eingesetzt. Die Architektur des Gesamtsystems und die Entscheidung, wo elektronische Schließkomponenten oder Ausweisleser mit Überwachungsfunktionen in Kombination mit Stellgliedern eingesetzt werden, entscheiden die jeweiligen Sicherheitsanforderungen an den Zu- oder Abgängen.“



Artikel als PDF

www.sicherheit.info
Webcode: 1137666



Where identity begins.

HELIX

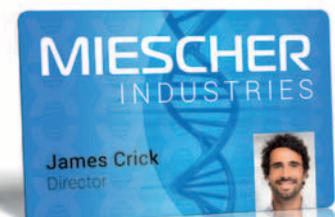
HEYDENSECURIT
Identifikation | Besuchermanagement

MAGiCARD

Master Dealer D/A/CH



Präsentation auf der
SicherheitsExpo in München -
Stand E01, 01. - 02. Juli 2015





Bilder: MG

Planung und Systemdesign

Beziehungen voll Harmonie?

Wenn es um die Konzeption und Projektabwicklung von Zutrittssystemen und gewerkeübergreifenden Anlagen geht, stellt sich immer wieder die Frage nach der Beratung und Planung: unabhängig, herstellerseitig oder beides zugleich? Wie sich die Bedürfnisse der Kunden mit den Ansätzen der Anbieter in Einklang bringen lassen, war Thema des PROTECTOR Forums Zutrittskontrolle 2015.

Eines ist heute klarer denn je: Für die Anbieter von Zutrittstechnik geht es in Sachen Kundenbeziehungen um mehr als nur einen einmaligen Auftrag. Es geht darum, nachhaltige Kundenzufriedenheit zu erreichen und zu pflegen. Dabei, so offenbart es die Diskussion schon zu Beginn, ist trotz aller Technisierung und Beschleunigung im Sicherheitsmarkt das Zwischenmenschliche gefragt. Klassische Tugenden bilden das Fundament für gelungene Projekte und anhaltenden Geschäftserfolg, wie auch Wilfried Joswig vom Verband für Sicherheitstechnik (VfS) erläutert: „Egal, in welche Branche man blickt, es zeigt sich immer wieder: Wenn man vernünftige Geschäfte machen will, dann basieren diese auf Vertrauen. Die Frage, die sich uns aber stellen sollte, ist: Wie erreicht man ein vertrauensvolles Verhältnis zwischen Systemlieferanten, Fachplanern und Kunden?“

Zuhören und Einfühlungsvermögen sind hier für Thomas Weber von Simonsvoss Grundvoraussetzungen: „In den unterschiedlichen vertikalen Märkten hat man auch verschiedene Schwerpunkte, was die Kunden- und Partneransprache angeht. Bei manchen dreht sich alles um die Sicherheit, bei anderen steht der Komfort im Mittelpunkt, bei wieder anderen, wie etwa Krankenhäusern, kann es auch die Hygiene sein. Man muss individuelle Ansätze herausarbeiten. Heute kann es oft auch die gut zu bedienende Software sein, auf die der Kunde besonders achten wird.“

Und Wilfried Joswig ergänzt: „Im Bereich der Zutrittskontrolle spielt ein umfangreicher Erfahrungsschatz eine große Rolle, nicht nur bezogen auf die Technik, sondern auch hinsichtlich Betriebsabläufe, Datenschutz, Personalverwaltung und dergleichen. Wichtig ist, auf Augenhöhe mit

Clex prime Sicherheit gestalten

U&Z

SICHERHEITS EXPO München
1.-2. Juli 2015
www.SicherheitsExpo.de
Halle 4, Stand B10

DER ELEKTRONISCHE TÜRRÜCKER

Schlichtes Edelstahl-Design trifft modernste Technik! Mit kompletter Elektronik, Mechanik sowie Stromversorgung im Türdrücker. Einfach und schnell montiert – ohne Verkabelung und Spezialwerkzeug.



Uhlmann & Zacher
SYSTEME AUS EINER HAND

25 JAHRE
1990
2015

www.UundZ.de



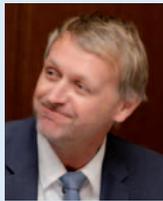
den Partnern zu reden und sich Vertrauen zu erarbeiten. Die technische Lösung steht dabei erst einmal im Hintergrund, bis eine Vertrauensbasis aufgebaut ist.“

Zuverlässigkeit entscheidet

Auch andere Qualitäten sind ausschlaggebend für die umfassende Kundenzufriedenheit, findet Axel Schmidt von Salto Systems: „Für uns war von Anfang an sehr bedeutsam, qualitativ sauber dazustehen. Die Technik muss bestmögliche Zuverlässigkeit für den Kunden bieten. Das schafft Vertrauen, genauso wie Kompetenz in der Beratung und der Planung. Dazu gehört es auch, die Grenzen aufzuzeigen, bis wohin man mit uns Lösungen erarbeiten kann. Wenn wir merken, der Kunde sucht eine Lösung, die wir nicht abbilden könnten, dann sagen wir das auch frei heraus und verkaufen ihm nicht etwas Unpassendes, sondern empfehlen ihn an einen Integrator weiter. Diese Ehrlichkeit schätzt der Kunde.“

Dem pflichtet Manfred Golfels von PCS Systemtechnik bei: „Für uns zählen natürlich auch in erster Linie die beiden Faktoren Vertrauen und Ehrlichkeit. Dabei heißt Vertrauen in Bezug auf die Partner ebenso, dass man ihnen bei Projekten nicht in die Quere kommt, etwa indem man direkt an den Endkunden herantritt. Gleichzeitig heißt es, ihm ein Netzwerk aus Kooperationspartnern anzubieten, damit auch kleine Mittelständler

„Auch die Benutzerfreundlichkeit von Software ist heute ein ausschlaggebender Faktor. Sie muss intuitiv sein und sich vernetzen können. Die Anlage muss NFC-ready sein und sollte auch ein gewisses Maß an Mobilität bieten, so dass man das System mit einer App bedienen kann. Außerdem wollen die Kunden – hier vor allem größere Unternehmen – schon vorab Informationen haben, wie man als Anbieter das Projekt angehen will. Man will Projektpläne sehen und erfahren, wie bestehende Hardware eingebunden wird. Das ist heute oft entscheidend in den Projekten.“



Robert Karolus, Product Manager,
Interflex Datensysteme GmbH & Co. KG



„Die Betreuung unserer Kunden basiert stark auf persönlichen Kontakten mit unseren Vertriebsmitarbeitern. Diese sind auch keine klassischen Verkäufer, sondern Systemberater mit einer hohen technischen Kompetenz und Verantwortung für die Zufriedenheit des Kunden. Sie beraten den Kunden von Anfang an und bieten ihm schließlich das richtige System für seine Bedürfnisse.“

Sven Däberitz, Vorstand, Intrakey Technologies AG

„Egal, in welche Branche man blickt, es zeigt sich immer wieder: Wenn man vernünftige Geschäfte machen will, dann basieren diese auf Vertrauen. Die Frage, die sich uns aber stellen sollte, ist: Wie erreicht man ein vertrauensvolles Verhältnis zwischen Fachplanern, Systemlieferanten und Kunden?“



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



TÜRTECHNIK

BKS

Identifizieren – Schließen – Organisieren
Das elektronische Schließsystem SE



Mehr Flexibilität erschließen.

Sicheres Schließen – seit mehr als 100 Jahren die Kernkompetenz von BKS – ist auch die zentrale Funktion des umfassenden elektronischen Schließsystems SE.

Mit dem modularen Sicherheitssystem lösen Sie jede Zutrittsanforderung und jede Objektsituation – wenn gewünscht auch in Kombination mit mechanischen Schließanlagen.

- Besonders geringer Energiebedarf der Produkte: bis zu 600.000 Schließzyklen bzw. bis zu 10 Jahre Standby/Standard-Batterie
- Schnelles Sperren und Ersetzen verlorengegangener Schlüssel oder Transponder
- Individuelle Vergabe von Zutrittsrechten
- Erfüllt die höchsten Sicherheitsklassen der Norm für mechatronische Schließzylinder DIN EN 15684

BKS GmbH | D-42502 Velbert

Tel. + 49 (0) 2051 2 01-423

www.g-u.com



„In Zukunft wird auch wichtig sein, wie man mit der Controller-Ebene umgeht, also mit der Frage, wie die Software die unterschiedlichen Komponenten anspricht.

Bewegen wir uns künftig noch in proprietären Welten oder wird sich durch die Unterstützung von Standards vieles ändern, auch bei den Schnittstellen zu den Controllern? Die Anbieter, die solche Fragen jetzt schon beherzigen, haben in letzter Zeit bei Ausschreibungen meist die Nase vorn.“

Thomas Maier, Vorstand, SOAA Standard für Industrieapplikationen eG

„Wir vollziehen einen großen Schritt in der Trennung zwischen Hardware und Software und werden in ein paar Jahren sehen, wie sich das im Systemaufbau auswirkt. Wie wird der Controller beim Kunden dann aussehen? Vielleicht hat er sogar die Form eines Smartphones, und man muss nur seine Software aufspielen? Traditionell versucht natürlich jeder Hersteller, auch seine Hardware zu platzieren, aber vielleicht verkaufen wir in der Zutrittskontrolle künftig in erster Linie Software“

Christian Nagel, Sales, Nedap Deutschland GmbH



„Wir müssen unsere Partner dazu befähigen, die Vorteile der Lösungen richtig zu kommunizieren. Wir investieren deshalb sehr viel in Training und Schulung. Das

vor allem auch vor dem Hintergrund, dass unsere Wertschöpfungskette breiter wird – wir bieten nicht nur Zutrittskontrolle, sondern auch IT-Sicherheit, Personalisierung oder Mobile-Access-Lösungen.“

Volker Kunz, Director of Sales – EMEA, HID Global GmbH

„Wir haben im Prinzip drei Vertriebsbereiche: erstens den indirekten Vertrieb, wo wir keinen Kontakt zum Kunden haben und auf beratende Partner setzen, zweitens den direkten Vertrieb von Sicherheitstechnik, wo wir mit eigenen Projektleitern und Beratern arbeiten, und drittens noch den Kanal des sogenannten Schließfachhandels, wo Systeme angeboten werden, die ohne große Projektierung selbst installiert werden können.“

Albrecht Kimmich, Product Manager Strategic Marketing, Kaba GmbH



ein großes Portfolio liefern können. Das ist häufig nötig, um im Markt zu bestehen.“

Einen vertriebsbedingt etwas anderen Ansatz verfolgt Jochen Becker von Primion Technology: „Wir vertreiben häufig nicht über ein Partnernetzwerk, sondern direkt an den Anwender. Deshalb werden wir mehr und mehr zum Systemintegrator und zum Projekthaus, um der Anforderung des Kunden, alles aus einer Hand bieten zu können, gerecht zu werden. Dabei muss man sich sehr wohl im Klaren sein, welche Gewerke man bedienen kann und will. Realistisch betrachtet ist man natürlich nicht immer in der Lage, alles aus einer Hand zu liefern – es gibt auch Projekte, für die man einen starken Partner braucht, um für den Kunden die bestmögliche Lösung zu schaffen.“

Ansätze und Absätze

Es wurde damit bereits angedeutet, dass es verschiedene Ansätze der Kundenansprache gibt. Einen weiteren skizziert Sven Däberitz von Intrakey: „Die Betreuung unserer Kunden basiert stark auf persönlichen Kontakten mit unseren Vertriebsmitarbeitern. Diese sind auch keine klassischen Verkäufer, sondern Systemberater mit einer hohen technischen Kompetenz und Verantwortung für die Zufriedenheit des Kunden. Sie beraten den Kunden von Anfang an und bieten ihm schließlich das richtige System für seine Bedürfnisse.“

Gerhard Haas von PHG wiederum verfolgt aufgrund der Ausrichtung seines Unternehmens eine andere Philosophie: „Da wir keine Komplettsysteme anbieten, sondern OEM-Komponenten, sind wir in die Beratung des Endkunden natürlich nicht übermäßig involviert. Unser Anspruch ist ein anderer, unseren OEM-Partnern nämlich für jedes denkbare Einsatzszenario den richtigen Produktmix anbieten zu können. Es soll kein Projekt scheitern, weil wir nicht die passenden Produkte anbieten können.“

Für Volker Kunz von HID Global funktionieren erfolgreicher Vertrieb und gekonnte Beratung heute nicht ohne starke Partner: „Da wir traditionell indirekten Vertrieb betreiben, setzen wir hauptsächlich auf Partner. Diese müssen aber heute technisch und vertrieblich fitter sein denn je, denn unser Anspruch wird immer höher, genauso wie die Themen, die wir besetzen, immer komplexer werden. Wir müssen also unsere Partner dazu befähigen, die Vorteile der Lösungen richtig zu kommunizieren. Wir investieren deshalb sehr viel in Training und Schulung. Dies vor allem auch vor dem Hintergrund, dass unsere Wertschöpfungskette breiter wird – wir bieten nicht nur Zutrittskontrolle, sondern auch IT-Sicherheit, Personalisierung oder Mobile-Access-Lösungen.“

Für Albrecht Kimmich ist die Ansprache und Beratung der Kunden stark abhängig vom Vertriebskanal: „Wir haben im Prinzip drei Vertriebsbereiche: erstens den indirekten Vertrieb, wo wir keinen Kontakt zum Kunden haben und auf beratende Partner setzen, zweitens den direkten Vertrieb von Sicherheitstechnik, wo wir mit eigenen Projektleitern und Beratern arbeiten, und drittens noch den Kanal des sogenannten Schließfachhandels, wo Systeme angeboten werden, die ohne große Projektierung selbst installiert werden können.“

Guter Rat ist billig?

So unterschiedlich die Ansätze der Unternehmen auch sein mögen, ihnen gemein ist doch der Aspekt, den Kunden direkt oder über geschulte Partner zu beraten und ihm ein passendes System auf Basis des eigenen Portfolios zu planen. Dennoch soll dies mit einem Blick über den Tellerrand geschehen, findet Christian Nagel von Nedap: „Natürlich muss jeder, der in beratender Tätigkeit zum Kunden geht, sich am Markt bestens auskennen. Hier ist es wichtig, dass man nicht die eigene Technik in den



Vordergrund stellt, sondern versucht, zusammen mit dem Kunden eine Lösung zu erarbeiten, die für ihn passt. Davor scheuen viele zurück, weil es leichter ist, nur das eigene Portfolio im Fokus zu haben. Aber besser ist es, einen Schritt zurückzutreten und offen nach der bestmöglichen Lösung zu suchen. Man muss dafür seine Grenzen kennen. Ein solches Vorgehen fällt sicherlich auch denjenigen leichter, die Systeme haben, an die sich Produkte von Drittherstellern und andere Gewerke anbinden lassen.“

Bei diesem Ansatz erhält der Kunde also die Leistungen für Beratung und Planung von einem Hersteller quasi als Dreingabe

zu den gekauften Produkten. Ein schlagenes Argument aus Sicht der Budgetverantwortlichen, die meist ungern zusätzlich einen Planer bezahlen möchten. Doch Beratung und Planung kosten Geld. Die Frage ist nur, wen? Jochen Becker erläutert das Dilemma: „In der Praxis ist es oftmals für uns schwierig, alle Aufwendungen, insbesondere für Planung, die Erstellung von aufwendigen Sicherheitskonzepten, gegenüber dem Kunden geltend zu machen, da wir ein Gesamtsystem verkaufen, inklusive Dienstleistungen für Projektsteuerung, Inbetriebnahme sowie After-Sales-Services, und vom Kunden erwartet wird, dass diese

Konzepte im Rahmen der Ausführungsplanung kostenneutral enthalten sind.“

Dieser Aufwand wird auf Kundenseite oft falsch eingeschätzt, findet Kester Brands von Tyco: „Der Anwender ist sich in den wenigsten Fällen bewusst, dass ein vernünftiges Sicherheitskonzept eine konkrete Analyse und Planung voraussetzt. Es gibt genügend Kunden, die blauäugig in die Projekte hineingehen und denken: Ich kaufe „ein Stück“ Zutrittskontrolle. So funktioniert es aber bei den komplexen System mit ihren Schnittstellen und Anbindungen von heute nicht. Die Hersteller können die Planung übernehmen oder der Kunde braucht

euroid 2015



Internationale Fachmesse und Konferenz
für Identifikation
Frankfurt am Main, 10. – 12.11.2015

Identifikation? ... dann sind Sie hier richtig!

Die Welt der ID-Technologien für Entwickler und Innovatoren –
hier entsteht Zukunft.

10101010
10101010100
10101111
0101010101
0101001001
101010100101
0010010
1010101010
011101010
10101010
01010101
10101010

Erfahren Sie, welche Produkte &
Innovationen die Branche zu bieten hat!

Conceptual partner Exhibition:



Weitere Informationen unter:
www.euro-id-messe.de oder +49 711 61946-0

ID WORLD

INTERNATIONAL CONGRESS



mesago
Messe Frankfurt Group



einen Fachplaner, der diesen doch umfassenden Themenblock abdeckt.“

Management-Attention!

Dass Planung kostet und ein unabhängiger Planer sich am Ende rechnen könnte, wird bei den Projektverantwortlichen oft nicht gesehen. Das findet auch Thomas Maier vom SOAA-Gremium: „Ob die Planungskosten für Sicherheitssysteme übernommen werden, hängt immer davon ab, wo die Management-Attention im Unternehmen liegt. Wenn es beispielsweise für die Zutrittskontrolle keine Aufmerksamkeit gibt, werden die Planungskosten auch nicht ins Budget übernommen. Mit dieser Situation müssen die Hersteller umgehen und anders kalkulieren, weil sie die reine Planungsleistung nicht bezahlt bekommen.“

Dass dies nicht ausweglos ist, weiß Sven Däberitz: „Wir haben in der Vergangenheit oft erlebt, dass man die teilweise erheblichen Aufwendungen für Planung und Beratung nicht abrechnen konnte. Dabei lässt das Fachwissen auf Kundenseite eher nach und die Ansprüche an uns wachsen dementsprechend. Deshalb haben wir uns intensiv überlegt, wie man Planung und Projektierungsleistungen sinnvoll anbieten und auch

verkaufen kann. Auch wenn man natürlich nicht alles verrechnen kann, so lässt sich doch ein erheblich Teil abrechnen, wenn man den Wert dieser Leistungen rechtzeitig und richtig argumentiert.“

Verkaufsförderung

Der Kunde ist bei der Auswahl seines neuen Systems unter Umständen aber nicht nur für gute Argumente hinsichtlich Planung zugänglich, sondern auch für Marketing und Werbebotschaften – und dies womöglich um einiges leichter. Moderator Boris Stamm fragt deshalb zu Recht in die Runde: „Was bringt das klassische Alleinstellungsmerkmal für den Vertrieb – ist es am Ende gar kaufentscheidend? Oder taugt es nur für die Broschüre, weil der Großteil der Anwender diese Sonderfunktionen überhaupt nicht braucht?“

Carsten Hoersch von Sesam sieht es zwiespältig: „Der Nutzen von Alleinstellungsmerkmalen ist schwer zu fassen. Denken wir einerseits an die klassische Ausschreibung, in der fünf Anbieter das Geforderte anbieten können. Hier kann bei der Präsentation der eigenen Lösung womöglich ein Alleinstellungsmerkmal hilfreich sein. Aber denken wir andererseits an die breite Masse von Anlagen, dann bringen diese

Sonderfunktionen dem Kunden oft wenig, denn was für einen Flughafen sinnvoll sein kann, muss es für den Mittelständler noch lange nicht sein.“

Axel Schmidt ergänzt: „Es gibt natürlich schon sinnvolle Alleinstellungsmerkmale, die für die Unternehmen und für die Kunden nützlich sind. Es kommt auf die Definition an, denn man kann beispielsweise auch sagen, man hat eines der breitesten Produktportfolios – vom Schrankschloss bis zum Vorhängeschloss, von Mifare Classic bis Desfire oder Ähnliches. Der Kunde hat dann den Vorteil, dass er nicht zwei verschiedene Systeme einsetzen muss. Es gibt also Alleinstellungsmerkmale, die vor allem bei größeren Anlagen zum Tragen kommen.“

Mut zur Differenzierung

Einen weiteren Aspekt, den man unter Alleinstellungsmerkmal verbuchen kann, nennt Jochen Becker: „Wir haben eine Managementsoftware entwickelt, die wir als Integrationsplattform nutzen. Dort vereinen wir Gewerke wie Videoüberwachung, Brandschutz, Zutrittskontrolle gepaart mit einer leistungsfähigen Scripting- und Workflow-Engine. Hierin sehen wir Wachstum und Potenzial,

ACCESS GRANTED

Elektronische Sicherheitssysteme

- Zutrittskontrolle
- VdS-Schaltanlagen
- Tastatur-, RFID- und Biometrie-Leser

Nr. 8 899042
VdS
Zertifiziert nach
ISO 9002

Mitglied im
BHE

www.sesam.de

Sesam GmbH Finsterbachstraße 1 86504 Merching T +49 8233 79445-0 info@sesam.de

weil das ein Ansatz ist, mit dem man sich von den Markbegleitern abheben kann.“

Für Thomas Maier ist das plausibel: „Man sieht, dass sich in vielen Ausschreibungen in letzter Zeit Unternehmen durchsetzen, die Managementsysteme haben, die leicht zu bedienen sind. Meist sind das auch Firmen, die Projektmanagement beherrschen.“

Sven Däberitz erläutert seinen Ansatz zur Differenzierung: „Wir haben es uns abgewöhnt, in jedem Preiskampf mitspielen zu müssen. Wir konzentrieren uns lieber auf komplexe Lösungen, bei denen Schnittstellen zu anderen Systemen nachgefragt werden; auf integrierte Lösungen, die gewerkübergreifend arbeiten. Dazu haben wir über die Jahre einen Baukasten aus Systemkomponenten geschaffen. Damit können wir auch Kundenwünsche, die zunächst einmal exotisch klingen, sehr gut und effizient anbieten. Es gibt am Ende ein stimmiges Gesamtsystem.“

Jürgen Schneider von NTP rät, nicht nur beim Auftreten am Markt, sondern auch bei der Begrifflichkeit zur Differenzierung: „Mit den Alleinstellungsmerkmalen ist es so eine Sache, denn es gibt objektive Merkmale und subjektiv empfundene Merkmale, welche die Frage der Nachprüfbarkeit mit sich bringen. Wenn ein Anbieter der Meinung ist, sein System ist das beste, mag das ja subjektiv berechtigt sein, aber ob der Kunde den Nutzen faktisch auch so empfindet, ist eine ganz andere Frage. Und man muss auch sagen, dass proprietäre Alleinstellungsmerkmale in einem sehr dicht besetzten Markt wie Deutschland bestenfalls temporär gültig sind. Mitbewerber werden schnell nachziehen, wenn sie Potenzial darin sehen.“

Kompetenzen und Positionen

Dennoch können sie nützen, wie Christian Nagel findet: „Alleinstellungsmerkmale sind auch ein Hilfsmittel, die der Vertrieb gerne nutzt. Aber der Kunde stellt oft ganz andere Fragen: Er will nicht wissen, wo das Alleinstellungsmerkmal liegt, sondern wo sich der Hersteller positioniert. Agiert er zukunftsorientiert und offen? Der Kunde möchte nicht mehr proprietär gebunden sein und sich in eine Abhängigkeit begeben, er möchte Wahlfreiheit und Investitionsschutz.“

Robert Karolus von Interflex lenkt den Blick in eine ähnliche Richtung: „Ich glaube, der Kunde fragt heute in erster Linie nach Kernkompetenzen und nicht nach Alleinstellungsmerkmalen. Er stellt sich die Frage, wo welches Unternehmen seine Stärken hat und ob er vielleicht noch einen Integrator hinzuziehen muss. Das gleiche gilt auch für die Planer und Berater, die ihre Kompetenzen unterschiedlich ausgebildet haben.“

Man kann also dem Kunden im eigenen Interesse raten, sich schlau zu machen, zu vergleichen und zu hinterfragen, welche Anbieter was leisten und wo ihre Stärken und Schwächen liegen. Auch die Einbeziehung eines unabhängigen Planers kann sich rechnen, wenn man im Vorfeld die richtigen Präferenzen setzt. Etwas Know-how in Sachen Projektmanagement und Technik hat auch noch keinem Anwender geschadet. MG



Artikel als PDF

www.sicherheit.info
Webcode: 1137667

Der Mix macht's



VOXIO® Touch Die neue Generation

- kapazitive Touch-Tastatur
- edles Glasdesign
- Symbole und Ziffern hintergrundbeleuchtet
- IF Design Award 2015 / reddot award 2015
- drei Status-LED (multicolor/RGB)
- Multi-ISO-Plattform (Legic® SM-4200 M)

RELINO® Leserfamilie für „Feller-System“ (Schweiz)

- kapazitive Touch-Tastatur
- Multi-ISO-Plattform
(Legic® SM-4200 M)



Unsere aktuelle
Produktpräsentation



Testen Sie Ihren richtigen Mix mit Ihrem OEM-Partner auf der

SICHERHEITSEXPO

01.- 02. Juli 2015 · Halle 4 · Stand C16

Mehr Ideen für Ihre Integration finden Sie unter: www.phg.de

phg
Die richtige Verbindung

phg Peter Hengstler GmbH + Co. KG
78652 Deißlingen · Deutschland
Telefon 0 74 20 / 89-0
www.phg.de · datentechnik@phg.de

ZU IHRER SICHERHEIT

GFOS liefert umfassende Sicherheitslösungen für die Sicherheit Ihres Unternehmens.



Bilder: MG

Standards und Zertifizierungen

Radkralle oder Turbolader?

Standards und Zertifizierungen erhitzen regelmäßig die Gemüter in der Sicherheitsbranche – die einen preisen sie als wertvolles Instrument zur Orientierung und Qualitätskontrolle, die anderen geißeln sie als Kostentreiber und Innovationsbremse. Was also dem einen der Turbolader für den Markt ist dem anderen die ungeliebte Radkralle am Wagen.

Die Diskussion während des PROTECTOR Forums Zutrittskontrolle 2015 bemüht sich, abseits dieses Schwarzweißdenkens die wichtigen Grautöne herauszuarbeiten. Dabei sind die Ansätze und Perspektiven von klassischen Richtlinien wie VdS oder Normen wie DIN/EN durchaus andere als die von neueren Bestrebungen in Form von NFC, SOAA, Onvif und Co.

Moderator Boris Stamm weist am zweiten Tag noch einmal auf den bereits am Tag zuvor thematisierten Bedeutungsschwund der VdS-Richtlinie hin und fragt eingangs: „Ist die von einigen zum Quasi-Standard erhobene VdS-Richtlinie heute in der Praxis noch von Bedeutung? Oder taugt sie in der Rückschau sogar als Negativbeispiel, wie man es nicht machen sollte?“

Bernd Lesemann von Opertis ist in Sachen Relevanz zurückhaltend: „Was die Anforderungen an Zutrittsanlagen angeht, findet sich insbesondere der VdS heute wenig bis gar nicht wieder. Man liest den Verweis auf die Richtlinien zum Einbruchschutz zwar selten noch in Ausschreibungen, aber ob diese in den Anlagen letztlich auch umgesetzt werden, ist eine andere Frage. Und im Grunde taucht der VdS nur noch in Verbindung mit Einbruchmeldeanlagen auf.“

Dem stimmt Dietmar Vetten von GST zu: „Bei uns spielt VdS bei Zutrittssystemen fast keine Rolle, auch nicht in Ausschreibungen, die wir auf dem Tisch hatten. Bei der Planung von EMA wird zumindest immer noch gefragt: Werden nach VdS zugelassene Komponenten verbaut?“

Dabei wird aber nicht berücksichtigt, ob die komplette Anlage gemäß VdS errichtet wird. Das mag auch daran liegen, dass die Zertifizierung am Ende die Funktionalität der Anlage bremsen würde.“

Voll in die Eisen?

Damit wurde schon ein viel bemühtes Gegenargument in Bezug auf Standards angesprochen: die Bremswirkung. Bernd Leseemann erklärt: „Oft bilden Standards nicht den aktuellen Stand der Technik ab, weil sie schlichtweg veraltet sind. Ebenso geht es den zertifizierten Geräten: Sie werden einmalig geprüft und attestiert, dann ist der Stempel drauf, und das Produkt wird nie wieder angerührt. Denn sonst hätte man erneut den hohen Aufwand der Neuvorstellung und der Gerätezertifizierung. Das hieße in der Praxis doppelten Aufwand an Zeit und Geld – der Kunde weiß dies zudem oft nicht zu schätzen.“

Volker Kraiss von Kraiss Consult ergänzt: „Es ist doch so, dass der VdS seine Richtlinien den jeweils gültigen Normen anpasst und teils individuell durchaus sinnvoll ergänzt beziehungsweise abändert. Dabei sollte nicht vergessen werden, dass VdS-Richtlinien keine Normen sind und nur in Einzelfällen wirklich verbindlich sind. Sie zu berücksichtigen, kann in Einzelfällen allerdings durchaus sinnvoll und hilfreich sein.“

Kurz und knapp sind somit die wesentlichen Hemmnisse althergebrachter Standards genannt: Sie sind meist schon bei der Einführung überholt, im weiteren Verlauf viel zu starr und in der Umsetzung für die Anbieter meist zu teuer, um sie flächendeckend auf ein Produktportfolio anzuwenden. Doch davon unberührt bleiben die positiven Aspekte, die

Standards verwirklichen sollen und auch können, wenn sie von allen Seiten unterstützt und in den Markt getragen werden. Im Wesentlichen sind dies Vergleichbarkeit, Interoperabilität, Investitionsschutz, Internationalisierung und Modernisierung. Dies soll auch mit einigen neuen Standards auf Geräte- und Protokollebene erreicht werden. So beschäftigte sich der Löwenanteil der Diskussion mit den recht unterschiedlichen Standards NFC, SOAA und Onvif sowie dem Echo, welches sie bisher am Markt hervorrufen – oder auch nicht.

Alles neu und besser?

Diese neuen Standards und Zertifizierungsansätze wollen es besser machen als der VdS und mehr Relevanz in der Praxis erreichen. Doch haben sie das Zeug dazu? Moderator Boris Stamm fühlt den Teilnehmern auf den Zahn: „Wie sind Ihre Erfahrung des vergangenen Jahres, wird NFC von den Kunden und Partnern nachgefragt? Wie sind die Reaktionen darauf?“

Harald Gilleßen von Gretsch-Unitas muss differenzieren: „Nachfragen zu NFC erhalte ich schon, aber bisher nur von meinen Kollegen im Außendienst. Die möchten gerne wissen, was es damit auf sich hat. Aktuell kenne ich aber noch keinen Kunden, der NFC als Technologie einsetzen möchte. Zumindest kommt es nicht explizit zur Sprache, vielmehr fragt er nach einer komfortablen Lösung, wie man das Handy als Medium nutzen kann. Dennoch gibt es im Markt natürlich eine gewisse Erwartungshaltung, weil das Thema überall präsent ist.“

Polichronis Sidiropoulos von Assa Abloy sieht die Anzeichen ebenfalls: „Im Markt herrscht derzeit eine gewisse



Trotz aller Standardisierungsbestrebungen braucht man in der Praxis heute immer noch Schnittstellen, die oft kostspielig geschaffen werden müssen. Vielleicht wird sich das künftig ändern, weil sich SOAA und Onvif in der Breite durchsetzen. Aber im Moment tauchen meist noch Probleme auf, wenn man im Projekt beispielsweise Online- und Offline-Komponenten zweier Hersteller miteinander mischen will.

Dietmar Vetten, Vertrieb, GST Gesellschaft für Sicherheitstechnik mbH

Aus meiner Sicht ist SOAA ein vernünftiger Ansatz und führt in die richtige Richtung. Leider gibt es noch zu wenig SOAA-kompatible Lösungen und Komponente. Ein echter Wettbewerb existiert noch nicht. Aber wenn ich als Anwender heute eine Ausschreibung machen würde, würde ich SOAA als Alternative zu einer proprietären Lösung mit ausschreiben.

Volker Kraiss, Senior Consultant, Kraiss & Wilke Security Consult GmbH



KABELLOSE ELEKTRONISCHE ZUTRITTSLÖSUNGEN

XS4 2.0

NEUES DESIGN
NEUE INTELLIGENZ
NEUE VIELSEITIGKEIT

- modernes Produktdesign für verschiedenste Türarten und Sonderlösungen, innen wie außen
- leicht zu installieren und intuitiv zu bedienen
- mit zukunftsweisender Technologie zur Vernetzung per SALTO Virtual Network (SVN) und für die Echtzeit-Zutrittskontrolle per SALTO Wireless Funkvernetzung
- offen für RFID-basierte Multiapplikation sowie Integration mit Sicherheits- und Gebäudetechnik

SALTO Systems GmbH
info.de@saltosystems.com
www.saltosystems.de

Zur Sicherheit: Hand auf's Herz.



INTUS 1600PS.

Hätten Sie nicht auch gerne eine biometrische Zugangskontrolle mit dem Komfort einer Fingerabdruckerkennung und dem Sicherheitsniveau einer Iriserkennung? Bei der INTUS 1600PS Handvenenerkennung halten Sie kurz die Hand vor den Sensor, und das System entscheidet hochpräzise, wer Zutritt erhält oder nicht. Hygienisch, schnell, komfortabel und dabei hochsicher. Eine typische Innovation von PCS.



Besuchen Sie uns:
SicherheitsExpo
MOC München
01. – 02.07.2015
Halle 4, Stand D04

Tel.: +49 89 68004-550
www.pcs.com

pcs



positive Unruhe, was das Thema NFC angeht – dies bestätigt auch unsere Vertriebsmannschaft. Verstärkt wird das Ganze sicherlich auch dadurch, dass mittlerweile mehr und mehr mobile Endgeräte die NFC-Technologie unterstützen. Dennoch bedarf es noch einiges an Klärung, speziell in Zusammenhang mit dem Geschäftsmodell – damit steht und fällt das Ganze.“

Volker Kraiss gibt sich ebenfalls zurückhaltend: „Von Seiten unserer Kunden gab es im letzten Jahr keine einzige wirklich ernsthafte Anfrage zu NFC. In Verbindung mit den sicherheitskritischen Geschäftsprozessen ist der Sicherheitsstandard der App-basierten Lösungen auch nicht ausreichend. Wirklich sichere Lösungen werden aus kommerziellen Gründen leider noch nicht angeboten. Wir warten noch darauf, dass eine neutrale Stelle eine Studie zum Thema Sicherheit von NFC durchführt, in der vor allem die Anwendbarkeit für die professionelle Zutrittskontrolle unter verschiedenen Blickwinkeln beleuchtet wird.“

Hemmnisse im Markt

Doch wie Dietmar Vetten anmerkt, bedeuten konkreten Nachfragen aus dem Markt noch lange nicht, dass Projekte mit NFC auch umgesetzt werden können: „Wir hatten im letzten Jahr tatsächlich drei Anfragen, die ganz konkret NFC einsetzen wollten. Bei ersten ging es um Bankberater, die mit den Blackberrys per NFC Türen öffnen sollten. Das Problem war jedoch, dass die Geräte NFC nicht unterstützten. Dann hatten wir eine Anfrage von Nokia und Microsoft, die in ihren Telefonen NFC integriert haben. Auch hier sollte ein Pilotprojekt in Sachen Zutritt gestartet werden, doch es gab erhebliche Schwierigkeiten mit den Mobilfunk-Providern und dem sicheren Zugang zur SIM-Karte. Das Dritte war ein

großes Institut in Deutschland, welches gerne NFC-Vorreiter sein wollte. Wir haben mit zwei Herstellern gesprochen, die dort die Zutrittskontrolle geliefert hatten, und eine Projektgruppe gebildet. Doch das Fazit war: Der Markt ist noch nicht so weit, wir können es nicht umsetzen.“

Hartmut Beckmann von Uhlmann & Zacher versucht daher, das Thema mobiler Zutritt vom NFC-Standard zu lösen: „Das Smartphone wird in naher Zukunft sicherlich noch stärker zum Einsatz kommen. Neben NFC oder Bluetooth wird die steigende Verbreitung mobiler Zutrittslösungen vielleicht auch mit dem Thema Cloud zusammenhängen. Vor allem, wenn ein Öffnungsbefehl aus größerer Entfernung an die Tür gesendet werden soll. Hier kann die Einbindung einer Cloud für die notwendige Grundlage sorgen.“

Marco Pompili von Axis Communications sieht Abwehrverhalten auch auf Seiten mancher Smartphone-Hersteller: „Ein Hinderungsgrund war bisher, dass Apple in seinen Geräten kein NFC unterstützt hat. Nun haben sie es zwar eingeführt, es ist jedoch



SmartIntego –
die perfekte Lösung
für integrierte
Zutrittskontrolle.



nicht offen für andere Anwendungen außer der eigenen Bezahlfunktion. Das bringt uns in der Zutrittskontrolle natürlich nicht weiter. Es könnte auch sein, dass Apple zukünftig ihre NFC-Funktionalität für Drittanbieter öffnet. Des Weiteren können Smartphone-Anwendungen im Bereich Zutritt auch mit Bluetooth realisiert werden“.

Für Harald Gilleßen ist es unter anderem eine Frage der Anwendung: „Ich sehe das Szenario, mit dem Smartphone bequem die Tür zu öffnen, eher im privaten Bereich. Das ist der komplette Gegensatz zu einer Zutrittskontrolle im Unternehmen, wo die Risiken ganz andere sind. Man muss einfach Sicherheit und Komfort genau abwägen.“

Nutzen von Harmonisierung

Einen anderen Ansatz verfolgt SOAA, das sich auf die Vereinheitlichung der Kommunikation von Offline-Zutrittskomponenten fokussiert hat. Hierfür besteht ebenfalls Bedarf am Markt, findet Polichronis Sidiropoulos: „Ich muss sagen, dass sich

SOAA-Nachfragen mittlerweile häufen. Die Idee ist eben gut und entspricht genau unserer Philosophie als Hersteller. Die größten Vorteile liegen ganz klar auf Kunden- und Betreiberseite. Aber auch die Anbieter können im Hinblick auf die OEM-Integration profitieren, indem sie sich von proprietären Lösungen etwas weiter lösen. Insgesamt sorgt man dadurch für mehr Flexibilität und schafft eine gewisse Vergleichbarkeit auf dem Gebiet.“

Hartmut Beckmann berichtet von ersten Erfolgen: „Da wir den SOAA-Standard relativ früh umgesetzt haben, sind heute bereits einige Installationen erfolgreich umgesetzt. Ein großer Vorteil ist, dass das Protokoll sehr umfangreich ist und aus diesem Grund sogar große Anlagen umgesetzt werden können. Dass die Lösung funktioniert, wurde auf der letzten Security live demonstriert. SOAA Ausweise, die bei einem Hersteller am Stand programmiert wurden, waren problemlos bei einem anderen Hersteller einsetzbar.“

Die Perspektiven von SOAA seien aufgrund seines recht umfangreichen Ansatzes



SMART
INTEGO

SmartIntego Schließzylinder, SmartHandle und GatewayNode – die neue Systemintegrations-Produktlinie von SimonsVoss.

Mit seinen leistungsfähigen Kommunikationsprotokollen lässt sich SmartIntego nahtlos in bestehende Leitsysteme für Gebäudesicherheitstechnik einbinden. Durch Autokonfiguration der Systemkomponenten über den SmartIntego Manager fällt der Integrationsaufwand im Vergleich mit anderen Systemen deutlich geringer aus.

Telefon: +49-89-99228-0 | www.simons-voss.de
www.smartintego.de





„Seit 2014 gibt es nun das Onvif-Profil für den Bereich Zutrittskontrolle und ich bin mir sicher, dass es den Markt stark öffnen wird. Der Hauptgrund, warum

Axis in diesen Bereich eingestiegen ist, war dass sich Partner und Kunden beschwert haben, immer proprietäre Zutrittslösungen von einem Anbieter kaufen zu müssen. Onvif schafft hier Abhilfe. Wir haben schon über 25 Softwarepartner gewinnen können, die Integrationen auf Onvif-Basis gemacht haben.“

Marco Pompili, Senior Business Development Manager, Axis Communications GmbH

„Es geht im Kern um Orientierung und Vereinfachung für den Anwender. Es soll ja durchaus Projekte geben, die international aufgesetzt werden, bei denen multinationale Unternehmen die Systeme in ihren örtlichen Niederlassungen synchronisieren und verknüpfen wollen. Hier können Standards und zugehörige Zertifizierungen von großem Nutzen sein. Doch gerade Letzteres fehlt meist, denn wo ist die neutrale Zertifizierungsstelle, die unabhängig abnimmt und die Anlagen mit dem nötigen Prüfsiegel versieht.“

Boris Stamm, Moderator des PROTECTOR-Forums Zutrittskontrolle



prinzipiell nicht schlecht, wie auch Volker Kraiss findet: „Die SOAA-Spezifikationen decken von Haus aus den größten Teil der erforderlichen Funktionen im Datenaustausch zwischen elektronischen Schließkomponenten, dem Ausweis und einem Ausweisleser ab. Unter individueller Nutzung von Standardfunktionen können auch bedingt proprietäre Lösungen umgesetzt werden. Da SOAA eine „offene Spezifikation ist“, kann jeder Hersteller einer ZK-Managementsoftware oder elektronischen Schließkomponenten die SOAA-Spezifikation anwenden. Anbieter von SOAA-kompatibler ZK-Managementsoftware, Ausweisen und Ausweisleser haben natürlich deutliche Wettbewerbsvorteile. Bei den Herstellern elektronischer Schließkomponenten ist man da eher geteilter Meinung. Für den Anwender eröffnet sich auf jeden Fall die Möglichkeit, bei der Beschaffung elektronischer Schließkomponenten mittels SOAA mehr Wettbewerb zu erzeugen.“

Harald Gilleßen ist hier noch skeptisch: „Bei SOAA sehe ich, wie bei anderen Harmonisierungsansätzen auch, das Problem des Nutzens für die Hersteller. Ich erkenne den Vorteil für den Anwender, sehe aber momentan nicht viele Hersteller, die diesen Standard vorantreiben wollen.“

Vielleicht muss man beharrlich bleiben und einen Standard langsam aufbauen und etablieren. Das zeigt auch das Beispiel Onvif aus dem Videobereich, welches anfangs belächelt und kritisiert wurde, nun aber quasi flächendeckend unterstützt wird. Eben dieser Onvif-Standard ist kürzlich auf Zutrittsanlagen erweitert worden – mit noch unklaren Ausgaben, aber viel Potenzial, wie Marco Pompili von Axis Communications findet: „Seit 2014 gibt es nun das Onvif-Profil für den Bereich Zutrittskontrolle, und ich bin mir sicher, dass es den Markt stark öffnen wird. Der Hauptgrund,

warum Axis in diesen Bereich eingestiegen ist, war, dass sich Partner und Kunden beschwert haben, immer proprietäre Zutrittslösungen von einem Anbieter kaufen zu müssen. Onvif schafft hier Abhilfe. Wir haben schon über 25 Softwarepartner gewinnen können, die Integrationen auf Onvif-Basis gemacht haben. Den Kunden stehen damit ganz neue Möglichkeiten offen, etwa Software von Firma A, Controller von Firma B und Leser von Firma C in einer individuellen Komplettlösung zu verknüpfen.“

Nicht müde werden

An Standards muss also etwas dran sein, was das nachhaltige Interesse an ihnen trotz aller Schwierigkeiten und Misserfolge der Vergangenheit begründet. Moderator Boris Stamm fasst zusammen und fordert: „Es geht im Kern um Orientierung und Vereinfachung für den Anwender. Es soll ja durchaus Projekte geben, die international aufgesetzt werden, bei denen multinationale Unternehmen die Systeme in ihren örtlichen Niederlassungen synchronisieren und verknüpfen wollen. Hier können Standards und zugehörige Zertifizierungen von großem Nutzen sein. Doch gerade Letzteres fehlt meist, denn wo ist die neutrale Zertifizierungsstelle, die unabhängig abnimmt und die Anlagen mit dem nötigen Prüfsiegel versieht?“

Für Volker Kraiss herrscht hier auch Fehlanzeige: Wie bei Onvif wird es vorerst auch bei SOAA keine Zertifizierung geben. Sofern wirklich erforderlich, bleibt es natürlich jedem Auftraggeber überlassen, eine unabhängige Prüfzelle – zum Beispiel den TÜV – mit einer verbindlichen Zertifizierung zu beauftragen. Die Anwendung der SOAA-Spezifikation ist allerdings auch keine „Plug & Play“-Lösung. Ein SOAA-Projekt muss hinsichtlich



seiner Umsetzbarkeit und der nachhaltigen Wirtschaftlichkeit individuell und unter Berücksichtigung vieler Faktoren neutral geprüft und vorbereitet werden.“

Bernd Lesemann ergänzt: „Es ist beim Kunden auch noch nicht gang und gäbe, dass er sein gesamtes elektronisches Schließsystem abgenommen haben will, Ein allgemeines Prüfsiegel existiert in dem Sinne also auch nicht.“

Dennoch wäre es individuell einzufordern, wie Volker Kraiss nachreicht: „Es

ist ja jedem Auftraggeber unbenommen, den TÜV zu beauftragen, sein System unabhängig zu prüfen. Das dauert dann eine gewisse Zeit und kostet einen bestimmten Betrag, aber am Ende bekommt der Betreiber ein Zertifikat für genau seine Anlage.“

Das sei in anderen Bereichen viel üblicher als in der Zutrittskontrolle, weiß Dietmar Vetten: „Bei Gaslöschanlagen lässt man die Systeme wesentliche häufiger vom TÜV begutachten, weil hier auch die Gefahr größer ist. Das machen sogar viele

Auftraggeber von sich aus, weil sie sicher gehen wollen, dass alles ordnungsgemäß installiert wurde.“

Es zeigt sich, dass das reine Entwerfen eines Standards und sein Niederschreiben als Spezifikation bei weitem nicht ausreichen, um ihm zum Durchbruch zu verhelfen. Man muss vor allem genügend Anbieter gewinnen, die ihn unterstützen und implementieren. Denn der Erfolg eines Standards steht und fällt mit der Akzeptanz im Markt und mit dem Nutzen, den er nachweislich bringt – das beinhaltet auch eine Nachprüfbarkeit durch Dritte. Letztlich müssen Anwender Standards einfordern und bereit sein, mit Pilotprojekten voranzugehen, damit die Verbreitung Fahrt aufnehmen kann. So bleibt es spannend zu beobachten, welche Rolle NFC, SOAA und Onvif im Zutrittssektor künftig spielen werden. MG



Artikel als PDF

www.sicherheit.info
Webcode: 1137668

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



Teilnehmer am ersten Tag des PROTECTOR Forums Zutrittskontrolle 2015.
 Sitzend von links: Manfred Golfes, Gerhard Haas, Volker Kunz, Jochen Becker, Axel Schmidt.
 Stehend von links: Jürgen Schneider, Wilfried Joswig, Robert Karolus, Christian Nagel, Moderator Boris Stamm, Kester Peter Brands, Chefredakteur Andreas Albrecht, Albrecht Kimmich, Thomas Weber, Carsten Hoersch, Sven Däberitz, Thomas Maier.

Bilder: MG

Wegweiser im Produktdschungel

Betreiber im Dickicht

Anwender, die ein neues Zutrittssystem planen oder ein altes aufrüsten möchten, sehen sich heute einer nie dagewesenen Fülle an Technologien und Produkten gegenüber. Ihr Wunsch ist klar: Das perfekte System für die eigenen Anforderungen finden. Doch der Weg dahin ist nicht selten verschlungen und steinig, da es an Orientierung im Produktdschungel fehlt.

levanz auf nahezu Null gesunken.“ Und Sven Däberitz von Intrakey ergänzt: „Vereinzelt kommt es vor, dass man Verweise auf den VdS in Ausschreibungen findet. Aber ich kann nicht sagen, dass Kunden direkt danach fragen, das kommt so gut wie nie vor.“

Das PROTECTOR Forum Zutrittskontrolle 2015 eröffnet mit einer Bestandsaufnahme, welche Wegweiser und Orientierungshilfen es am Markt gibt, und wie sie sich zum Wohle der Anwender nutzen lassen. Dabei zeichnet sich schon zu Beginn der Diskussion eines klar ab: Einstmals bedeutende Standards und viel zitierte Richtlinien entpuppen sich heute bestenfalls als ausgetretene Pfade durchs Technikdickicht. Moderator Boris Stamm formuliert es provokant: „Es gibt nach wie vor ein Druckstück des VdS, in dem manche Planer früher ihre heimliche Bibel sahen – die Richtlinie 2367 zur Planung von Zutrittskontrollanlagen. Aber heute fragt man sich schon: Welcher Hahn kräht noch danach? Findet

man diese Richtlinie noch in Ausschreibungen? Fordern sie die Kunden ein oder ist sie längst tot?“

Viel Widerspruch gibt es indes nicht. So erklärt Thomas Weber von Simonsvoss: „Diese VdS-Richtlinie ist hinsichtlich der vorgegebenen technischen Anwendung veraltet. Vieles vom dem, was heute gefordert wird, findet sich darin überhaupt nicht wieder. Nehmen wir einmal die starken Trends in Richtung IP-Technik und Ethernet-Verbindungen. Das wird künftig auch von den Endkunden klar bevorzugt werden.“ Ähnlich sieht es Gerhard Haas von PHG: „Die Richtlinie des VdS ist mit Sicherheit nicht schlecht als Anhaltspunkt, aber in der Praxis hatte sie schon früher nur wenig Bedeutung – heute ist die Re-

Schleichender Bedeutungsverlust

Die Gründe, warum sich die Richtlinien des VdS in der Praxis nicht behaupten können, scheinen vielfältig. Carsten Hoersch von Sesam skizziert seine Ansicht in Bezug auf Errichter: „Wir verkaufen größtenteils über Errichter-Partner, von denen wir damals auch einige für die Idee der VdS-Zertifizierung gewinnen konnten. Diese haben dann die Systemzulassung gemacht und sind zertifizierte Errichter für Zutrittskontrollanlagen geworden. Doch die Nachfrage und Notwendigkeit auf Kundenseite war derart gering, dass das Anerkennungsverfahren für Errichter mittlerweile wieder ausgelaufen ist. Es gibt also keine zertifizierten Errichter mehr – Geräte und Systeme aber schon.“



„Es gibt nach wie vor ein Druckstück des VdS, in dem manche Planer früher ihre heimliche Bibel sahen – die Richtlinie 2367 zur Planung von Zutrittskontrollanlagen. Aber heute fragt man sich schon: Welcher Hahn kräht noch danach? Findet man diese Richtlinie noch in Ausschreibungen, fordern sie die Kunden ein oder ist sie längst tot?“
Boris Stamm, Moderator des PROTECTOR Forums Zutrittskontrolle

„Es grenzt manchmal an Schizophrenie, wenn Ausschreibungen nicht nur das erste Mal aufgehoben werden, weil zu wenige Bieter da waren, sondern dann sogar noch ein zweites Mal aufgehoben werden müssen. Der Grund ist nicht selten, dass gleichzeitig verschiedenste Normen und Richtlinien erfüllt werden sollten, nicht nur BSI und VdS. Man muss hier realistisch sein und Kompromisse eingehen, ansonsten kriegt man nicht genügend Angebote und kann nicht vernünftig vergleichen.“

Axel Schmidt, Geschäftsführer, Salto Systems GmbH



Robert Karolus von Interflex fasst die Entwicklung folgendermaßen zusammen: „Früher war die Forderung nach VdS-Zertifizierungen sicherlich ein Trend gerade in Ausschreibungen im öffentlichen Bereich. Da gab es auch noch mehr Geräte, die vom VdS zertifiziert waren. Heute wird es nicht mehr so oft von den Unternehmen gefordert. Der finanzielle Aufwand einer Zertifizierung ist im Übrigen für die Hersteller nicht unerheblich.“

Trotz des guten Ansatzes des einstigen Verbandes der Sachversicherer sind die Schwierigkeiten seiner Zertifizierungen teilweise „hausgemacht“, wie auch Carsten Hoersch ergänzt: „Kurz und knapp formuliert, ist der VdS mit seiner Zertifizierung daran gescheitert, dass kaum ein Versicherer diese Anlagen überhaupt eingefordert hat.“ Das liegt in der Natur der Sache, findet Kester Brands von Tyco: „VdS ist im Bereich der Einbruchmeldeanlagen Pflicht. Die Versicherer gewähren auch entsprechende Rabatte und stellen diese Forderungen auf. Doch bei der Zutrittskontrolle ist es keine Pflicht, und es werden auch keine Rabatte gegeben oder es fehlen die

Die kleinmittelgroße Zutrittskontrolle



SCALA, die schlüssellose Zutrittskontrolle, passt einfach immer: Von der Einzeltür bis zur Absicherung mehrerer Türen. SCALA ist

beliebig erweiterbar und eignet sich für private, gewerbliche und öffentliche Objekte jeder Größe. www.assaabloy.de/scala



ASSA ABLOY

SCALA – die frei skalierbare Zutrittskontrolle.

ASSA ABLOY, the global leader
in door opening solutions



„Diese VdS-Richtlinie ist hinsichtlich der vorgegebenen technischen Anwendung veraltet. Vieles vom dem, was heute gefordert wird, findet sich darin überhaupt nicht wieder. Nehmen wir einmal die starken Trends in Richtung IP-Technik und Ethernet-Verbindungen. Das wird künftig auch von den Endkunden klar bevorzugt werden.“

Thomas Weber, Corporate Vice President Product Management, Simonsvoss Technologies GmbH

„Wie oft einem heute noch die Forderung nach einer VdS-Zertifizierung begegnet, hängt stark davon ab, mit wem man es auf Kundenseite zu tun hat. Manchmal sitzt dort ein Fachplaner, der die VdS-Richtlinie nach wie vor als Grundvoraussetzung sieht und die Klasse C als Ausschlusskriterium für Ausschreibungen verwendet. Damit nimmt er an, alle wesentlichen Anforderungen abgeprüft zu haben. Tatsächlich ist durch gestiegene Anforderungen speziell im Bereich der Konformität zu Unternehmensprozessen die Auswahl eines geeigneten Systems außerordentlich komplex geworden, deutlich vielschichtiger, als es die VdS 2358 aktuell vorsieht, und ein solch pauschales Vorgehen ist weder clever noch zeitgemäß.“



Jochen Becker, Leiter Business Development & Product Management, Primion Technology AG

entscheidenden Anreize. „Hinzu kommt, dass die VdS-Richtlinie stark auf die einstmals sehr proprietäre Welt der Zutrittskontrolle Bezug nimmt. Die Anbieter verlassen diese jedoch zunehmend und setzen auf offenere und interoperable Systeme.



Vielfältige Verschiebungen

Daraus resultiert eine Art Verschiebung in der Bedeutung von Zertifizierungs- und Regelungsinstanzen. Zusammen mit der Veränderung der Technik wandelt sich auch die Zertifizierungskompetenz. So ist logischerweise nicht mehr der VdS das Maß der Dinge, sondern eher das BSI (Bundesamt für Sicherheit in der Informationstechnik), das stärker auf IT-Standards setzt. Auch Common Criteria spielen je nach Anlagengröße und Internationalität des Kunden verstärkt eine Rolle.

Jürgen Schneider von NTP gibt zu bedenken: „Heute geht es in allen Sicherheitsbereichen stark in Richtung IT-Standards. Moderne Sicherheitsgewerke sind heute sehr eng verknüpft mit der IT-Welt. Man muss also auch die Sicherheit aus dieser Perspektive sehen und sich fragen: Wie kann man erreichen, dass eine Gefahrenmeldeanlage oder Zutrittskontrollsystem im Firmennetzwerk sicher verankert ist? Wenn es um die objektive Bewertung von End-to-end-Security geht, ist naturgemäß das BSI eine wichtige Anlaufstelle.“

Das bestätigt Robert Karolus: „Das Schlagwort BSI kommt heute immer wieder in Ausschreibungen vor, vor allem in

Verbindung mit der Sicherheit von Karten. Hier legen die Unternehmen großen Wert darauf, dass die Medien von einer unabhängigen Stelle zertifiziert wurden. Wenn sie also eine neue Technologie selektieren, soll diese die Common Criteria 4 erfüllen, damit sie die nächsten Jahre nicht gehackt werden kann. Es geht hier auch um Investitionsschutz.“

Dem Trend zugute kommt auch die Internationalität, wie Volker Kunz von HID Global anmerkt: „Das BSI hat in Verbindung mit Common Criteria auch nicht nur eine rein deutsche Bedeutung wie der VdS, sondern mindestens eine europaweite. Viele Unternehmen agieren heute global, und demnach richten sie sich mehr nach internationalen Standards.“

Stichwort Realitätsbezug

Ein Grundproblem von Richtlinien und Normen ist seit jeher, dass sie einen mehr oder weniger theoretischen Sollzustand beschreiben, der in der Praxis nur in Ausnahmefällen in Perfektion zu erreichen sein wird. So muss sich jede normative Instanz oder Zertifizierungsstelle fragen, wie praxistauglich ihre Anforderungen sind und was einer flächendeckenden Umsetzung möglicherweise entgegensteht.

So kritisiert Manfred Golfels von PCS Systemtechnik: „Ich habe den Eindruck, dass die Richtlinien des BSI insgesamt recht praxisfern sind. Es wurden zwar ein paar Aspekte aufgenommen, die darauf abzielen, Systeme besonders sicher zu machen, aber sonst vernachlässigt man vieles, was der Anwender wirklich braucht. Denn ich kenne keinen Anwender, der die hundertprozentige Sicherheit benötigt und diese auch bezahlen möchte. Vieles in diesem Regelwerk mag technisch möglich sein, geht aber an dem, was am Markt benötigt wird, vorbei.“





„Für uns als Leser-Hersteller besteht eigentlich fast keine Nachfrage nach VdS. Wir entwickeln und produzieren letztlich das, was der Markt nachfragt. Und meiner Meinung nach ist es auch viel wichtiger, ein sicheres Kartenverfahren und eine verschlüsselte Kommunikation zu verwenden, statt auf eine VdS-Richtlinie zu setzen, die diesen Aspekt so gut wie gar nicht abdeckt.“



Gerhard Haas, Bereichsleiter Datentechnik,
PHG Peter Hengstler GmbH + Co. KG

Auch Kester Brands plädiert für mehr Realismus angesichts manch haarsträubender Umsetzung von Systemen: „Wir treiben die Diskussion mit dem Verweis auf das BSI auf die Spitze. Man muss aber das Gesamtbild betrachten. Der verschlüsselte Leser und die hochsicheren Karten sind nur einzelne Bestandteile einer Lösung. Wenn man aber den Leser zur Absicherung einer Hochsicherheitstür in eine Gipskartonwand setzt, erübrigt sich jede Verschlüsselung. Wie man es dreht und wendet: Das Gesamtkonzept, die Lösung und Umsetzung beim

Kunden muss stimmig sein, sonst braucht man nicht über Hochsicherheit im Sinne von BSI oder VdS zu reden.“

Thomas Weber meint: „Nach meinem Kenntnisstand ist es so, dass sich das BSI hauptsächlich als das IT-Unternehmen des Bundes sieht. Dort beschäftigt man sich logischerweise mit Netzwerktechnologie und allem, was mit Datensicherheit zu tun hat. Gefährdungen, die in die Common Criteria hineinreichen, sind aber nicht primär Thema des BSI. Hier kann man sich aber zum Beispiel vom TÜV IT Nord entsprechend

zertifizieren lassen. Denn es nützt ja nichts, ein technisch hochsicheres System zu haben, wenn jemand abends immer wieder die Kellertür zum Lüften offen lässt.“

Geprüfte Sicherheit?

Damit wird klar: Niedergeschriebene Normen und Richtlinien sind wichtig. Doch ebenso wichtig ist deren praktische Anwendung und Prüfung. Hier mangelt es noch an Konsequenz, wie auch Moderator Boris Stamm findet: „Die Kernfrage bei allen



» AirKey – Das Smartphone ist der Schlüssel «

AirKey ist so dynamisch, wie die Bedürfnisse der Kunden. Bei AirKey werden Schlüssel per Internet verschickt. Weltweit und in Sekundenschnelle. Die Daten liegen dabei stets im hochsicheren EVVA-Rechenzentrum.



Jetzt AirKey gewinnen

» Am **Gewinnspiel** teilnehmen unter www.evva-airkey.com

Richtlinien lautet doch: Wer überprüft die Anwendung? Müssten sich nun BHE und VfS mit dem BSI und dem VdS zusammenschließen und etwas erarbeiten, das der TÜV vor Ort individuell prüft?“

Ein Teil davon ist – ohne Wertung des Realitätsbezugs – ja schon möglich, wie Jürgen Schneider anmerkt: „Der TÜV IT und andere zugelassene europäische Prüfstellen bieten solche Prüfungen an und beschäftigen sich intensiv mit den Zertifizierungen. Für einige große Telekommunikationsunternehmen wurden dort auch die Zertifizierungsprüfungen nach Common Criteria evaluiert. Das BSI bestätigt dies abschließend und veröffentlicht die Zertifizierungen.“

Diese Zertifizierungen sind momentan aber noch selten und betreffen eher große Konzerne mit speziellen Anforderungen. Für den Massenmarkt fehlt es noch an einem angepassten Geschäftsmodell beziehungsweise den entsprechend hohen Zahlen an Zertifizierungen, meint auch Axel Schmidt von Salto Systems: „Ich hätte gar nichts gegen einen unabhängigen Zertifizierer. Aber man sollte immer bedenken, dass auch Zertifizierer Unternehmen sind, die wirtschaftlich arbeiten müssen. Voraussetzung ist, dass man dort ein Businessmodell hinter der Zertifizierung von Zutrittssystemen sieht und sich genügend Betreiber dazu bereit erklären, diese durchzuführen.“

Wünschenswert wäre dies auch aus Kundensicht, wie Christian Nagel von Nedap findet: „Der Kunde braucht Anhaltspunkte für die Entscheidung und wünscht sich Gewissheit, dass sein System den Anforderungen entspricht. Und dazu müsste man am besten unabhängige Instanzen einbinden, um die Vergleichbarkeit zu erreichen, die der Kunde will.“

Rahmen und Augenmaß

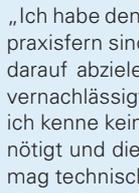
Anhaltspunkte für den Anwender sind sicher dringend nötig. Noch stammen diese in der Praxis aus verschiedenen Richtungen – sei es von aktuellen oder nicht mehr ganz aktuellen Richtlinien, von unabhängigen Planern und Beratern und natürlich auch von Herstellern, die oft starke Präsenz beim Kunden zeigen.

Thomas Maier vom SOAA-Gremium skizziert es folgendermaßen: „Eine eventuelle Problematik – nicht nur was Sicherheit betrifft – richtet sich beim Endkunden auch nach der Beratung und der Frage, wer



„Normen und Standards sind Anhaltspunkte für den Anwender, aber dieser muss sie auch einfordern. Denn viele Hersteller fürchten, dass gemeinsame Standards ihre Produkte am Ende austauschbar machen und proprietäre Alleinstellungsmerkmale verschwinden lassen. Wenn das Bedürfnis am Markt groß genug ist und die Anwender Interoperabilität einfordern, können sich Standards durchsetzen – vorausgesetzt, sie sind technologisch machbar.“

Jürgen Schneider, Nedap Technology Partner [nTp] for Security Management GmbH



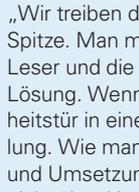
„Ich habe den Eindruck, dass die Richtlinien des BSI insgesamt etwas praxisfern sind. Es wurden zwar ein paar Aspekte aufgenommen, die darauf abzielen, Systeme besonders sicher zu machen, aber sonst vernachlässigt man vieles, was der Anwender wirklich braucht. Denn ich kenne keinen Anwender, der die hundertprozentige Sicherheit benötigt und diese auch bezahlen möchte. Vieles in diesem Regelwerk mag technisch möglich sein, geht aber an dem, was am Markt benötigt wird, vorbei.“

Manfred Golfes, Senior Produktmanager, PCS Systemtechnik GmbH



„Wir verkaufen größtenteils über Errichter-Partner, von denen wir damals auch einige für die Idee der VdS-Zertifizierung gewinnen konnten. Diese haben dann die Systemzulassung gemacht und sind zertifizierte Errichter für Zutrittskontrollanlagen geworden. Doch die Nachfrage und Notwendigkeit auf Kundenseite war derart gering, dass das Anerkennungsverfahren für Errichter mittlerweile wieder ausgelaufen ist. Es gibt also keine zertifizierten Errichter mehr – Geräte und Systeme aber schon.“

Carsten Hoersch, Geschäftsführer, Sesam Elektronische Sicherheitssysteme GmbH



„Wir treiben die Diskussion mit dem Verweis auf das BSI auf die Spitze. Man muss aber das Gesamtbild betrachten. Der verschlüsselte Leser und die hochsicheren Karten sind nur einzelne Bestandteile einer Lösung. Wenn man aber den Leser zur Absicherung einer Hochsicherheitsstür in eine Gipskartonwand setzt, erübrigt sich jede Verschlüsselung. Wie man es dreht und wendet: Das Gesamtkonzept, die Lösung und Umsetzung beim Kunden muss stimmig sein, sonst braucht man nicht über Hochsicherheit im Sinne von BSI oder VdS zu reden.“

Kester Peter Brands, Regional Manager Western Europe, Tyco Security Products

diese durchführt. Sehr häufig sind das Lieferanten, die vor Ort beraten. Doch wie tun sie das? Vermutlich nicht immer ganz objektiv und auch nicht umfassend im Sinne der IT. Dabei sollte der Fokus der Anwender auf der IT liegen, weil sich hier und heute die Sicherheit eines Firmenausweises entscheidet. Hier muss noch Aufklärungsarbeit geleistet werden.“

Jochen Becker von Primion Technology pflichtet bei: „Wir benötigen in jedem Fall eine anerkannte Referenz, auf welche man sich als Anbieter oder Anwender beziehen kann. Oftmals ist die Situation in Unternehmen so, dass ein Mitarbeiter zum Projektmanager für die Aus-

wahl und Einführung eines neuen Sicherheitssystems bestimmt wird. Dieser Mitarbeiter hat vielleicht keine ausreichende Erfahrung mit entsprechenden Systemen und muss sich auf einem Markt mit vielen Anbietern zurecht finden. Daher ist es auch gut, dass es Regelwerke wie VdS- oder BSI-Richtlinien gibt, die gewisse Grundlagen vorgeben.“

Realistisch ausschreiben

Nicht selten münden die Überlegungen zu einem neuen Zutrittssystem in einer mehr oder weniger realistischen Ausschreibung, mit der sich dann die Lieferanten und



Errichter konfrontiert sehen. Hier gibt es klaren Optimierungsbedarf, wie Wilfried Joswig vom Verband für Sicherheitstechnik (VfS) weiß: „Mein persönlicher Eindruck ist, dass im Moment Planung und Ausschreibung eher über Leistungsmerkmale von Technik getrieben werden als über Anforderungen von Richtlinien. Das ist ein abstruser Ansatz, denn ich bin nach wie vor der Meinung, dass man die Bedürfnisse der Nutzer ermitteln und dann daraus ableiten muss, welche Technik zum Einsatz kommt. Alles andere führt häufig dazu, dass der Kunde am Ende unzufrieden ist. Denn Richtlinien sind auch nicht immer auf die Gebräuchlichkeit von Systemen ausgerichtet, sondern eher hinsichtlich Verfügbarkeit und Stabilität.“

Albrecht Kimmich von Kaba ergänzt: „Vor allem beim Thema VdS und Ausschreibungen gab es immer wieder Konfliktpotenzial. Es wurden in der Vergangenheit öfter Ausschreibungen ins Leben gerufen, bei denen man alles 200 Prozent richtig machen wollte und sämtliche Normen aufgelistet hat, die zur Hand waren. Das ist absolut kontraproduktiv. Wir haben selbst auch nie die VdS-Zertifizierung in elektronischer Zutrittskontrolle durchlaufen, und wir haben dadurch kein Projekt verloren.“

Axel Schmidt berichtet ebenfalls von solchen Problemen bei Ausschreibungen: „Es grenzt manchmal an Schizophrenie, wenn Ausschreibungen nicht nur das

erste Mal aufgehoben werden, weil zu wenige Bieter da waren, sondern dann sogar noch ein zweites Mal aufgehoben werden müssen. Der Grund ist nicht selten, dass gleichzeitig verschiedenste Normen und Richtlinien erfüllt werden sollten, nicht nur BSI und VdS. Man muss hier realistisch sein und Kompromisse eingehen, ansonsten kriegt man nicht genügend Angebote und kann nicht vernünftig vergleichen.“

Man kann sich also weder blind auf Richtlinien verlassen noch auf die Beratung der Lieferanten. Die Anwender – und ihre eigenen Experten auch in Sachen IT – sitzen mit im Boot und sind für die nachhaltige Sicherheit und die Zuverlässigkeit der Systeme selbst mit verantwortlich. Alle Beteiligten sollten daran mitwirken, ihr Wissen zu vergrößern und die Qualität der installierten Anlagen hoch zu halten. MG



Artikel als PDF

www.sicherheit.info
Webcode: 1137665

„Ein Sicherheitssystem kostet nur Geld.“

Dass ist, was wir oft hören. Bis wir gemeinsam mit dem Kunden einen genaueren Blick auf seine Prozesse werfen. Und dann entdeckt er, dass unsere Workflow-Lösung seine Verwaltungsprozesse drastisch vereinfacht. Und wenn er hört, dass er seine bestehende Hardware behalten kann, wird es richtig interessant...

Vielleicht können wir auch Ihnen helfen?

Entdecken Sie unsere Lösungen auf www.nedapsecurity.com/de