www.gfos.com

ZU IHRER SICHERHEIT

GFOS liefert umfassende Sicherheitslösungen für die Sicherheit Ihres Unternehmens.

GFOS
Security – inspired by you.

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-Richtinie 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 diese 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 Lesemann 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

SALTO
inspiredaccess

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

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

DIGITALES ZUTRITTSMANAGEMENT IN GEBÄUDESYSTEMEN

SmartIntego – die perfekte Lösung für integrierte Zutrittskontrolle.

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

SimonsVoss technologies

„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 Onfiv wird es vorerst auch bei SOAA keine Zertifizierung geben. Sofern wirklich erforderlich, bleibt es natürlich jedem Auftraggeber überlassen, eine unabhängige Prüfstelle – 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 sichergehen 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**