TAS
SICHERHEITS- UND
KOMMUNIKATIONSTECHNIK

2022
Pressespiegel

www.tas.de

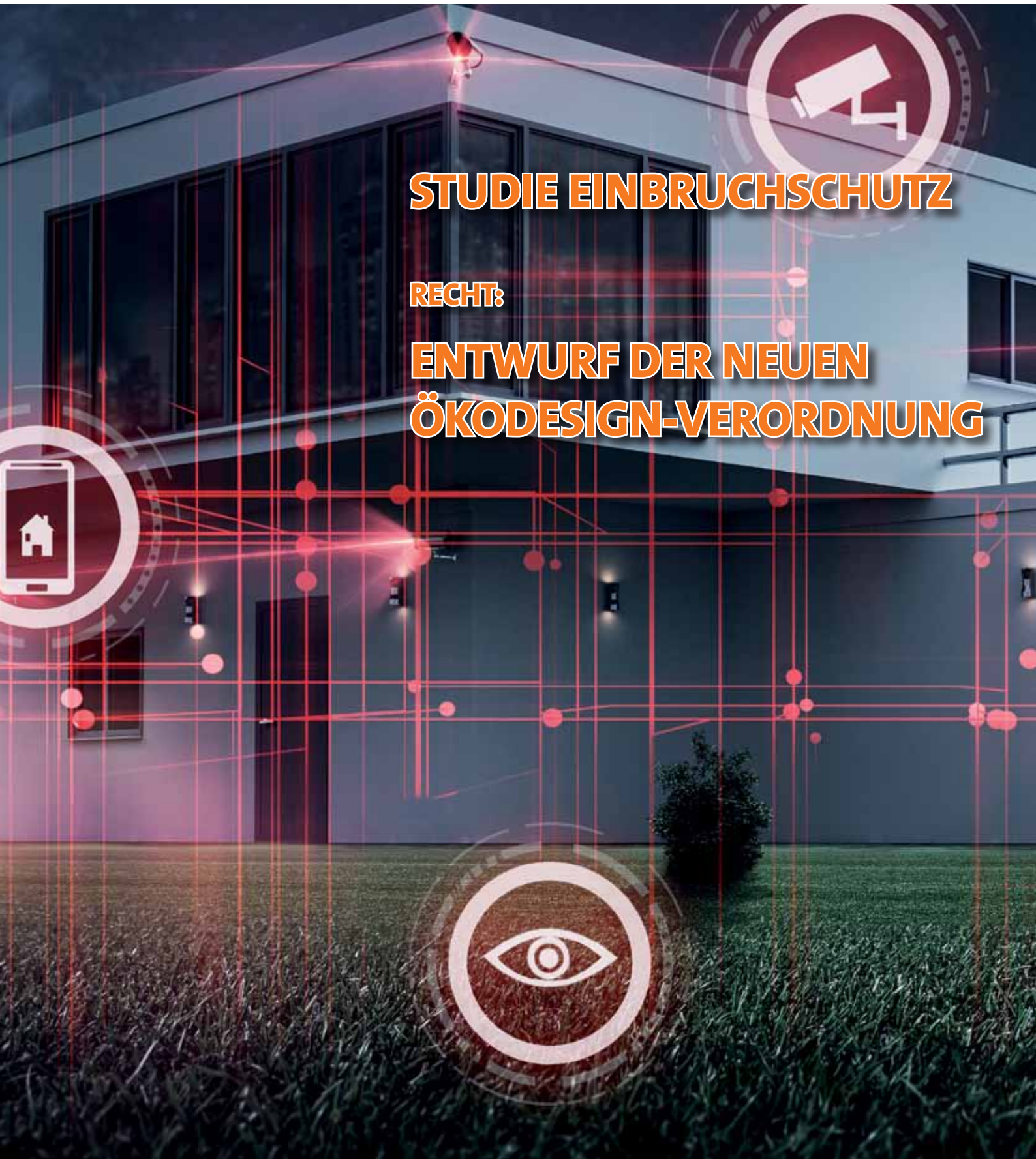
Artikel Unternehmen

22571 · ISSN 2191-9232 Einzelverkaufspreis: 16,- Euro

»SicherheitsPraxis

Fachzeitschrift für Errichterbetriebe, Gutachter, Planungsbüros und Systemhäuser

4 » November 2022 · www.prosecurity.de



STUDIE EINBRUCHSCHUTZ

RECHT:

ENTWURF DER NEUEN ÖKODESIGN-VERORDNUNG

Mobiliar erhöht die Sicherheit ihres Rechenzentrums

FASTCOM Technology SA kündigt die Fertigstellung des Projekts mit der Mobiliar für deren bestehendes Rechenzentrum an. Die Sicherheit musste gemäß der FINMA und interner Sicherheitsnormen erhöht werden. Der Metallbau der Schiebetüren wurde in Kooperation mit GILGEN door systems durchgeführt. Für eine optimale Sicherheit wurde die Lösung „SMACS FlexMat" in der Schleuse integriert und sichert gleichzeitig die Flüsse von Personen und Handgepäck.

Die Mobiliar betreibt ein eigenes Rechenzentrum. Um sich an neue interne Sicherheitsstandards sowie Anforderungen der FINMA anzupassen, muss die Zugangssicherheit zu diesem Rechenzentrum erhöht werden. Das Upgrade muss als Nachrüstung erfolgen, indem es sich harmonisch in die bestehende Infrastruktur integriert. Es müssen auch die Widerstandsklasse der Türen sowie deren Feuerwiderstand verbessert werden. Bei der Vereinzelungskontrolle soll sichergestellt werden, dass die Nutzer, wenn nötig, die Schleuse auch mit Material passieren können. Die Kontrolle erfolgt automatisch und spezielle Durchgangsprozesse wie z.B. VIP-Eintritte sollen adaptierbar sein. Außerdem soll die Schleuse komfortabel in der Nutzung sein und optimal an die Architektur des Gebäudes angepasst werden können.

Die SMACS FlexMat ist die Lösung, mit der die geforderten Spezifikationen erfüllt werden. Das SMACS-System integriert sich nahtlos in die bestehende Infrastruktur. Die Schleuse sichert gleichzeitig die Personen- und Materialflüsse. Spezielle Modi, inklusive Notausgangsmodus, und spezifische Durchgangsprozesse sind verfügbar.

www.fastcom-technology.com

Adam Stroud, CEO von Paxton, wird zu einem der 50 ehrgeizigsten Unternehmensleiter Großbritanniens für 2022 ernannt

Adam Stroud, CEO des internationalen Herstellers von elektronischen Sicherheitssystemen Paxton, wurde zu einem der LDC Top 50 Most Ambitious Business Leaders ernannt. Damit wird seine Leistung gewürdigt, Paxton auf seinem Weg zu internationalem Wachstum und Marktresistenz zu führen.

Die LDC Top 50, die in Zusammenarbeit mit der Times vergeben werden, würdigen die inspirierenden Führungskräfte, die hinter einigen der erfolgreichsten und am schnellsten wachsenden mittelständischen Unternehmen in Großbritannien stehen. In diesem Jahr erhielt LDC mehr als 750 Nominierungen, eine Rekordzahl im fünften Jahr der Preisverleihung.

Die Platzierung unter den Top 50 ist eine große Anerkennung für Adam, der 1996 im Unternehmen angefangen hat. In seiner Rolle als CEO seit 2012 hat Adam das Unternehmen zum Erfolg geführt. In dieser Zeit hat Paxton sein Produktportfolio erweitert und sich für kostenlose Errichterschulungen und einen erstklassigen Kundensupport eingesetzt, um sicherzustellen, dass die Kunden die besten Erfahrungen mit den Systemen von Paxton machen. Paxton konzentriert sich auch auf die Schaffung einer großartigen Unternehmenskultur und Arbeitsumgebung und wurde 2022 zum vierten Mal in den letzten fünf Jahren in die Liste der „Best Companies to Work For" aufgenommen.

Adam sagte: „Das Streben nach Weltklasse-Produkten und Kundenservice ist Teil unserer DNA. Ich glaube fest an die Kraft ehrgeiziger Ziele, die uns motivieren und ausrichten. Als Unternehmen sind wir entschlossen und leidenschaftlich bei dem, was wir tun." Und weiter: „Ich bin stolz darauf, in die LDC Top 50 Most Ambitious Business Leaders aufgenommen worden zu sein und Paxton bei dieser feierlichen Veranstaltung zu vertreten."

www.paxton-access.com/de/

Sicherheitsplattform für Fernzugriff – spezielle Konditionen für BHE-Mitglieder

Foto: Istock/Remote-support

Seit Kurzem erhalten BHE-Mitglieder Sonderkonditionen für den Fernzugriff auf Übertragungseinrichtungen (ÜE) sowie Gefahrenmeldeanlagen (GMA) über unsere Secure Platform. Durch den Fernzugriff lassen sich mögliche Störungen feststellen bzw. eingrenzen, wodurch Servicetechniker wesentlich effektiver eingesetzt werden können. Ein Einsatz vor Ort ist nicht mehr in jedem Fall notwendig. Das Ergebnis: kürzere Servicezeiten und damit eine Reduzierung von Servicekosten.

Als Basisdienst stellt die herstellerunabhängige Plattform, die auch an das BHE-Sicherheitsnetzwerk angeschlossen ist, eine sichere Verbindung zwischen dem Service-PC beim Errichter und den angebundenen Gefahrenmeldeanlagen her. Darüber hinaus lassen sich flexibel weitere Dienste, wie z. B. Monitoring verschiedener Alarmsysteme, buchen.

Als einziger in Deutschland durch den VdS zertifizierter RAISP übernehmen wir als *Remote Access Infrastructure Service Provider* die Verantwortung für die Sicherheit der Plattform. Die Benutzerintegrität wird durch Mehrfaktor-Authentifizierung und Verschlüsselungsverfahren gewährleistet.

www.tas.de

Security

Sicherheitsplattform für Fernzugriff mit speziellen Konditionen für BHE-Mitglieder

22.11.2022 - Für den Fernzugriff auf Übertragungseinrichtungen (ÜE) sowie Gefahrenmeldeanlagen (GMA) über die TAS Secure Platform erhalten BHE-Mitglieder Sonderkonditionen.

Durch den Fernzugriff lassen sich mögliche Störungen feststellen beziehungsweise eingrenzen, wodurch Servicetechniker effektiver eingesetzt werden können. Ein Einsatz vor Ort ist nicht mehr in jedem Fall notwendig. Das Ergebnis: kürzere Servicezeiten und damit eine Reduzierung von Servicekosten.

Als Basisdienst stellt die herstellerunabhängige Plattform, die auch an das BHE-Sicherheitsnetzwerk angeschlossen ist, eine sichere Verbindung zwischen dem Service-PC beim Errichter und den angebundenen Gefahrenmeldeanlage
sich flexibel weitere Dienste, wie z. B. Monitoring verschieden

TAS übernimmt als VdS-zertifizierter Remote Access Infrastructure Service Provider (RAISP) die Verantwortung für die Sicherheit der Plattform. Die Benutzerintegrität wird durch Mehrfaktor-Authentifizierung und Verschlüsselungsverfahren gewährleistet. Weitere Sicherheitsmaßnahmen sind unter anderem:

Foto: iSto

Für die Nutzung seiner Sicherheitsplattform mit Fernzugriff gewährt TAS BHE-Mitgliedern Sonderkonditionen.

UNTERNEHMEN 17. November 2022

TAS-Plattform: BHE bietet Mitgliedern spezielle Konditionen

Seit Kurzem erhalten BHE-Mitglieder Sonderkonditionen für den Fernzugriff auf Übertragungseinrichtungen (ÜE) sowie Gefahrenmeldeanlagen (GMA) der TAS-Sicherheitsplattform.

Durch den Fernzugriff der „Secure Platform“ lassen sich mögliche Störungen feststellen beziehungsweise eingrenzen, wodurch Servicetechniker wesentlich effektiver eingesetzt werden können. Ein Einsatz vor Ort ist nicht mehr in jedem Fall notwendig. Das Ergebnis: kürzere Servicezeiten und damit eine Reduzierung von Servicekosten.

Als Basisdienst stellt die herstellerunabhängige Plattform, die auch an das BHE-Sicherheitsnetzwerk angeschlossen ist, eine sichere Verbindung zwischen dem Service-PC beim Errichter und den angebundenen Gefahrenmeldeanlagen her. Darüber hinaus lassen sich flexibel weitere Dienste, wie zum Beispiel Monitoring verschiedener Alarmsysteme, buchen.

TAS gewährleistet umfangreiche Sicherheitsmaßnahmen

Als einziger in Deutschland durch den VdS zertifizierter RAISP übernimmt TAS als Remote Access Infrastructure Service Provider die Verantwortung für die Sicherheit der Plattform. Die Benutzerintegrität wird durch Mehrfaktor-Authentifizierung und Verschlüsselungsverfahren gewährleistet. Weitere Sicherheitsmaßnahmen sind unter anderem:

- Dokumentation aller Plattformzugriffe unter Berücksichtigung der Datenschutzvorgaben
- Mandantentrennung
- Systemschutz durch mehrere Firewalls, kontinuierliches Monitoring der Plattform und regelmäßige Penetrationstests
- Separater und sicherer 1:1 Zugang der ÜEs und Gefahrenmeldeanlagen auf die TAS Secure Platform

- Dokumentation aller Plattformzugriffe unter Berücksichtigung der Datenschutzvorgaben
- Mandantentrennung
- Systemschutz durch mehrere Firewalls, kontinuierliches Monitoring der Plattform und regelmäßige Penetrationstests
- Separater und sicherer 1:1 Zugang der ÜEs und Gefahrenmeldeanlagen auf die TAS Secure Platform

Kontakt

*TAS Sicherheits- und Kommunikationstechnik Telefonbau A. Schwabe GmbH & Co. KG

Langmaar 25
41238 Mönchengladbach
Deutschland

+49 2166 858 179
+49 2166 858 150

E-MAIL WEBSEITE

Verwandte Artikel

Eagle Eye Networks 2023 Trends in Video Surveillance

Foto: TAS

Um Router und IoT-Geräte vor Hacker-Angriffen zu schützen, hat TAS verschiedene Lösungen im Bereich der Übertragungstechnik entwickelt.

GEFAHRENMELDETECHNIK 1. September 2022

Schutz gegen Hacker-Angriffe auf Router und IoT-Geräte

Um Router und IoT-Geräte vor Hacker-Angriffen zu schützen, hat TAS verschiedene Lösungen im Bereich der Übertragungstechnik entwickelt.

Gegen Cyberangriffe durch Hacker geschützte und hochverfügbare Verbindungen sicherzustellen, ist das Kerngeschäft von TAS Sicherheits- und Kommunikationstechnik; auf der Security Essen präsentiert das Unternehmen verschiedene Lösungen und Innovationsprojekte im Bereich der Übertragungstechnik, um Router und IoT-Geräte entsprechend zu schützen. Hierzu gehören die bisher einzigen Übertragungseinrichtungen, welche nach Richtlinien für die Cybersicherheit von Systemen und Komponenten der Brandschutz- und Sicherheitstechnik durch den VdS zertifiziert wurden. Denn: Der Trend zur Vernetzung und Integration von komplexen Brandschutz- und Sicherheitsanlagen in eine smarte Gebäudeumgebung führt zu hohen Sicherheitsanforderungen im Hinblick auf Cyber-Security.

Router und IoT-Geräte vor Hacker-Angriffen schützen

TAS betreibt außerdem eine sichere und herstellerunabhängige Plattform für Remote Services. Auf dieser können verschiedene Sicherheitsgewerke für Monitoring und Fernwartung aufgeschaltet werden. Einzigartig ist nicht nur die Flexibilität, die TAS übernimmt hierbei auch die Verantwortung für die Cyber-Security. So ist das Unternehmen der bislang der einzige in Deutschland nach VdS-zertifizierte Remote Access Infrastructure Provider (Raisp). Eine weitere effiziente Lösung ist die direkte Anbindung von Sprechstellen für normkonforme Personennotruf- und Notfall-Gefahren-Reaktions-Systeme. Je nach Sprechstellen-Hersteller kann die NGRS-Lösung mit bis zu sechs Sprechstellen normkonform auch ohne Intercom oder zusätzliches IP-Gateway umgesetzt werden.

So gelingt sicherer Fernzugriff auf Gefahrenmeldeanlagen

Fernzugriff ist auch für Gefahrenmeldeanlagen inzwischen üblich. Dabei müssen allerdings mehre Aspekte beachtet werden, um die Sicherheit zu gewährleisten.

Artikel lesen

Ihre Kompetenz für sichere Alarmübertragung bringt das Unternehmen auch in Forschungsprojekten ein. Es entwickelt zum Beispiel ein zentrales Sicherheitsgateway für die Zusammenführung aller sicherheitsrelevanten Systeme im Gebäude sowie Lösungen zur Integration in intelligente 5G Netze.

Halle 7, Stand 7D17

77500

ISSN 1866-2420

SECURITY INSIGHT

FACHZEITSCHRIFT FÜR UNTERNEHMENSSICHERHEIT UND WIRTSCHAFTSSCHUTZ

September/Oktober
05/ 2022
EPr. 15,– €

www.prosecurity.de

Corona-Politik unterscheiden mochten, so einte sie die radikale Ablehnung der Medien und ihr Hass auf Journalisten. Ein Virus, der sich dem Schlesinger-Skandal bei uns auszubreiten droht.

„Fast jeder zweite Bundesbürger“, schreibt die „Berliner Zeitung“, „will wegen der hohen Energiepreise auf die Straße gehen, wenn es zu Demonstrationen kommt. Laut einer aktuellen Umfrage des Meinungsforschungsinstituts Insa sagten 44 Prozent aller Befragten, sie würden „sicher oder mit großer Wahrscheinlichkeit an Demonstrationen gegen die hohen Energiepreise teilnehmen“, wird „Bild“ zitiert. Auffällig: Rund 50 Prozent der FDP-Wähler „halten Proteste offenbar für notwendig und wollen an solchen Demos teilnehmen“, wie es heißt. Dabei war die FDP bei den Jungwählern zur Bundestagswahl noch der Renner gewesen. Der Wind dreht sich schnell in diesen Zeiten.

> „Jeder Zweite kann sich vorstellen, auf die Straße zu gehen.“

Die auslösenden Faktoren der Gelbwesten-Proteste in Frankreich klingen jedoch wie eine leise Ouvertüre zu dem was demnächst in Deutschland orchestriert werden soll – und wahrscheinlich auch wird. Deshalb sind Fratzschers mahnende Worte ernst zu nehmen. „Explodierende Mieten und ein steigendes Armutsrisiko in den letzten zehn Jahren, eine Spaltung bei Bildung und Gesundheit in der Pandemie und nun bei der Inflation könnte Deutschland vor eine soziale Zerreißprobe stellen“, befürchtet DIW-Chef Fratzscher. Auch andere Wirtschaftsführer zeichnen ein düsteres Bild. Deutsche-Bank-Chef Christian Sewing warnte laut „Handelsblatt“ im Juli auf einer Bankenkonferenz in Frankfurt, es bedrohe den sozialen Frieden in Deutschland, wenn in Umfragen 40 Prozent der Menschen angäben, sie könnten am Monatsende nicht mehr sparen. Die Lage könnte sich noch verschärfen.

Bundesinnenministerin Nancy Faeser gibt sich entspannt. In einer Talkrunde des Redaktionsnetzwerkes Deutschland bekannte sie: „Ich glaube nicht an Wutbürger und auch nicht an Gelbwesten-Proteste.“ NRW-Innenminister, Herbert Reul (CDU), verteilt inzwischen bereits die Etikettierung an die möglichen Protestierer. Er habe Sorge, so der Sender ntv, dass die Stimmung im Land schlechter wird und dass Themen wie der russische Krieg gegen die Ukraine, die Energiekrise und steigende Preise den Verschwörungsgläubigen neue Nahrung geben. „Es geht jetzt nicht mehr um Protestler, sondern es geht fast um so was wie neue Staatsfeinde, die sich da etablieren“, sagte er im „Frühstart“ von ntv.

Personalkarussell keine Lösung

In dieser Situation ist das Gebot der Stunde, die Lage zu entschärfen. Man muss dem Thüringischen Verfassungsschutzchef Kramer recht geben, wenn er – wie im Gespräch mit ZDFheute.de – die Auffassung vertritt: „Das Vertrauen der Bevölkerung in die staatlichen Institutionen und Behörden wird meines Erachtens entscheidend dafür sein, ob der soziale Frieden erhalten bleibt und wir diese Krise gemeinsam bewältigen.“ Diese Erkenntnis bleibt jedoch Allgemeinplatz, wenn die Umsetzung nicht konkret benannt und konsequent angegangen wird. Einmal kräftig am Personalkarussell zu drehen, mit der Hoffnung, jetzt die „richtigen“ Leute für die Ämter zu finden, ist mit Sicherheit eine wenig erfolgversprechende Idee.

Zweifellos hat das Land schon manche Krise und den einen oder anderen Skandal überstanden. Eine weitgehende Kontinuität des persönlichen Besitzstandes und vielleicht auch die Chance auf einen Zuwachs haben die Volksseele immer wieder im Zaum gehalten. Auch die vermeintliche oder tatsächliche Bedrohung während des Kalten Krieges schaffte so etwas wie eine übergeordnete Raison.

Die sich nun abzeichnende Lage steht unter einem anderen Stern. Und die Bedingungen haben sich geändert. Die bisher meinungsmachenden Medien büßen immer mehr an Einfluss ein. Der Blick auf die eigene Perspektive und das Verhalten der Verantwortlichen in Politik und Wirtschaft wird differenzierter. Fehlverhalten wird schärfer wahrgenommen.

Trigema-Chef Wolfgang Grupp prangert wohl deshalb nicht ganz ohne Grund, Verantwortungslosigkeit und Gier unter seinen „Kollegen“ an, wenn er im Gespräch mit der „Mainpost“ kritisiert: „Heute hört man oft: ‚Kein Problem, ich habe schon dreimal Insolvenz gemacht, es geht mir gut.‘ Wenn das so weitergeht, werden wir ein Desaster erleben.“

Die Gewerkschaften, Jahrzehnte für ihre Tätigkeit als SPD-gelenkte Ordnungsmacht gelobt, gehen mehr und mehr ihres Einflusses verlustig. Schon die französischen Gelbwesten haben gezeigt, dass auch ohne organisatorischen Kern eine Massenbewegung entstehen kann, die in der Regierung für weiche Knie sorgt.

Wenn diese nicht für einen sozial ausgewogenen Ausgleich der Belastungen sorgt, steht es um die innere Sicherheit nicht gut. Und am Ende könnte die Regierung sogar in die Knie gehen.

Peter Niggl

Schutz gegen Hacker-Angriffe auf Router und IoT-Geräte

Gegen Cyber-Angriffe geschützte und hochverfügbare Verbindungen sicherzustellen, ist das Kerngeschäft von TAS Sicherheits- und Kommunikationstechnik.

Auf den großen Messen der Sicherheitstechnik, Security Essen und Intersec Building in Frankfurt, präsentiert die TAS verschiedene Lösungen und Innovationsprojekte im Bereich der Übertragungstechnik. Hierzu gehören die bisher einzigen Übertragungseinrichtungen, welche nach Richtlinien für die Cyber-Sicherheit von Systemen und Komponenten der Brandschutz- und Sicherheitstechnik durch den VdS zertifiziert wurden. Denn: Der Trend zur Vernetzung und Integration von komplexen Brandschutz- und Sicherheitsanlagen in eine smarte Gebäudeumgebung führt zu hohen Sicherheitsanforderungen im Hinblick auf Cyber-Security.

Ebenfalls betreibt TAS eine sichere und herstellerunabhängige Plattform für Remote Services. Auf der Plattform können verschiedene Sicherheitsgewerke für Monitoring und Fernwartung aufgeschaltet werden. Einzigartig ist nicht nur die Flexibilität, die TAS übernimmt hierbei auch die Verantwortung für die Cyber-Security. So ist das Unternehmen das bislang einzige in Deutschland nach VdS-zertifizierte Remote Access Infrastructure Provider (RAISP).

Eine weitere effiziente Lösung ist die direkte Anbindung von Sprechstellen für normkonforme Personennotruf- und Notfall-Gefahren-Reaktions-Systeme.

Ihre Kompetenz für sichere Alarmübertragung bringt die TAS auch in Forschungsprojekten ein. Das Unternehmen entwickelt z. B. ein zentrales Sicherheitsgateway für die Zusammenführung aller sicherheitsrelevanten Systeme im Gebäude sowie Lösungen zur Integration in intelligente 5G Netze.

SECURITY ESSEN,
20. – 23. SEPTEMBER
HALLE 7, STAND 7D17

INTERSEC BUILDING IN FRANKFURT,
02. – 06. OKTOBER
HALLE 8.0, STAND J80

PROTECTOR

7-9|2022
September
50. Jahrgang

ASW Bundesverband –
Allianz für Sicherheit in der Wirtschaft e.V.

schlütersche
www.sicherheit.info

Security Essen 2022

Statements von Ma
Ausstellern und Ver
den der Leitmesse

Corporate Security 4

Studie zu Einflussfa
auf die Sicherheitswirt-
schaft | 86

t liefern handeln

Wie Hanwha Techwin Lieferunterbrechungen verhindert und gewissenhaft mi KI umgeht | 54

Foto: Hanwha Techwin

Foto: Genetec

Kay Ohse, Regional Sales Director Germany, Switzerland, Austria, Eastern Europe, Genetec GmbH.

triebs- und Marketingpläne kurzfristig umstrukturieren. Erschwerend kam hinzu, dass die Entwicklung der Pandemie nicht absehbar war. Wir haben uns daher im Jahr 2020 dazu entschlossen, eine eigene digitale Veranstaltung namens Connect DX durchzuführen, die unsere Erwartungen bezüglich Teilnehmern und Feedback weit übertroffen hat. Nichtsdestotrotz war in den vergangenen zwei Jahren aber auch erkennbar, dass digitale Events keine Live-Veranstaltungen ersetzen können. Ich bin mir daher sicher, dass es auch in Zukunft Präsenzveranstaltungen und Messen geben muss, um sich nicht aus den Augen zu verlieren. Der zwischenmenschliche Aspekt ist in der heutigen Zeit durch nichts zu ersetzen. Gleichzeitig haben wir aber auch gesehen, dass digitale Formate eine sehr große Akzeptanz erfahren haben. Das war vor der Corona-Krise nicht so. Nun stehen uns zwei Formate zur Verfügung, die Genetec in Zukunft nutzen wird, um je nach Anlass möglichst vielen Interessierten die Teilnahme zu ermöglichen. Um sich zukunftsfähig aufzustellen, sollten Veranstalter daher beide Formate im Portfolio haben und sinnvoll miteinander verknüpfen. In den nächsten Jahren werden daher vor allem kleinere hybride Veranstaltungen an Bedeutung gewinnen.

Was bietet eine Präsenzveranstaltung wie die Security, das der virtuelle Raum nicht leisten kann? Warum sind klassische Messen nach wie vor so gefragt?

» **Kay Ohse:** Der persönliche Kontakt auf Messen wie der Security zu Kunden, Partnern und Lieferanten ist durch nichts zu ersetzen. Wer sich einmal gegenüberstand, hat später auch per Telefon oder Web-Meeting ein ganz anderes Verhältnis miteinander. Darüber hinaus lassen sich Produkte und Lösungen vor Ort bedeutend einfacher präsentieren und entsprechende Rückfragen beantworten. In den vergangenen zwei Jahren haben wir aber auch eine gewisse Müdigkeit im Hinblick auf digitale Events beobachten können. Der im Vergleich zur Vor-Corona-Zeit große Andrang bei Präsenzveranstaltungen ist aus unserer Sicht maßgeblich auf dieses Phänomen zurückzuführen. Die Branche möchte sich endlich wieder direkt ins Gesicht schauen und sich über Trends und Innovationen austauschen.

Wie haben die vergangenen zwei Jahre Pandemie die Veranstaltungs- und Messelandschaft insgesamt verändert und wie wird sie sich künftig noch wandeln müssen, um zukunftsfähig zu sein?

» **Kay Ohse:** Die Pandemie kam für uns alle sehr überraschend. Bei Genetec mussten wir unsere Ver-

> „Der zwischenmenschliche Aspekt ist in der heutigen Zeit durch nichts zu ersetzen. Die Branche möchte sich endlich wieder direkt ins Gesicht schauen und sich über Trends und Innovationen austauschen."

Welche Innovationen erwarten Sie technologisch oder konzeptionell auf der Messe? Wo liegen die Trends unserer Zeit?

» **Kay Ohse:** In der traditionellen Sicherheitsbranche setzt sich nun die Erkenntnis durch, dass Digitalisierung weit mehr leisten kann als der klassische Ansatz, der auf isolierten Gewerken basiert. Die Grenzen der bisher getrennten Sicherheitsgewerke lösen sich auf. Einzelne Applikationen werden durch übergreifende Plattformen ersetzt oder in diese integriert. Anwender wünschen sich dabei volle Flexibilität, um schnell auf geänderte Anforderungen reagieren zu können. Zusätzlich ermöglicht das Einbetten dieser Plattformen in die IT-Infrastruktur, dass Sicherheits-Anwendungen und operative Prozesse voneinander profitieren können. Zudem können die gestiegenen Anforderungen besser adressiert werden, sei es der Einsatz von künstlicher Intelligenz, die Verbesserung der Cybersecurity, der Schutz der Privatsphäre oder die Einhaltung des Datenschutzes. Ich bin persönlich gespannt, wie dieser erweiterte Ansatz zur Digitalisierung von den unterschiedlichen Herstellern aufgegriffen und auf der Messe vorgestellt wird.

Halle 5, Stand 5C40

Genetec GmbH: www.genetec.com

Was bietet eine Präsenzveranstaltung wie die Security, das der virtuelle Raum nicht leisten kann?

» **Frank Lisges:** Der persönliche Kontakt zwischen Menschen bietet die Möglichkeit, gezielter aufeinander einzugehen. Fachliche Themen werden im Dialog ausgetauscht, sodass hier ein deutlich höheres Verständnis entsteht. Optik und Haptik können besser vermittelt werden. Und auch das ist wichtig: Es bleibt einfach mehr Raum für Spontaneität, Zwischenfragen und gemeinsame Ideenentwicklung. Die Interaktion findet auf verschiedenen Ebenen statt.

Wie haben die vergangenen zwei Jahre die Messelandschaft verändert?

» **Frank Lisges:** Ich gehe davon aus, dass wir zunehmend zu hybriden Veranstaltungen und Ausstellungen kommen werden. Einerseits muss die Möglichkeit der persönlichen Begegnung bestehen, anderseits müssen Produktneuerungen zeitnah und virtuell vermittelt werden.

Wie beurteilen Sie die Situation der Sicherheitsbranche angesichts weltweiter Krisen, Klimawandel, Rohstoff- und Fachkräftemangel?

» **Frank Lisges:** Als Unternehmen müssen wir weit über die Erfolgsrezepte vergangener Jahrzehnte hinausdenken. Es ist nicht mehr selbstverständlich, notwendiges Material „just-in-time" beschaffen zu können. Hier gilt es strategische Entscheidungen zu treffen, die eine verlässliche Verfügbarkeit sicherstellen, ohne dadurch betriebswirtschaftliche Grundsätze zu vernachlässigen. Politik und Unternehmen müssen mit hoher Priorität Berufe unterhalb der akademischen Ausbildung attraktiver machen. Auch die Kunden-Lieferantenbeziehung sollte deutlich partnerschaftlicher ausgerichtet werden, um sich gegenseitig zu unterstützen. Klimawandel und Energiekrise werden nach meiner Einschätzung dazu führen, dass sich die sicherheitstechnischen Gewerke deutlich auf diese Themen erweitern. Hier sei beispielsweise die sichere Übertragung von Gebäudedaten an „interessierte Stellen", wie Energieversorger, Abrechnungsstellen, Dienstleister genannt.

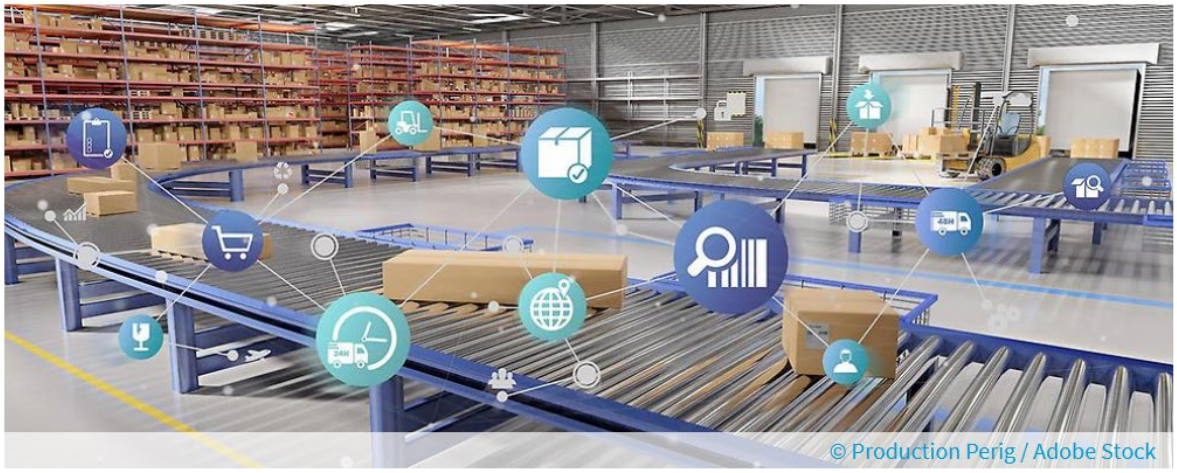
Foto: TAS

Frank Lisges, Geschäftsführer, TAS Sicherheits- und Kommunikationstechnik.

Halle 7, Stand 7D17

TAS Sicherheits- und Kommunikationstechnik: www.tas.de

Lehrgang zum Nachhaltigen Lieferkettenmanagement



Stand: **08.07.2022**

Die Industrie- und Handelskammer (IHK) Mittlerer Niederrhein hat in Kooperation mit der IHK Düsseldorf und der IHK Potsdam den bundesweit ersten Zertifikatslehrgang zum neuen Lieferkettengesetz entwickelt. Der Pilotlehrgang, der im März abgeschlossen und im Juni mit dem Deutschen Award für Nachhaltigkeitsprojekte 2022 in der Kategorie „Dienstleistung – Beratung / Schulung“ ausgezeichnet wurde, wird künftig den Unternehmen am Mittleren Niederrhein über das IHK-Weiterbildungsprogramm angeboten. Am Pilotlehrgang haben insgesamt neun Unternehmen teilgenommen. Dazu gehören auch die Scheidt & Bachmann GmbH und die Telefonbau Arthur Schwabe GmbH & Co. KG aus Mönchengladbach. IHK-Hauptgeschäftsführer Jürgen Steinmetz überreichte die Teilnahmezertifikate.

„Das Lieferkettensorgfaltspflichtengesetz wird viele Unternehmen vor Herausforderungen stellen“, sagt Steinmetz. Mit dem Zertifikatslehrgang gebe die IHK Unternehmen und ihren Mitarbeitenden eine Reihe von Werkzeugen an die Hand, um die gesetzlichen und gesellschaftlich steigenden Anforderungen an ein nachhaltiges Lieferkettenmanagement zu bewältigen.

„Nachhaltige Lieferketten spielen für die TAS als Unternehmen, das in internationalen Beschaffungs- und Absatzmärkten tätig ist, eine essenzielle Rolle. Als Wegbereiter für nachhaltige Lösungen ausgeklügelter Sicherheitskonzepte überprüfen wir auch unsere eigenen Prozesse und entwickeln sie weiter. Der neue Zertifikatslehrgang der IHK Mittlerer Niederrhein bietet uns hier einen großen Mehrwert“, sagt Stefan Koerfgen, Leiter Beschaffung / Produktion der Telefonbau Arthur Schwabe Telefonbau GmbH & Co. KG.

Das 2023 in Kraft tretende Lieferkettensorgfaltspflichtengesetz verpflichtet Unternehmen, direkt oder indirekt ihre Auswirkungen auf Menschen und Umwelt zu kennen, zu bewerten und in ihre Geschäftsentscheidungen, Kundenbeziehungen und Einkaufsprozesse einzubeziehen. Um diesen Anforderungen praktisch zu bewältigen, hat die IHK Mittlerer Niederrhein gemeinsam mit dem Programm „Business Scouts for Development“, der IHK Potsdam und der IHK Düsseldorf einen neuen IHK-Zertifikatslehrgang entwickelt, der sich an Mitarbeitende insbesondere aus den Bereichen Einkauf, Produkt-/Unternehmensentwicklung, Nachhaltigkeit/CSR und an die Geschäftsführung richtet. Der IHK-Zertifikatslehrgang ist branchenübergreifend konzipiert und richtet sich sowohl an die unmittelbar vom Gesetz betroffenen Großunternehmen als auch an kleine und mittlere Unternehmen (KMU), die als Lieferanten mittelbar betroffen sein können.

Mit Hilfe des Sorgfaltspflichten-Ansatzes (Due Diligence) zeigt der Lehrgang auf, wie ein ganzheitliches Nachhaltigkeitsmanagement in diesem Sinne aussehen kann. Der modulartige Aufbau ermöglicht den Teilnehmenden eine fachliche Vertiefung des Themas mit Praxisbezug und individueller Begleitung bis hin zur Umsetzung eines eigenen Projektes als fachpraktischen Leistungsnachweis.

Vier Termine stehen für den Online-Zertifikatslehrgang Nachhaltiges Lieferkettenmanagement (IHK) bereits fest (weitere Informationen und Anmeldemöglichkeiten sind unter den angegebenen Links zu finden): 6. September bis 9. Dezember 2022 (www.mittlerer-niederrhein.ihk.de/E042-ZX122); 11. Januar bis 28. April 2023 (www.mittlerer-niederrhein.ihk.de/E042-ZX123); 10. Mai bis 11. August 2023 (www.mittlerer-niederrhein.ihk.de/E042-ZX223) und 6. September bis 8. Dezember 2023 (www.mittlerer-niederrhein.ihk.de/E042-ZX323).

Bildunterschriften:

Bildunterschriften:
Foto 1: IHK-Hauptgeschäftsführer Jürgen Steinmetz (l.) überreichte im Beisein von Manuel Neumann (IHK-Business Scout, r.) das Teilnahmezertifikat an Stefan Koerfgen (Leiter Beschaffung / Produktion der Telefonbau Arthur Schwabe GmbH & Co. KG). Foto: IHK

Foto 2: Philipp Gockel (Contract Manager / In-house Lawyer bei der Scheidt & Bachmann GmbH, Mitte) hat seinen Zertifikatslehrgang abgeschlossen und von IHK-Hauptgeschäftsführer Jürgen Steinmetz (l.) im Beisein von Manuel Neumann (IHK-Business Scout) das Teilnahmezertifikat erhalten. Foto: IHK

Downloads

Telefonbau Arthur Schwabe GmbH & Co. KG

Größe: 330 kb **Download**

TAS SICHERHEITS- UND KOMMUNIKATIONSTECHNIK

‹ Zurück zur Übersicht

29.11.2022

Klimaziele erreichen durch Digitalisierung

Kategorie: Forschungsfeld 2, Gesamtprojekt, Veröffentlichung

Gebäude- und Prozesswärme sollen deutlich weniger Kohlendioxid freisetzen – in Privathaushalten genauso wie in der Industrie. Der Hebel für mehr Klimaschutz ist groß, schließlich entfällt fast die Hälfte des Gesamtenergieverbrauchs der EU auf Gebäude.

Neben der Substitution fossiler Energieträger wie Öl und Gas durch erneuerbare Energien sowie der Gebäudesanierung muss der Wärmebedarf insgesamt reduziert werden. Hierbei spielt die Digitalisierung eine wesentliche Rolle, um eine echte Wärmewende voranzutreiben. Gemeint sind intelligente Strom-, Wasser- oder Gaszähler, die den Wärmebedarf erfassen und optimieren. Seit April 2021 ist ein in Deutschland bislang einmaliges Forschungsprojekt gestartet – WärmewendeNordwest, kurz WWNW, das vom Bundesministerium für Bildung und Forschung (BMBF) bis zum Jahre 2025 gefördert wird. In dem Verbundvorhaben sind insgesamt 21 Partner, die in den verschiedenen Forschungsfeldern des Großprojektes Digitalisierungskonzepte für Gebäude, Campusareale und Quartiere in der Region Oldenburg/Bremen erarbeiten.

Intelligente Verbrauchssteuerung durch Smart Meter

War es früher der einfache analoge Stromzähler, wird es in Kürze ein „Smart Meter“ sein, der den Stromverbrauch erfasst. Dieser kann herausfinden, welche Geräte zu welchen Zeiten am meisten Strom verbrauchen und bietet dadurch die Möglichkeit der Steuerung. So können z. B.

- Stromerzeuger die Stromproduktion mit den Daten von Smart Metern zuverlässiger planen und sicherstellen
- Verbraucher ihre Smart-Home-fähigen Geräte optimieren
- Betreiber von Photovoltaikanlagen die Stromeinspeisung ins Netz überwachen und steuern, auch der Stromanbieter kann innerhalb festgelegter Regeln bestimmen, wann eingespeist werden kann und wann nicht

Datenaustausch muss sicher sein

Die Messdaten werden über ein Kommunikationsmodul – dem Smart Meter Gateway – übertragen. Ein integriertes Sicherheitsmodul sorgt dafür, dass sowohl der ständige Informationsfluss vor unberechtigten Zugriffen und Manipulation geschützt sowie der Datenschutz gewährleistet ist. Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) entwickelte daher das Bundesministerium für Sicherheit in der Informationstechnik (BSI) entsprechende Vorgaben an vertrauenswürdige Produktkomponenten – Smart Meter Gateways mit integriertem Sicherheitsmodul. Messsysteme, die nicht den Anforderungen des BSI entsprechen, dürfen in Zukunft nicht mehr verbaut werden.

Sichere Gateways und Router als Grundlage für Mehrwertdienste

SiGRun (Sichere Gateways und Router als Grundlage für Mehrwertdienste) ist eines der Teilprojekte der WärmewendeNordwest. In diesem Projekt geht es um die Weiterentwicklung der technologischen Infrastruktur für weitere Einsatzbereiche. Die Nutzung soll nicht nur auf Stromdaten beschränkt sein, das Ziel ist die Kopplung verschiedener Sektoren der Energiewirtschaft wie Strom, Wärme und Kälte. Und darüber hinaus: Neben den Sektoren Elektrizität und Wärmeversorgung wird auch die Gebäudeüberwachung zur Optimierung des Gesamtsystems mit einbezogen. Besonders für die Wohnungswirtschaft sind neben der Erfassung der Verbrauchswerte auch weitere Gebäudedaten und –dienste von Interesse. Dabei werden zunächst verschiedene Use Cases und die Anforderungen an einen Sektor übergreifenden Einsatz der Technologie ermittelt. Hierzu gehören beispielsweise die Analyse von Smart Home Anwendungen sowie Personen-Notruf oder Brand-, Einbruch- und Überfallmeldungen. Gerade hier – bei den Sicherheitsketten für verschiedene Alarmbearbeitungen – baut man auf etablierte Techniken und Normen auf, die auch für Smart Meter Gateways genutzt werden können.

Smarte Services brauchen höchste Sicherheit

Die Zielsetzungen des Forschungsprojektes SiGRun sind ambitioniert. Einerseits soll der Anwendungsbereich von Smart Meter Gateways erweitert werden, um Insellösungen zu vermeiden, bei denen Router bzw. Gateways verschiedener Sektoren zum Einsatz kommen. Auf der anderen Seite: Je mehr Verbindungen durch offene bzw. flexible Schnittstellen geschaffen werden, umso höher sind die Anforderungen an Ausfallsicherheit und Schutz gegen Angriffe bei der gesamten Datenübertragung. Es kommt nicht von ungefähr, dass *TAS Sicherheits- und Kommunikationstechnik* als Spezialist für die sichere Alarmübertragung und Mitglied in verschiedenen Normausschüssen, einer der Teilnehmer des Forschungsprojekts SiGRun ist. Übertragungsgeräte der TAS gehören seit Langem zum Standard im Markt für die sichere Übertragung von Alarmmeldungen, die auch im BOS-Bereich (Behörden und Organisationen mit Sicherheitsaufgaben) anerkannt sind. Zudem hat das bundesweit tätige Unternehmen eine Plattform für den sicheren und herstellerübergreifenden Remote Access von Gefahrenmeldeanlagen entwickelt, die erfolgreich bei Großkunden und Leitstellenbetreibern eingesetzt wird. Die Erfahrungen aus diesen Bereichen wird das Unternehmen insbesondere bei der Definition der Schnittstellen für

die Sektorenkopplung, der kompletten Planung und Erstellung einer Hardware- und Embedded Software Systemarchitektur, den Bau eines Prototypen für ein Smart Meter Gateway sowie bei der Anbindung des sog. „Smart Meter Gateway Admin" einbringen. Dabei sollen die Standards aus der Sicherheitskette für Alarmmeldungen beim Datenaustausch genutzt werden – ein breites Feld neuer Geschäftsmodelle auf Basis der Gateways kann sich hiermit eröffnen!

Dieser Artikel wurde in der Juli/August-Ausgabe der Fachzeitschrift für Unternehmenssicherheit und Wirtschaftsschutz Security Insight unter https://www.sicherheit.info/energieeinsparung-durch-digitalisierung veröffentlicht und ist hier auch als PDF zu finden: Download.

Mehr Informationen erhalten Sie auf der Website von TAS: https://www.waermewende-nordwest.de/klimaziele-erreichen-durch-digitalisierung/

Autor:in

Anke Staupendahl
Telefonbau Arthur Schwabe
Mitarbeiterin FF2
Anke.Staupendahl@tas.de
www.tas.de

‹ Zurück zur Übersicht

16.02.2022

Drei Fragen an...TAS

Kategorie: Forschungsfeld 2, Gesamtprojekt

TAS
SICHERHEITS- UND
KOMMUNIKATIONSTECHNIK

*In dieser Beitragsreihe stellen wir Ihnen das Projektkonsortium der Wärmewende Nordwest etwas genauer vor: Welche fachliche Expertise bringen die einzelnen Partnerinnen und Partner mit? Was ist ihre Rolle im Projekt? Wie reflektieren sie die Bedeutung von Wärmewende Nordwest für ihr Arbeitsgebiet und für die Region? Hier finden Sie Antworten und Ihre Ansprechpartner*innen.*

Was sollten wir zum TAS wissen?

TAS Sicherheits- und Kommunikationstechnik ist ein Hersteller von Kommunikationselektronik und ein Dienstleistungsunternehmen, das Überwachungs- und Sicherungsanlagen für Liegenschaften plant und installiert.

Kunden sind schwerpunktmäßig überregionale Unternehmen mit lokalen Filialen, wie z. B. Banken, Tankstellen und die Systemgastronomie. Im vergangenen Jahr startete als weiterer Dienstleistungsbereich die „TAS Secure Platform“, eine innovative Cloud-Lösung zur sicheren Fernwartung von Alarmanlagen durch autorisierte externe Marktteilnehmer wie z. B. mittelständische Errichterbetriebe.

Als Hersteller bietet TAS innovative Kommunikationsprodukte für Marktsegmente mit Sicherheitsbedarf an, die von großen Konzernen nicht adäquat bedient werden. Dafür unterhält TAS eine große Entwicklungsabteilung, die von der Hardware- und Softwareerstellung über die mechanische Konstruktion bis zum serienreifen Produkt alles im Griff hat und den gesamten Produktlebenszyklus, auch über viele Jahre hinweg, qualitätsbewusst begleiten kann. Eine eigene Fertigung am Standort Mönchengladbach mit hoher Fertigungstiefe ermöglicht flexible Reaktionen auf Kundenwünsche und Marktänderungen.

Woran arbeitet ihr konkret im Projekt?

Im Projekt Wärmewende Nordwest (WWNW) hat TAS gemeinsam mit den Partnern im Forschungsfeld 2 (FF2) die Aufgabe übernommen, das bereits erarbeitete Know-How der sicheren Übertragung von Brand-, Einbruch-, Überfall- und Personennotruf- Meldungen in die Roadmap des BMWi zur Digitalisierung der Energiewende einzubringen. Die spezielle Aufgabe für TAS besteht darin, gemeinsam vom BSI und VdS zugelassene Kommunikationsadapter für SMGW mit integrierter, normkonformer Alarmübertragungseinrichtung zu entwickeln und zu fertigen. Diese sollen dann im Feldversuch zum Einsatz kommen, der im weiteren Projektverlauf geplant ist.

Darüber hinaus gilt es, die bereits von TAS am Markt etablierte Cloud-Plattform für die Fernwartung von Alarmanlagen mit dem Smart-Meter-Gateway-Admin und dessen Fernzugangs-Plattform zu synchronisieren, eine Aufgabe, die in der Querschnittsaktivität 1 (QA1) zu bearbeiten ist.

Welchen Beitrag leistet ihr durch eure Arbeit, um die Klimaziele erreichen zu können?

Entscheidend für die Akzeptanz von Produkten und Systemen, die dabei helfen, die Klimaziele zu erreichen, ist ein gutes Kosten-/Nutzen-Verhältnis. Es kommt also darauf an, dass durch die Digitalisierung der Energiewende keine zusätzlichen Kosten entstehen, vielleicht sogar für den Verbraucher ein Kostensenkungspotenzial generiert werden kann. Dem steht entgegen, dass elektronische Gateways mit Internetanschluss einen „digitalen Hauszugang" darstellen, der mindestens so gut gegen Einbruch (Cybercrime) geschützt werden muss wie die physische Haustür mit ihrem Türschloss. Trotz höchster Sicherheitsanforderungen muss dieser „elektronische Hauszugang" jedoch mit akzeptablen Kosten bereitgestellt werden. Gelingen kann das nur bei gemeinsamer Nutzung von vielen Gewerken im Gebäude (Sektorkopplung). Bereits installierte Sicherheits-Infrastruktur bei bestehenden oder von der Bauordnung vorgeschriebenen Alarmanlagen/ Brandmeldeanlagen könnte hier mittels preiswert zu realisierendem Upgrade zu einer sinnvollen Sektorkopplung beitragen.

Ein gemeinsam genutzter Sicherheitsrouter für alle Gewerke ist also ein wesentlicher Beitrag zur Kostenreduktion bei gleichzeitigem Sicherheitsgewinn und somit zur Akzeptanz von Systemen zur CO_2-Reduktion. Eine wichtige Aufgabe des Projektes ist daher, mit intensivem Marketing und verstärkten Normungsaktivitäten im Projekt, diese Akzeptanz auch in Industrie und Handwerk zu fördern.

Autor:in

Stefan Vieten
Telefonbau Arthur Schwabe
Mitarbeiter FF2
stefan.vieten@tas.de
Fon: +49 2166 858 182

Fachbeiträge

ALARMSYSTEME

Hacker kommen auch Remote nicht rein

Sicherer Remote Zugang: Erfolgreiche Zertifizierung nach VdS 3836 für Übertragungsgeräte von TAS

Cyberangriffe auf IT-Systeme sind alltägliche Praxis. Wenn auch längst nicht alle, so sind doch viele Unternehmen mittlerweile so gut geschützt, dass sie direkte Angriffe abwehren können. Die Gefahren lauern aber auch woanders – z. B. bei Cyberangriffen auf IoT-Geräte. Hier kann Cybersicherheit nicht immer gewährleistet werden. Und das, obwohl der Datenaustausch durch die zunehmende Vernetzung der softwarebasierten Komponenten steigt.

Ein Einfallstor für Hacker ist beispielsweise der Remote Zugriff auf Anlagen und Produkte über einen konventionellen Router. Für einen direkten Fernzugriff müssen in der Firewall des Routers Ports freigegeben werden, über welche die Kommunikation zur Übertragungseinrichtung weitergeleitet wird. Mit jedem geöffneten Port steigt jedoch das Risiko, angreifbar zu werden. Wenn zudem unsichere Kennwörter verwendet werden und/oder die Software der Endgeräte veraltet ist, haben selbst weniger versierte Cyberkriminelle leichtes Spiel beim Zugang zum System. Nicht nur im Bereich der kritischen Infrastruktur kann dies fatale Folgen haben. Wenn Alarme nicht mehr übertragen werden können oder Anlagen stillstehen, weil Kernkomponenten ausfallen, ist die Sicherheit von Menschen, Unternehmenswerten und Gebäuden bedroht.

Was macht einen Remote Zugang sicher?

Bei der Sicherheit von Systemen und Produktkomponenten mit Netzwerkfunktionalität kommt es darauf an, eine sichere und ständig verfügbare Kommunikation mit 24/7 Überwachung der Leitungswege zu gewährleisten, den Schutz der Datenintegrität sicherzustellen und den Zugriff zu kontrollieren. Bei Remote Services müssen dabei sowohl die Übertragungsgeräte selbst als auch die Plattform für den Fernzugriff gegen Cyberangriffe optimal geschützt werden. Für beides hat das Unternehmen TAS Sicherheits- und Kommunikationstechnik eine Lösung. Der Spezialist in der Übertragungstechnik bietet ein sicheres Gateway für die Übertragung von Alarmen, Sprache und (Monitoring-) Daten sowie eine sichere Infrastruktur für den Remote Access an.

◀ VdS übergibt erstes VdS 3836-Zertifikat für Komponenten der Brandschutz und Sicherheitstechnik. (v.l.n.r.) Christoph Schäfer, Produktmanager der TAS, Günter Grundmann Abteilungsleiter im VdS-Labor für elektronische Sicherungstechnik und Daniel Kaumanns, verantwortlicher Produktmanager für die TAS Secure Platform

„Unser Ziel war es, eine ganzheitlich sichere Lösung für Remote Services anbieten zu können."

Daniel Kaumanns,
Produktmanager TAS Secure Platform

Cybersicherheit der Übertragungsgeräte

Die von TAS entwickelten Übertragungsgeräte TAS-Link IV und Siro-Port sind die ersten in Deutschland, die nach VdS 3836 zertifiziert sind – eine Anerkennung der Cybersicherheit für Komponenten der Brandschutz- und Sicherheitstechnik. Die VdS 3836 wurde im Abgleich mit verschiedenen Richtlinien erarbeitet: dem IEC 62443 zur IT-Sicherheit für Netze und Systeme, dem Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft zu den Anforderungen an Smart Home Installationen sowie der ETSI TS 103 645 – Cyber Security for Consumer IoT.

Durch das proprietäre Betriebssystem können die Zugriffsmöglichkeiten von vornherein auf die Ports beschränkt werden, die auch wirklich benötigt werden. Außerdem unterstützt die neue Generation von TAS-Link und Siro-Port auch IPsec für die verschlüsselte Datenübertragung und bietet weitere Sicherheitsfeatures.

Sichere Plattform für Remote Access

Eine VdS-Zertifizierung hat die TAS bereits im letzten Jahr für ihre im Hause entwickelte TAS Secure Platform erhalten. Damit ist das Unternehmen der erste Remote Access Infrastructure Provider (RAISP), der in Deutschland durch VdS zertifiziert wurde. Erfüllt wurden nicht nur die hohen Sicherheitsanforderungen an die Infrastruktur der Fernzugriffsplattform, sondern auch die Anforderungen an den Service Provider. Dieser ist verantwortlich für sichere, ständig verfügbare Verbindungen und Schutz gegen Cyberangriffe. Bislang fehlte es an der klar geregelten Verantwortung beim Fernzugriff auf Alarmsysteme – mit der Folge von Haftungsrisiken für die Betreiber. Mit den kommenden Normen TS 50136-10 für Remote Access und EN 50710 für Remote Services ändert sich dies zukünftig.

Für Daniel Kaumanns, verantwortlicher Produktmanager für die TAS Secure Platform, sind beide VdS-Zertifizierungen ein Gütesiegel für die Cyber-Sicherheit in der Übertragungstechnik. „Unser Ziel war es, eine ganzheitlich sichere Lösung für Remote Services anbieten zu können – angefangen bei der Infrastruktur über Gateways bis hin zur Verantwortungsübernahme für den sicheren Fernzugriff auf Gefahrenmeldeanlagen. Kunden, die unsere Plattform sowie flexibel buchbare Services nutzen, bezahlen monatlich nur für die Remote Dienste, die auch benötigt werden. Es muss weder in eine eigene Infrastruktur noch in den Betrieb oder in die Weiterentwicklung investiert werden." ●

Messe-Highlights

Auf der Security Essen (20.–23. September) und der Intersec Building in Frankfurt (2.-6. Oktober) präsentiert TAS verschiedene Lösungen und Innovationsprojekte im Bereich der Übertragungstechnik:

- VdS-zertifizierte Übertragungseinrichtungen nach Richtlinien für die Cybersicherheit von Systemen und Komponenten der Brandschutz- und Sicherheitstechnik
- Herstellerunabhängige Plattform für Remote Services, auf die verschiedene Sicherheitsgewerke für Monitoring und Fernwartung aufgeschaltet werden können
- Lösung zur direkten Anbindung von Sprechstellen für normkonforme Personennotruf- und Notfall-Gefahren-Reaktions-Systeme

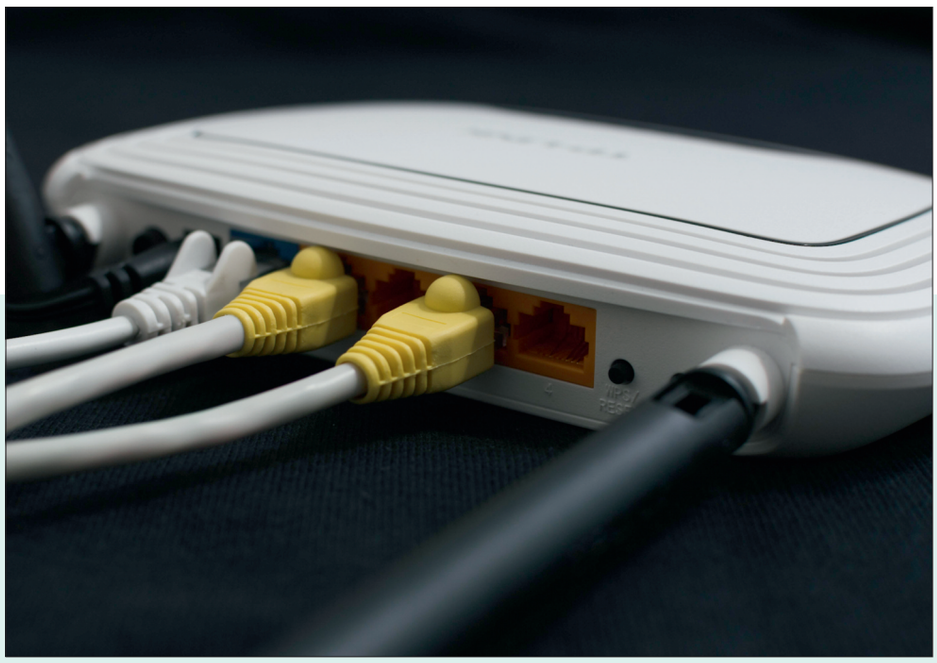
Security Essen:
Halle 7, Stand 7D17

Intersec Building in Frankfurt:
Halle 8.0, Stand J80

TAS Sicherheits- und Kommunikationstechnik
Mönchengladbach
Tel.: +49 2166 858 0
info@tas.de
www.tas.de

Erste VdS-Zertifizierung für Cyber-Sicherheit bei Übertragungsgeräten

Funktionale IT-Sicherheit dank VdS 3836 – den Hackern ein Schnippchen schlagen



Durch die ständige Verbindung mit dem Internet müssen auch Gefahrenmeldeanlagen angemessen geschützt sein (Foto: Lorenzo Cafaro via Pixabay)

Dass das Internet kein sicherer Ort ist, weiß inzwischen auch jeder Laie. Das ganze Ausmaß der Bedrohungen wird jedoch auch von Experten gerne verdrängt. Tagtäglich steigt die Zahl der bekannten Sicherheitslücken und dementsprechend auch die der Schadsoftwares, die diese Lücken ausnutzen können. Althergebrachte Schutzmaßnahmen wie Virenscanner und Firewalls reichen da allein nicht mehr aus, wenn sensible Bereiche geschützt werden sollen. Besonders bei vernetzten Geräten im Bereich des „Internet of Things" (IoT) lässt die Cyber-Sicherheit oft zu wünschen übrig. s+s report sprach mit Daniel Kaumanns von TAS und Sebastian Brose von VdS über dieses aktuelle Thema und über adäquate Lösungen.

s+s report: Fangen wir zunächst ganz grundlegend an: Wie kann man sich einen Hacker-Angriff auf Anlagen und Produkte der Sicherheitstechnik vorstellen? Und welche Folgen kann so ein Angriff haben?

Daniel Kaumanns: Hacker können beispielsweise den Remote-Zugriff auf Anlagen und Produkte nutzen. Dieser Remote-Zugriff wird eingerichtet, damit der Errichter oder der Betreiber aus der Ferne die Anlage, etwa eine Einbruchmeldeanlage, konfigurieren oder warten kann. Dazu muss diese Anlage mit dem Internet verbunden sein, was in der gängigen Praxis leider meist über einen konventionellen Router geschieht. Für einen direkten Fernzugriff werden noch heute einfach Ports im Router selbst freigegeben, über die die Kommunikation zur Übertragungseinrichtung weitergeleitet wird. Mit jedem geöffneten Port steigt jedoch das Risiko, angreifbar zu werden. Wenn zudem unsichere Kennwörter verwendet werden und/oder die Software der Endgeräte veraltet ist, haben selbst weniger versierte Cyber-Kriminelle leichtes Spiel beim Zugang zum System.

Sebastian Brose: Nicht nur im Bereich der kritischen Infrastruktur kann dies fatale Folgen haben. Was passiert etwa, wenn eine Einbruchmeldeanlage Alarme nicht mehr übertragen kann? Oder wenn komplette Anlagen stillstehen, weil Kernkomponenten ausfallen? Hier ist die Sicherheit von Menschen, Unternehmenswerten und Gebäuden bedroht!

s+s report: Angesichts dieser Bedrohungslage stellt sich die Frage: Was zeichnet einen sicheren Remote-Zugang aus?

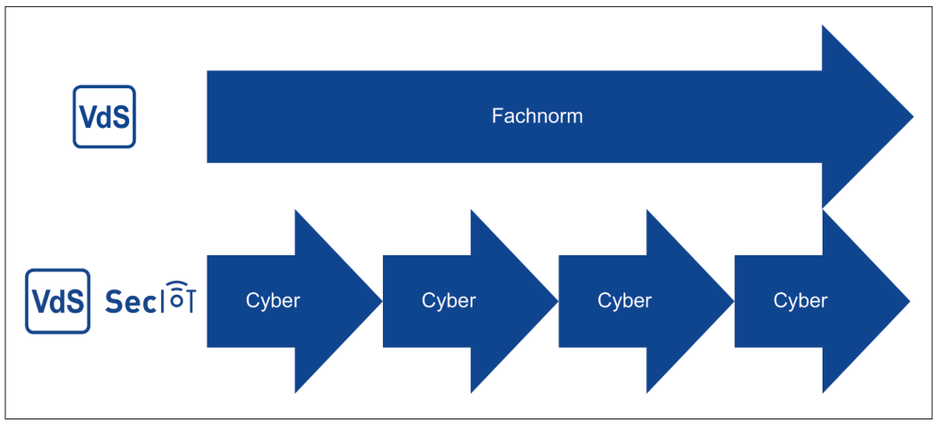
Sebastian Brose: Dass einfach Ports im Router freigegeben werden, sollte ein für alle Mal der Vergangenheit angehören. Stattdessen sollen sichere Konstrukte genutzt werden, beispielsweise mit einem Trust-Anchor, einer Art Vermittlungsstelle oder Plattform im Internet, zu der

sich beide Seiten aktiv verbinden. Neben der Systemarchitektur mit beispielsweise einer sicheren Plattform müssen auch die Komponenten wie die Übertragungseinrichtung optimal geschützt werden.

Die Übertragungseinrichtung ist ja nicht nur für den Fernzugriff immer online, sondern in erster Linie für die Alarmübertragung. Für beides hat das Unternehmen TAS Sicherheits- und Kommunikationstechnik eine VdS-anerkannte Lösung: ein sicheres Gateway für die Übertragung von Alarmen, Sprache und (Monitoring-)Daten sowie eine sichere Infrastruktur für den Remote Access.

s+s report: Herr Kaumanns, welche Übertragungsgeräte Ihrer Firma tragen das VdS-Siegel?

Daniel Kaumanns: Die von TAS entwickelten Übertragungsgeräte TAS-Link IV und SIRO-Port sind die ersten in Deutschland, die nach VdS 3836 zertifiziert sind und somit das SecIoT-Siegel tragen dürfen. Dieses Siegel zeichnet eine besondere Eignung der Cyber-Sicherheit für Komponenten der Brandschutz- und Sicherheitstechnik aus. Durch das proprietäre Betriebssystem können die Zugriffsmöglichkeiten von vornherein auf die Ports beschränkt werden, die auch wirklich benötigt werden. Neben diesem Schutz durch „Security by Design“ unterstützt die neue Generation von TAS-Link- und SIRO-Port-Übertragungsgeräten auch das Protokoll IPsec für die verschlüsselte Datenübertragung und bietet weitere Sicherheitsfeatures, die dem höchsten Level der Cyber-Security entsprechen. Ein unberechtigter Zugriff auf die Übertragungsgeräte ist damit nahezu unmöglich.



Produkte müssen bzgl. Cybersicherheit schnelleren Überarbeitungszyklen folgen (Grafik: VdS)

s+s report: Die zertifizierte Technik ist aber nur ein Baustein für eine sichere Einrichtung des Fernzugriffs. Welche weiteren Komponenten sind wichtig?

Sebastian Brose: Wie vorhin bereits angedeutet: Die gesamte Infrastruktur für den Remote-Zugriff spielt ebenso eine wichtige Rolle. Bereits im letzten Jahr hat die Firma TAS eine VdS-Zertifizierung für die in ihrem Hause entwickelte „TAS Secure Platform“ erhalten. Auch hier war das Unternehmen Vorreiter in puncto Cyber-Sicherheit und der erste Remote Access Infrastructure Service Provider (RAISP), der in Deutschland durch VdS zertifiziert wurde. Erfüllt wurden dabei nicht nur die hohen Sicherheitsanforderungen an die Infrastruktur der Fernzugriffsplattform, sondern auch die Anforderungen an den Service Provider. Dieser ist schließlich verantwortlich für sichere, ständig verfügbare Verbindungen und für den Schutz gegen Cyber-Angriffe.

Zertifikatsübergabe bei der Firma TAS in Mönchengladbach: (v. l. .n. r.) Christoph Schäfer, Produktmanager bei TAS, Günter Grundmann, Abteilungsleiter im VdS-Labor für elektronische Sicherungstechnik, und Daniel Kaumanns, verantwortlicher Produktmanager für die TAS Secure Platform (Foto: VdS)

Bislang fehlte es in der Normenwelt an klaren Regeln für den Fernzugriff auf Alarmsysteme – mit der Folge von Haftungsrisiken für die Betreiber. Mit den kommenden Normen TS 50136-10 für Remote Access und EN 50710 für Remote Services ändert sich zukünftig die unklare Lage.

Daniel Kaumanns: Beide VdS-Zertifizierungen sind ein Gütesiegel für unsere Arbeit an der Cyber-Sicherheit in der Übertragungstechnik. Unser Ziel war es, eine ganzheitlich sichere Lösung für Remote Services anbieten zu können – angefangen bei der Infrastruktur über Gateways bis hin zur Verantwortungsübernahme für den sicheren Fernzugriff auf Gefahrenmeldeanlagen. Kunden, die unsere Plattform sowie flexibel buchbare Services nutzen, bezahlen monatlich nur für die Remote Dienste, die auch benötigt werden. Es muss weder in eine eigene Infrastruktur noch in den Betrieb oder in die Weiterentwicklung investiert werden.

Sebastian Brose: Hier zeigt sich, dass bei Monitoring und Fernwartung von Gefahrenmeldeanlagen

Allgemeine Anforderungen	Benutzer-/ Zugriffsmanagement	Vertraulichkeit und Integrität	Protokollierung/ Ereigniserfassung	Datenfluss	begleitende Maßnahmen
Offline-Funktionalität	Zugriffsschutz durch Authentisierung	Transport-verschlüsselung	Audit Log	sichere Kopplung	Dokumentation der Komponente
sicherer Grundzustand	keine festen Codes	Integrität der Daten bei der Übertragung	Benachrichtigung bei sicherheitsrelevanten Ereignissen	Fremdprodukte/ -dienste	umfassende Bereitstellung von Support
Anpassung der Konfiguration	individualisierte Benutzerkonten	Gewährleistung der Integrität der Software	Export von Ereignissen	„Call-Home"-Funktion	automatische Update-Prüfung
Handhabung von Fehlfunktionen/ Störungen	minimale Zugriffsrechte von Benutzerkonten	Plausibilität von Benutzereingaben/ -aktionen	Erfassung von Telemetriedaten	Verwaltung von Schnittstellen	
Schnittstellen-Sicherheit	zusätzlicher Schutz kritischer Daten	Sicherung von Konfigurationsdaten	Zeitstempel und Zeitsynchronisation	Absicherung von Remote-Zugängen	
sichere Außerbetriebnahme	Time-Out	Sicherung von Nutzdaten			
Manipulations-sicherheit					
DoS-Handling					
Fremdprodukte/ -dienste					

Zentrale Handlungsfelder und zugrundeliegende Anforderungen (Tabelle: VdS)

höchste Sicherheitsanforderungen und Wirtschaftlichkeit durchaus Hand in Hand gehen können. Und eins darf man nicht vergessen: Geschlossen werden müssen die Lücken in den Produkten sowieso. Entweder für die VdS-Prüfung oder nach dem ersten Schaden. Und dass der eintritt, ist sicher.

ETSI TS 103 645 *„Cyber Security for Consumer Internet of Things: Baseline Requirements"*

s+s report: In welchem Verhältnis stehen die VdS-Richtlinien zu anderen Normen und Regelwerken im Bereich der Cyber-Security? Besteht da nicht die Gefahr, dass sich die Anforderungen widersprechen?

Sebastian Brose: Die Richtlinien VdS 3836 stehen inhaltlich in keinem Widerspruch zu Regelwerken, die sich international für den Bereich Cyber-Security in industriellen Anwendungen etabliert haben. Insbesondere zur Normenreihe IEC 62443 besteht eine hohe Kongruenz. So sind die Anforderungen an Komponenten und Systeme in den Richtlinien VdS 3836 in drei unterschiedliche Klassen strukturiert: Klasse A, Klasse B und Klasse C. Diese Nomenklatur entspricht den Anforderungen der Normenreihe IEC 62443 in den Security-Leveln 1–3.

IEC 62443 *„Industrial communication networks – Network and system security"*

Darüber hinaus sind in den Richtlinien VdS 3836 weitere Regelwerke wie beispielsweise das Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) zu den Anforderungen an Smart-Home-Installationen und Geräten des „Internet der Dinge" sowie die ETSI TS 103 645 erfasst.

s+s report: In der Informationstechnik finden bekanntlich neue Entwicklungen in rasantem Tempo statt. Besteht nicht die Gefahr, dass die gerade zertifizierten Produkte schon schnell wieder veraltet und damit unsicher sind?

Sebastian Brose: Wir dürfen Sicherheit nicht mehr als Zustand verstehen, der einmal erreicht wird und dann so bestehen bleibt. Das Zukunftsinstitut hat es treffend so formuliert: „In einer komplex vernetzten Welt, in der sich Bedrohungen und Risiken ständig verändern, ist Sicherheit immer nur punktuell oder phasenweise gegeben. Sicherheit kann somit nicht mehr als ein Endzustand verstanden werden, den es zu erreichen gilt, sondern nur noch als permanenter Prozess, auf den sich Individuen, Organisationen und letztlich die gesamte Gesellschaft bestmöglich einstellen müssen." Dementsprechend sind auch

Unsere Gesprächspartner: Daniel Kaumanns, MBA, (links) ist bei TAS Sicherheits- und Kommunikationstechnik tätig im Produktmanagement Übertragungstechnik und Remote Services sowie verantwortlicher Produktmanager für die TAS Secure Platform; Dipl.-Wirtschaftsjurist (FH) Sebastian Brose (rechts) ist stellvertretender Bereichsleiter und Abteilungsleiter Produktmanagement im Bereich Produkte und Unternehmen bei VdS

die Anforderungen, der Prüf- und Zertifizierungsprozess und die Produktüberwachung für die VdS 3836 abweichend geregelt und neu gedacht.

s+s report: Wie sehen Sie die weitere Entwicklung auf diesem Gebiet?

Sebastian Brose: Die Vernetzung von Systemen und Komponenten der Brandschutz- und Sicherungstechnik hat gerade erst begonnen und wird durch technologische Trends beschleunigt, die in Zukunft erweiterte Anforderungen an die Informationssicherheit stellen. Perspektivisch halten die Richtlinien VdS 3836 auch mit den technologischen Entwicklungen Schritt, die in den kommenden Jahren neue Dimensionen bei der Vernetzung von Systemen und Komponenten der Brandschutz- und Sicherungstechnik einführen werden. Stichwörter in dem Zusammenhang sind KI-basierte Systeme oder selbstüberwachende Systeme, bei denen permanente Prüfungen der Leistungsmerkmale in Echtzeit zum Tragen kommen. All das wird ohne nachgewiesene Cybersicherheit nicht akzeptiert werden. Denn wir dürfen eins nicht vergessen: Die Anlagen werden immer noch einzig und allein zum Schutz von Leib, Leben und Sachwerten installiert!

Daniel Kaumanns: Sicherheitstechnik und IoT sind heute kaum noch trennbar, alles wird immer mehr miteinander vernetzt. Die Sicherheit muss in diesem Kontext neu gedacht werden. Vor diesem Hintergrund werden unabhängige Qualitätsaussagen immer wichtiger. Eine VdS-Zertifizierung – so wie jetzt die gemäß VdS 3836 – ist dabei ein wichtiger Schritt in diese Richtung, für uns und unsere Kunden bleibt VdS ein Garant für Sicherheit.

s+s report: Wir danken Ihnen für dieses Gespräch!

VdS 3836 und SecIoT

Zur besseren Kenntlichmachung der Produkte, die die Anforderungen nach VdS 3836 erfüllen, hat VdS das SecIoT-Logo (s. u.) geschaffen. Weiterführende Informationen zur VdS-zertifizierten Cyber-Sicherheit für vernetzte Produkte, zu den Richtlinien VdS 3836 und zu SecIoT finden Sie unter dem Kurzlink vds.de/3836 oder via QR-Code:

VdS SecIoT

Cyber Security für Komponenten der Brandschutz und Sicherheitstechnik

VdS übergibt erstes VdS 3836-Zertifikat

Pressemitteilung 13/2022

Köln, 05. Mai 2022. Cyber-Angriffe auf IT-Systeme sind alltägliche Praxis. Wenn auch längst nicht alle, so sind doch viele Unternehmen mittlerweile so gut geschützt, dass sie direkte Cyber-Angriffe abwehren können. Die Gefahren lauern woanders – z. B. durch Angriffe auf IoT-Geräte. Gerade hier lässt die Cyber-Sicherheit oft zu wünschen übrig. Und das, obwohl der Datenaustausch durch die zunehmende Vernetzung der softwarebasierten Komponenten steigt.

Ein Einfallstor für Hacker ist beispielsweise der Remote Zugriff auf Anlagen und Produkte über einen konventionellen Router – keinesfalls eine Ausnahmeerscheinung, sondern leider gängige Praxis. Für einen direkten Fernzugriff müssen in der Firewall des Routers Ports freigegeben werden, über welche die Kommunikation zur Übertragungseinrichtung weitergeleitet wird. Mit jedem geöffneten Port steigt jedoch das Risiko, angreifbar zu werden.

Wenn zudem unsichere Kennwörter verwendet werden und/oder die Software der Endgeräte veraltet ist, haben selbst weniger versierte Cyber-Kriminelle leichtes Spiel beim Zugang zum System. Nicht nur im Bereich der kritischen Infrastruktur kann dies fatale Folgen haben. Was passiert, wenn Alarme nicht mehr übertragen werden können? Wenn komplette Anlagen stillstehen, weil Kernkomponenten ausfallen? Hier ist die Sicherheit von Menschen, Unternehmenswerten und Gebäuden bedroht.

Vor diesem Hintergrund hat VdS die Richtlinien VdS 3836 „Cyber-Sicherheit für Systeme und Komponenten der Brandschutz- und Sicherheitstechnik“ implementiert und ein Zertifizierungsverfahren eingeführt, das nun erstmals bei einer Übertragungseinrichtung des Unternehmens TAS GmbH erfolgreich durchgeführt wurde. Eine Zertifizierung nach VdS 3836 eröffnet Unternehmen eine Reihe an Wettbewerbsvorteilen. Denn der Trend zur Vernetzung und Integration von komplexen Brandschutz- und Sicherheitsanlagen in eine smarte Gebäudeumgebung führt dazu, dass erweiterte Sicherheitsanforderungen im Hinblick auf Cyber-Security erfüllt werden müssen. Unternehmen, die sich dieser Aufgabe stellen, stärken ihre Wettbewerbssituation und verfügen über breitere Vermarktungschancen.

Eine weitere VdS-Zertifizierung hat die TAS bereits im letzten Jahr für ihre im Hause entwickelte TAS Secure Platform erhalten. Damit war das Unternehmen der erste VdS-zertifizierte Remote Access Infrastructure Provider (RAISP) in Deutschland.

Foto: TAS

Der VdS übergibt erstes VdS 3836-Zertifikat für Komponenten der Brandschutz und Sicherheitstechnik (vlnr.): Christoph Schäfer, Produktmanager der TAS, Günter Grundmann, Abteilungsleiter im VdS-Labor für elektronische Sicherungstechnik, und Daniel Kaumanns, verantwortlicher Produktmanager für die TAS Secure Platform.

UNTERNEHMEN 13. Juni 2022

VdS-Zertifizierung für Übertragungsgeräte von TAS

Die von TAS entwickelten Übertragungsgeräte TAS-Link IV und Siro-Port sind die ersten in Deutschland, die nach VdS 3836 zertifiziert sind.

Übertragungsgeräte der Firma TAS Sicherheits- und Kommunikationstechnik sind nach VdS 3836 erfolgreich zertifiziert worden – ein wichtiger Baustein im Kampf gegen Cyberkriminalität. Denn Cyberangriffe auf IT-Systeme sind alltägliche Praxis. Wenn auch längst nicht alle, so sind doch viele Unternehmen mittlerweile so gut geschützt, dass sie direkte Cyberangriffe abwehren können. Die Gefahren lauern woanders – zum Beispiel durch Angriffe auf IoT-Geräte. Gerade hier lässt die Cybersicherheit oft zu wünschen übrig. Und das, obwohl der Datenaustausch durch die zunehmende Vernetzung der softwarebasierten Komponenten steigt.

Ein Einfallstor für Hacker ist beispielsweise der Remote Zugriff auf Anlagen und Produkte über einen konventionellen Router – keinesfalls eine Ausnahmeerscheinung, sondern leider gängige Praxis. Für einen direkten Fernzugriff müssen in der Firewall des Routers Ports freigegeben werden, über welche die Kommunikation zur Übertragungseinrichtung weitergeleitet wird. Mit jedem geöffneten Port steigt jedoch das Risiko, angreifbar zu werden. Wenn zudem unsichere Kennwörter verwendet werden und/oder die Software der Endgeräte veraltet ist, haben selbst weniger versierte Cyberkriminelle leichtes Spiel beim Zugang zum System. Nicht nur im Bereich der Kritischen Infrastruktur kann dies fatale Folgen haben. Was passiert, wenn Alarme nicht mehr übertragen werden können? Wenn komplette Anlagen stillstehen, weil Kernkomponenten ausfallen? Hier ist die Sicherheit von Menschen, Unternehmenswerten und Gebäuden bedroht!

Was macht einen Remote Zugang sicher?

Bei der Sicherheit von Systemen und Produktkomponenten mit Netzwerkfunktionalität kommt es vor allem darauf an, eine sichere und ständig verfügbare Kommunikation mit 24/7 Überwachung der Leitungswege zu gewährleisten, den Schutz der Datenintegrität sicherzustellen und den Zugriff zu kontrollieren. Um im Beispiel von Remote Services zu bleiben, müssen dabei sowohl die Übertragungsgeräte selbst als auch die Plattform für den Fernzugriff gegen Cyberangriffe optimal geschützt werden. Für beides hat das Unternehmen TAS Sicherheits- und Kommunikationstechnik eine Lösung. Der bundesweite Anbieter von Sicherheitslösungen und Spezialist in der Übertragungstechnik bietet sowohl ein sicheres Gateway für die Übertragung von Alarmen, Sprache und (Monitoring-) Daten an als auch eine sichere Infrastruktur für den Remote Access.

Cybersicherheit der Übertragungsgeräte von TAS durch VdS-Zertifizierung bestätigt

Die von TAS entwickelten Übertragungsgeräte TAS-Link IV und Siro-Port sind die ersten in Deutschland, die nach VdS 3836 zertifiziert sind, eine Anerkennung der Cybersicherheit für Komponenten der Brandschutz- und Sicherheitstechnik. Die VdS 3836 wurde im Abgleich mit verschiedenen Richtlinien erarbeitet – dem IEC 62443 zur IT-Sicherheit für Netze und Systeme, dem Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft zu den Anforderungen an Smart-Home-Installationen sowie der Etsi TS 103 645 – Cyber Security for Consumer IoT.

Durch das proprietäre Betriebssystem können die Zugriffsmöglichkeiten von vornherein auf die Ports beschränkt werden, die auch wirklich benötigt werden. Neben diesem Schutz durch Security by Design unterstützt die neue Generation von TAS-Link und Siro-Port Übertragungsgeräten auch Ipsec für die verschlüsselte Datenübertragung und bietet weitere Sicherheitsfeatures, die dem höchsten Level der Cyber Security entsprechen. Ein unberechtigter Zugriff auf die Übertragungsgeräte ist damit nahezu unmöglich.

VdS zertifiziert Betreiber von Remote Services

TAS ist als Remote Access Infrastructure Provider (RAISP) durch VdS unter Berücksichtigung der Normen EN 50710 und TS 50136-10zertifiziert worden.

Artikel lesen

Sichere Plattform für Remote Access

Eine VdS-Zertifizierung hat die TAS bereits im letzten Jahr für ihre im Hause entwickelte TAS Secure Platform erhalten. Auch hier ist das Unternehmen Vorreiter in puncto Cybersicherheit und der erste Remote Access Infrastructure Provider (Raisp), der in Deutschland durch VdS zertifiziert wurde. Für Daniel Kaumanns, verantwortlicher Produktmanager für die TAS Secure Platform, sind beide VdS-Zertifizierungen ein Gütesiegel für die Cybersicherheit in der Übertragungstechnik. Ihr Ziel sei es gewesen, eine ganzheitlich sichere Lösung für Remote Services anbieten zu können – angefangen bei der Infrastruktur über Gateways bis hin zur Verantwortungsübernahme für den sicheren Fernzugriff auf Gefahrenmeldeanlagen. Kunden, die ihre Plattform sowie flexibel buchbare Services nutzten, bezahlten monatlich nur für die Remote Dienste, die auch benötigt würden. Es müsse weder in eine eigene Infrastruktur noch in den Betrieb oder in die Weiterentwicklung investiert werden.

Hier zeigt sich, dass bei Monitoring und Fernwartung von Gefahrenmeldeanlagen höchste Sicherheitsanforderungen und Wirtschaftlichkeit Hand in Hand gehen können.

22571 · ISSN 2191-9232 Einzelverkaufspreis: 16,- Euro

»SicherheitsPraxis

Fachzeitschrift für Errichterbetriebe, Gutachter, Planungsbüros und Systemhäuser

2 » Juni 2022 · www.prosecurity.de

» *Die Anwendungen für video-basierte IoT-Lösungen nehmen deutlich zu. Gibt es bestimmte Bereiche, in denen Sie Schwerpunkte setzen und Partner suchen?*

Wir suchen nicht gezielt nach Partnern. Im Grunde genommen kann jeder mitmachen, der eine gute Idee hat und die genannten Voraussetzungen erfüllt. Aber wir setzen strategische Schwerpunkte in vertikalen Märkten, in denen wir besonderes Potenzial sehen. Das ist international unterschiedlich, weil die lokalen Märkte sich unterscheiden und es auch unterschiedliche gesetzliche Rahmenbedingungen gibt. In Deutschland liegen unsere strategischen Schwerpunkte in den Bereichen Logistik, Parken, Bauwesen, Einzelhandel, Alarmleitstellen und Cloud-Computing. In diesen Bereichen sehen wir hierzulande besonderes Wachstumspotenzial. Video-basierte IoT-Lösungen für die Kennzeichenerkennung, Steuerung von Zufahrten oder Erkennen von freien Stellplätzen in Parkhäusern beispielsweise sind derzeit stark gefragt.

Sie bieten in diesen Bereichen auch eigene Lösungen an. Machen sich Ihre Lösungen und die Ihrer Partner nicht gegenseitig Konkurrenz?

Technisch gesehen steht ein Kamerasystem mit eigener Analyseintelligenz grundsätzlich im Wettbewerb mit spezialisierten Systemlösungen. Ein typisches Beispiel ist die Kennzeichenerkennung. Das gilt aber nicht nur für Hikvision, sondern für alle Kamerahersteller. Es gibt im Markt einen Mix aus Herstellerlösungen und integrierten Lösungen spezialisierter Anbieter. Wofür sich der Kunde am Ende entscheidet, hängt von vielen Faktoren ab.

Tim Hancock, Partner Alliance Manager Hikvision Deutschland GmbH

Welchen Anteil an Ihrem Umsatz macht das Geschäft mit Technologie-Partnern aus?

Tim Hancock: Da es unterschiedliche Vermarktungswege gibt, ist es schwer, den tatsächlichen Umsatz des Partnergeschäfts genau zu beziffern. In jedem Fall gewinnt die Zusammenarbeit mit Technologie-Partnern erheblich an Bedeutung und ist ein wichtiger Faktor in unserer Wachstumsstrategie.

Viele der Lösungen, die Sie und Ihre Partner auf dem Innovation Summit gezeigt haben, sind keine klassischen Sicherheitsanwendungen. Welche Rolle spielt der Sicherheitsmarkt für Sie als Kamerahersteller?

Der Sicherheitsmarkt ist nach wie vor wichtig und wird es auch bleiben. Aber dadurch, dass die Kamera zum Sensor wird und nicht nur Bilder, sondern vorverarbeitete Informationen liefern kann, entstehen immer neue Anwendungen in anderen Bereichen. Das Wachstum video-basierter IoT-Lösungen spielt sich daher weniger bei etablierten Sicherheitsanwendungen ab als in anderen vertikalen Märkten. Das spiegelt sich auch in unserem Technology-Partner-Netzwerk wider.

Erfolgreiche Zertifizierung nach VdS 3836

Erste Anerkennung für Cyber-Sicherheit bei Übertragungsgeräten

vlnr. Christoph Schäfer, Produktmanager der TAS, Günter Grundmann Abteilungsleiter im VdS-Labor für elektronische Sicherungstechnik und Daniel Kaumanns, verantwortlicher Produktmanager für die TAS Secure Platform

Cyber-Angriffe auf IT-Systeme sind alltägliche Praxis. Wenn auch längst nicht alle, so sind doch viele Unternehmen mittlerweile so gut geschützt, dass sie direkte Cyber-Angriffe abwehren können. Die Gefahren lauern woanders – z. B. durch Angriffe auf IoT-Geräte. Gerade hier lässt die Cyber-Sicherheit oft zu wünschen übrig. Und das, obwohl der Datenaustausch durch die zunehmende Vernetzung der softwarebasierten Komponenten steigt.

Ein Einfallstor für Hacker ist beispielsweise der Remote Zugriff auf Anlagen und Produkte über einen konventionellen Router – keinesfalls eine Ausnahmeerscheinung, sondern leider gängige Praxis. Für einen direkten Fernzugriff müssen in der Firewall des Routers Ports freigegeben werden, über welche die Kommunikation zur Übertragungseinrichtung weitergeleitet wird. Mit jedem geöffneten Port steigt jedoch das Risiko, angreifbar zu werden. Wenn zudem unsichere Kennwörter verwendet werden und/oder die Software der Endgeräte veraltet ist, haben selbst weniger versierte Cyber-Kriminelle leichtes Spiel beim Zugang zum System. Nicht nur im Bereich der kritischen Infrastruktur kann dies fatale Folgen haben. Was passiert, wenn Alarme nicht mehr übertragen werden können? Wenn komplette Anlagen stillstehen, weil Kernkomponenten ausfallen? Hier ist die Sicherheit von Menschen, Unternehmenswerten und Gebäuden bedroht!

Was macht einen Remote Zugang sicher?

Bei der Sicherheit von Systemen und Produktkomponenten mit Netzwerkfunktionalität kommt es vor allem darauf an, eine sichere und ständig verfügbare Kommunikation mit 24/7 Überwachung der Leitungswege zu gewährleisten, den Schutz der Dateninte-grität sicherzustellen und den Zugriff zu kontrollieren. Um im Beispiel von Remote Services zu bleiben, müssen dabei sowohl die Übertragungsgeräte selbst als auch die Plattform für den Fernzugriff gegen Cyberangriffe optimal geschützt werden. Für beides hat das Unternehmen TAS Sicherheits- und Kommunikationstechnik eine Lösung. Der bundesweite Anbieter von Sicherheitslösungen und Spezialist in der Übertragungstechnik bietet sowohl ein sicheres Gateway für die Übertragung von Alarmen, Sprache und (Monitoring-) Daten an als auch eine sichere Infrastruktur für den Remote Access.

Cyber-Sicherheit der Übertragungsgeräte

Die von TAS entwickelten Übertragungsgeräte TAS-Link IV und SIRO-Port sind die ersten in Deutschland, die nach VdS 3836 zertifiziert sind, eine Anerkennung der Cyber-Sicherheit für Komponenten der Brandschutz- und Sicherheitstechnik. Die VdS 3836 wurde im Abgleich mit verschiedenen Richtlinien erarbeitet – dem IEC 62443 zur IT-Sicherheit für Netze und Systeme, dem Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft zu den Anforderungen an Smart Home Installationen sowie der ETSI TS 103 645 – Cyber Security for Consumer IoT.

Durch das proprietäre Betriebssystem können die Zugriffsmöglichkeiten von vornherein auf die Ports beschränkt werden, die auch wirklich benötigt werden. Neben diesem Schutz durch Security by Design unterstützt die neue Generation von TAS-Link und SIRO-Port Übertragungsgeräten auch IPsec für die verschlüsselte Datenübertragung und bietet weitere Sicherheitsfeatures, die dem höchsten Level der Cyber Security entsprechen. Ein unberechtigter Zugriff auf die Übertragungsgeräte ist damit nahezu unmöglich.

Sichere Plattform für Remote Access

Eine VdS-Zertifizierung hat das Unternehmen bereits im letzten Jahr für ihre im Hause entwickelte TAS Se- »

cure Platform erhalten. Auch hier ist das Unternehmen Vorreiter in puncto Cyber Sicherheit und der erste Remote Access Infrastructure Provider (RAISP), der in Deutschland durch VdS zertifiziert wurde. Erfüllt wurden nicht nur die hohen Sicherheitsanforderungen an die Infrastruktur der Fernzugriffsplattform, sondern auch die Anforderungen an den Service Provider. Dieser ist verantwortlich für sichere, ständig verfügbare Verbindungen und Schutz gegen Cyber-Angriffe. Bislang fehlte es an der klar geregelten Verantwortung beim Fernzugriff auf Alarmsysteme – mit der Folge von Haftungsrisiken für die Betreiber. Mit den kommenden Normen TS 50136-10 für Remote Access und EN 50710 für Remote Services ändert sich zukünftig die unklare Lage.

Für Daniel Kaumanns, verantwortlicher Produktmanager für die TAS Secure Platform, sind beide VdS-Zertifizierungen ein Gütesiegel für die Cyber-Sicherheit in der Übertragungstechnik. „Unser Ziel war es, eine ganzheitlich sichere Lösung für Remote Services anbieten zu können – angefangen bei der Infrastruktur über Gateways bis hin zur Verantwortungsübernahme für den sicheren Fernzugriff auf Gefahrenmeldeanlagen. Kunden, die unsere Plattform sowie flexibel buchbare Services nutzen, bezahlen monatlich nur für die Remote Dienste, die auch benötigt werden. Es muss weder in eine eigene Infrastruktur noch in den Betrieb oder in die Weiterentwicklung investiert werden."

Hier zeigt sich, dass bei Monitoring und Fernwartung von Gefahrenmeldeanlagen höchste Sicherheitsanforderungen und Wirtschaftlichkeit Hand in Hand gehen können.

www.tas.de

Rohrabschottungen

Warum einfach, wenn's auch kompliziert geht?

Rohrabschottungen verhindern, dass Feuer, Rauch und zu hohe Temperaturen in andere Geschosse, Wohnungen und Nutzungseinheiten übertragen werden. Sie kommen als brandschutztechnische Maßnahme zur Anwendung, wenn Rohrleitungen durch Wände oder Decken mit Anforderungen an den Feuerwiderstand geführt werden. Grundlegende Schutzziele werden in § 3 und § 14 der Musterbauordnung (MBO) definiert.

Dipl.-Ing. (FH) Heidi Burow-Strathoff
Ingenieurin im baulichen Brandschutz MPA NRW von 1990 bis 2013, stellvertretende Prüfstellenleiterin für haustechnische Anlagen; Mitarbeit im europäischen Normungsgremium für Rohr- und Kabelabschottungen; Installationskanäle, seit 10/2013 Brandschutzsachverständige bei G+H ISOLIERUNG, Engineering Services.

Aktive Verbandstätigkeit im bvfa seit 2013, Obfrau mehrerer Arbeitsgruppen.

In diesem Artikel wird gezeigt, welche Anforderungen der bauliche Brandschutz stellt, was bei der Montage von klassifizierten Abschottungen mit Verwendbarkeitsnachweis zu beachten ist und welche rechtliche Verantwortung der Ausführende hat. Weiterhin erfolgt eine Abgrenzung zu den Erleichterungen nach der Muster-Leitungsanlagenrichtlinie (MLAR) sowie ein Ausblick, welche Änderungen zu erwarten sind.

Umsetzung durch Normbrandprüfungen

Zumeist erfolgt der brandschutztechnische Nachweis über die Wirksamkeit einer Abschottung auf Grundlage einer Normbrandprüfung. Je nach Produktart kann man bei einer Vielzahl von Produkten zwischen der deutschen Prüfnorm (DIN 4102-11), wie für Rohrabschottungen, und dem europäischen Prüfverfahren (EN 1366-3) wählen.

Verwendbarkeitsnachweise: es ist kompliziert

In Deutschland erteilen verschiedene Stellen baurechtliche Verwendbarkeitsnachweise auf die genannten Klassifizierungen. Sie unterscheiden sich in Abhängigkeit des Rohrwerkstoffes und der Anwendung. Nachweis sind hierfür die 1997 eingeführten allgemeinen bauaufsichtlichen Prüfzeugnisse (AbP).

Die allgemeinen bauaufsichtlichen Zulassungen (AbZ) für Abschottungen brennbarer Rohre gibt es seit den 80er Jahren. Aktuell werden von den Prüfstellen die AbP für brennbare und nicht brennbare Rohre auf Basis von Streckenisolierungen aufgestellt. Das Deutsche Institut für Bautechnik (DIBt) stellt Bauartgenehmigungen (AbG) für die Abschottung brennbarer mit brandschutzechnisch wirksamen intumeszierenden Baustoffen ausgestatten Rohre und für nicht brennbare Entsorgungs- und Versorgungsleitungen mit brennbaren Anschlussleitungen aus. Durch die Novellierung der MBO 2016 und die Einführung der Musterverwaltungsvorschrift Technische Baubestimmungen (MVVTB) 2017 wurden die bisherigen Zulassungen durch das Deutsche Institut für Bautechnik (DIBt) geändert und die Bauartgenehmigungen eingeführt.

Bauart vs. Bauartgenehmigung

Eine Bauartgenehmigung schreibt den Einbau detailliert vor, damit die errichtete Abschottung auch brandschutztechnisch wirkt, zusätzlich werden für die auf der Baustelle verwendeten Bauprodukte AbZ ausgestellt. Um diese Vorgaben umzusetzen, ist ein hoher personeller und kostenintensiver Aufwand erforderlich. Die aufgeführten Verweise bei den AbPs sind in der MVVTB nachzulesen.

Die Praxis

In der Umsetzung erfordert dieses Regelwerk sehr detaillierte Kenntnisse über die vollständige Leitungsverlegung. Sind Brandschutzanforderungen vorhanden, gibt es folgende Lösungsmöglichkeiten der Umsetzung:

Klassifizierte Rohrdurchführungen mit Verwendbarkeitsnachweis

Technisch kommen durchgängige Isolierungen unterschiedlicher Art gerne in Verbindung mit intumeszierenden Bandagen zum Einsatz. Für brennbare Leitungssysteme gibt es Manschetten. Die Verwendbarkeitsnachweise werden immer detaillierter. Anders als noch vor 10 Jahren, wird mittlerweile bei Isolierungen jeder Produktname aufgeführt. Folgende Randbedingungen müssen vor Erstellung der Rohrabschottungen geklärt und beachtet werden:

- Offenes/geschlossenes Leitungssystem
- Rohrwerkstoff
- Rohrwandstärke
- Isoliertypen (z.B. Polyurethan)
- Isolierproduktnamen
- Isolierdicke und -länge
- Abstand der 1.Abhängung

Bei nichtbrennbaren Rohren gibt es bzgl. der Leitungsbefestigung auch Vorgaben: Wurden Dübel mit Brandschutznachweis verwendet und die zulässigen Zugspannungen der Abhängungen eingehalten?

Übereinstimmungserklärung des Errichters und die Haftung

Wer Rohrabschottungen nach Verwendbarkeitsnachweis errichtet, haftet durch Ausstellen einer Übereinstimmungserklärung für die korrekte Ausführung. Die Vorgaben einzuhalten ist auch nicht einfach: Oft sind die Kernlochbohrungen zu klein, es gibt kaum Arbeitsraum zwischen Rohrdurchführung und Bauteillaibung. Die geforderte Isolierdicke kann nicht aufgebracht werden, Leitungen mit großen Durchmessern liegen relativ dicht beieinander.

Können Vorgaben des AbP/AbG nicht eingehalten werden, sollte frühzeitig der Hersteller der Rohrabschottung kontaktiert werden, um den Sachverhalt zu bewerten und ggf. Kompensationsmaßnahmen festzulegen. Dies alles wird in einer Herstellererklärung dokumentiert bzw. eine „Nicht wesentliche Abweichung" zu den Einbaubestimmungen des Verwendbarkeitsnachweises erklärt. Abschließend kann der Errichter eine Übereinstimmungserklärung ausstellen.

Rohrdurchführungen nach den Erleichterungen der MLAR

Die MLAR wurde 1988 für den Anwender erstellt und beinhaltet einfache Regeln für die Erfüllung brandschutztechnischer Anforderungen bei Leitungsanlagen. Sie wurde von jedem Bundesland eingeführt und regelmäßig überarbeitet, die letzte Fassung ist von Februar 2015. Für nichtbrennbare und brennbare Rohre sind hier einige „Erleichterungen" festgeschrieben, wie bei der Leitungsdurchführung bei Wänden mit Brandschutzanforderungen vorzugehen ist.

Randbedingungen MLAR ohne Dämmung (Abschnitt 4.3.1)

- Rohrleitungen aus nichtbrennbaren Baustoffen ≤ 160 mm
- Rohrleitungen aus brennbaren Baustoffen mit einem Außendurchmesser ≤ 32 mm
- Mindestbauteildicken Wand/Decke: 60 mm Feuerhemmend (F30), 70 mm Hochfeuerhemmend (F60), 80 mm Feuerbeständig (F90)
- Restspaltverschluss mit nichtbrennbaren Baustoffen (z. Bsp. Mörtel), Mineralfasern (Restspaltbreite ≤ 50 mm), aufschäumenden Baustoffen (Restspaltbreite ≤ 15 mm)
- Abstandsregeln der Leitungen untereinander: mind. gleicher Durchmesser
- Kennzeichnungsschild muss nicht ausgestellt werden
- die Rohrabhängungen und deren Befestigungen werden nicht berücksichtigt
- sämtliche Vorgaben sind einzuhalten

Wird eine Rohrdurchführung nach diesen Vorgaben verschlossen, ist man in Übereinstimmung mit geltendem Recht, erhält jedoch keine klassifizierte Abschottung, denn ein nicht brennbares Rohr ohne Dämmung mit einem Rohraußendurchmesser ≤ 160 mm, welches durch eine 80 mm dicke Massivwand ohne Brandschutzmaßnahme vermörtelt durchgeführt wird, erfüllt die Anforderungen an klassifizierte Abschottungen nicht. Alle Randbedingungen müssen jedoch eingehalten werden.

Wieder neue Verwendbarkeitsnachweise

Am 29.11.2021 wurden die Hersteller von Brandschutzprodukten in einer Veranstaltung vom DIBt informiert, dass es die AbG ab 2026 in dieser Form nicht mehr geben wird. Stattdessen sollen „Anwendungsregeln" durch das DIBt veröffentlicht werden. Danach sollen von den Prüfstellen AbPs erstellt werden. In diesem Jahr will man prüfen, welche Bereiche weiterhin Bauartgenehmigungen vom DIBt bekommen sollen. Ende 2022 gibt es dazu weitere Informationen.

Aus persönlicher Sicht gesprochen: Die Hersteller waren darauf nicht vorbereitet. Vier Jahre nachdem Bauartgenehmigungen eingeführt wurden, setzt man einen Prozess in Gang, um sie wieder abzuschaffen.

Fazit

Rohrabschottungen zu planen und zu errichten ist mittlerweile sehr komplex, wenn man in Übereinstimmung mit dem Baurecht agieren will. Die Umsetzung von Brandschutzanforderungen nach den Erleichterungen der MLAR ist einfach anwendbar, hat jedoch Grenzen. Es empfiehlt sich aus Gründen des Anlagenschutzes, bei Neubauten im Zuge der Sanierung unter Beachtung einiger Aspekte immer Rohrabschottungen mit Verwendbarkeitsnachweis zu errichten. Neu eingeführte Verwendbarkeitsnachweise für Mischinstallationen haben im Markt zu einer großen Verunsicherung geführt. Die Frage ist, ob diese Nachweise (erstellt nach einem Ad-hoc-Brandprüfszenario) wirklich gebraucht werden, um sicher zu bauen. Der Bundesverband Technischer Brandschutz (bvfa) hat zur Aufklärung ein öffentlich zugängliches Positionspapier erstellt. Eine erneute Umstellung der Verwendbarkeitsnachweise kann der Autorin nach nur angestoßen werden, wenn alle Akteure beteiligt werden – wovon wir noch weit entfernt sind.

77500

ISSN 1866-2420

SECURITY INSIGHT

FACHZEITSCHRIFT FÜR UNTERNEHMENSSICHERHEIT UND WIRTSCHAFTSSCHUTZ

TITELTHEMA

Uiguren und die Neue Seidenstraße

Zusammenarbeit und Rivalität mit China birgt ständig neue Herausforderungen

Januar/Februar
01/ 2022
EPr. 15,– €

www.prosecurity.de

Gefahren erkennen mit Radartechnologie

Der Einsatz von Videoüberwachungssystemen zur Identifizierung von Personen und deren Handlungen etwa auf öffentlichen Plätzen ist mittlerweile Standard. Immer häufiger kommen dabei auch Lösungen auf Basis Künstlicher Intelligenz zum Einsatz. Sie soll helfen, bestimmte Verhaltensmuster oder Bewegungsabläufe zu erkennen und anhand von Kriterien zu entscheiden, ob beispielsweise eine gefährliche Handlung vorliegt.

Gefördert vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

Vergleichsweise neu dagegen ist die Idee, Radar-Technologie (Radio Detection and Ranging) für Szenarien wie der Überwachung von öffentlichen Plätzen oder Bahnhöfen einzusetzen. Auf Radar basierende Sicherheitslösungen sind bislang vor allem beim Militär anzutreffen, aber auch im zivilen Bereich haben sie Einzug gefunden. Hier vor allem im industriellen Sektor, zur Anwesenheitserkennung von Personen innerhalb einer Produktionsanlage oder als Teil von Sicherheitslösungen wie beim Perimeterschutz. Sie kommt immer häufiger dort zur Anwendung, wo optische Sensoren an ihre Grenzen stoßen.

Radargeräte arbeiten dagegen völlig anders als Videoüberwachungssysteme. Ausgestrahlte elektromagnetische Wellen treffen auf ein Objekt und anhand der Reflexion zum Ursprung lassen sich verschiedene Informationen auswerten. Durch das Bewegen der Radarantenne oder mit Hilfe von mehreren gerichteten Antennen (Array) sind Systeme in der Lage, die Distanz zu einem Objekt, seine Geschwindigkeit, Winkelposition und andere Parameter zu bestimmen.

Gegenüber optischen Sensoren haben Radare dabei einige Vorteile. Sie sind gegen Umwelteinflüsse wie Nebel, Niederschlag oder auch Rauch quasi „immun“. Zudem haben sie in der Regel je nach Einsatzgebiet eine größere Reichweite in der Detektierung und können mehrere Objekte gleichzeitig erfassen und über größere Bereiche nachverfolgen. Objekte lassen sich auch klassifizieren und sind in der Auswertung anonym, da etwa Personen nur als Radarquerschnitt erkennbar, aber nicht identifizierbar sind. Denn die Radartechnologie liefert kein Bild, sondern Farbspektren und Wellenlinien – vergleichbar mit Messungen von Wärmebildkameras bei Häusern. Radarstrahlen sind sogar in der Lage, bestimmte Hindernisse zu durchdringen. Auf öffentlichen Plätzen etwa sind Personen mithilfe von Radargeräten auch dann zu erkennen, selbst wenn sie sich hinter anderen Menschen befinden oder Hindernisse eine optische Erfassung erschweren würden.

Dateninterpretation mittels KI

Während die Radartechnik als solche seit Jahrzehnten weiterentwickelt worden ist, sind für den Einsatz zur Flächenüberwachung mit spezifischen Anforderungen (das Erkennen von Personen mit und ohne Gegenstände, als gefährlich eingestufte Handlungen und Bewegungsmuster) vor allem softwarebasierte Herausforderungen zu lösen. Hier kommt ähnlich wie bei der Videoüberwachung auch der Einsatz von Künstlicher Intelligenz ins Spiel. Dabei hilft KI zu erkennen, ob ein gefährliches oder ungefährliches Verhalten bei Menschen vorliegt, zum Beispiel ob Personen in eine Schlägerei verwickelt sind. Ist das der Fall, schlägt das System Alarm. Um dies zu bewerkstelligen, müssen Personen oder Gegenstände dem Radarsystem als Muster klassifiziert werden, damit es diese zuverlässig erkennt und unterscheiden kann. Für die Klassifizierung können etwa Verfahren im Rahmen von KI-basierten Lösungen zur Mustererkennung unter Einsatz „Neuronaler Netzwerke“ angewandt werden. Als Merkmale für die Mustererkennung werden die sogenannten Mikro-Doppler-Signale verwendet. Diese umfassen ein bewegungscharakteristisches Profil einzelner Objektklassen, wie sich bewegende Personen oder mitgeführte Gegenstände. Um eine hinreichende Anzahl von Trainingsdaten für ein solches System zu generieren, wird dieses mit Aufzeichnungen von speziellen Radar-Video-Geräten trainiert. Hierbei „hilft“ die auf die Videosignale angewandte Bilderkennung mit einer Annotation dem Radarsystem, die erfassten Objekte korrekt zu klassifizieren.

Praktische Anwendung in Vorbereitung

Der Einsatz eines Radarüberwachungssystems für die Personenerkennung auf öffentlichen Plätzen und Bahnhöfen soll im Rahmen eines Forschungsprojekts in Mönchengladbach erarbeitet und in der Praxis erprobt werden. Das Projekt mit dem Namen „KIRaPol.5G“ wird vom Land NRW gefördert und umfasst die Radarüberwachung mit KI-Unterstützung unter Nutzung des Mobilfunkstandards 5G zur Datenübermittlung. Das Konsortium besteht aus den Unternehmen IMST GmbH, TAS Sicherheits- und Kommunikationstechnik sowie m3connect GmbH, der Hochschule Niederrhein und der Polizei Mönchengladbach. Als assoziierte Partner sind die Bundespolizei und das bayerische Landeskriminalamt mit an Bord.

Neue Möglichkeiten durch Mobilfunkstandard 5G

Die Anwendung von 5G in der Sicherheitstechnik stößt insgesamt auf ein breites Interesse, da neue Möglichkeiten eröffnet werden. Radar-Sensordaten und hochauflösende Videos mit hoher Bandbreite für die Verarbeitung in Edge- und Cloud-Computersystemen werden über 5G versendet. Dabei ist ein privates 5G Netz, im Gegensatz zu WLAN oder Operatornetzen ausfallsicher, und stellt durch Authentifizierung ein sehr hohes Schutzniveau dar. Somit ermöglicht erst 5G die effektive Entwicklung und Durchführung datenschutz- und richtlinienkonformer Überwachung in sicherheitsrelevanten Bereichen.

Im Projekt „KIRaPol.5G“ arbeitet TAS Sicherheits- und Kommunikationstechnik, ein bundesweit tätiger Spezialist für Übertragungstechnik und vernetzte Sicherheitslösungen, u. a. an der Gesamtkonzeption eines fusionierten Video- und Radarsensors, der in die 5G Netzwerkarchitektur eingebunden wird sowie dem Ausbau eines von TAS entwickelten Sicherheitsrouters um ein 5G-Kommunikationsmodul. Damit kann sowohl die 5G-spezifische Architektur für Netzsicherheit als auch Netzverfügbarkeit genutzt werden. Zudem soll die auf KI basierende Sensorintelligenz in die Cloud übertragen werden. Hierfür hat das Unternehmen mit der TAS Secure Platform eine „intelligente“ Lösung parat, die Sensordaten datenschutz- und richtlinienkonform berechtigten Nutzern zur Verfügung stellt.

► www.tas.de

PROTECTOR

5|2022
Mai
50. Jahrgang

ASW Bundesverband –
Allianz für Sicherheit in der Wirtschaft e.V.

schlütersche
www.sicherheit.info

Effektive Technik

Wie Lidar die Detektion in öffentlichen Gebäuden revolutioniert | 28

Smarter Mehrzweck

Gewerkeübergreifende Integration von Videotechnik | 36

Verschärfte Forderungen

Was das IT-Sicherheitsgesetz 2.0 für Betreiber bedeutet | 46

Den Durchblick behalten

Radarsysteme zum Einsatz im öffentlichen Bereich unter Einhaltung der Datenschutzrichtlinien | 18

Foto: Fraunhofer IZM / Volker Mai

Kompakte Radargeräte gehören zum Standard teilautonom fahrender Fahrzeuge. Die Systeme eignen sich aber auch zum Einsatz im öffentlichen Bereich.

Den Durchblick behalten

Radarsysteme werden beispielsweise in der Messtechnik eingesetzt. Sie können jedoch auch im öffentlichen Bereich Videosysteme unterstützen.

HENDRICK LEHMANN

Radarsysteme, die bisher zur Detektion an Flughäfen oder in der Messtechnik eingesetzt werden, haben Eigenschaften, die sie auch für die Überwachung öffentlicher Bereiche empfehlen. Aber noch ist aktuell die Videoüberwachung Mittel der Wahl zur Überwachung von Objekten oder Bereichen. Ob öffentlicher Platz, Großveranstaltung oder Objektschutz, Videoüberwachungskameras sind aus dem Alltag nicht mehr wegzudenken. Sie ermöglichen die optische Identifizierung von Personen und Objekten und sind Dank fortschreitender Entwicklung auch immer häufiger bei Nacht und in schlechten Wetterverhältnissen besser einsetzbar. Gleichzeitig sind mit ihrem Einsatz auch die Anforderungen an den Datenschutz gestiegen. Die Datenschutzgrundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG) legen strenge Maßstäbe an Videoüberwachungslösungen, insbesondere, wenn sie von staatlicher Seite betrieben werden. Das betrifft Technologien zur Kennzeichenerkennung, die Überwachung öffentlicher Räume sowie die automatisierte Gesichtserkennung mithilfe Künstlicher Intelligenz (KI). Der Einsatz der Videoüberwachung an öffentlich zugänglichen Orten bedarf etwa in der Regel eines Nachweises einer besonderen Kriminalitätsbelastung. Die Landespolizeigesetze haben in den letzten Jahren entsprechende Passagen aufgenommen, auch zur Frage, welche Art der Aufzeichnung zulässig ist und wann die Aufnahmen zu löschen sind.

„Radare eignen sich ideal für den Einsatz in Umgebungen, in denen andere Detektionssysteme wie Videoüberwachungslösungen eher Schwierigkeiten haben."

Hendrick Lehmann,
freier Mitarbeiter PROTECTOR

Bewährte Technologie

Bei Radar (Radio Detection And Ranging) handelt es sich um eine Technologie, bei der

sich mittels Funkwellen Objekte erkennen und ihre Position sowie ihre Geschwindigkeit ermitteln lassen. Die umgangssprachlich benannten Radarstrahlen sind elektromagnetische Wellen, die mitunter in sehr hohen Frequenzbereichen (drei bis 300 GHz) arbeiten. Höhere Frequenzbereiche ermöglichen mitunter eine sehr genaue Auflösung von Objekten, bei allerdings abnehmender Reichweite. In der Messtechnik etwa kommen „Terahertzradare" zum Einsatz (über 100 GHz), um Materialfehler in der Produktion zu entdecken oder als Körperscanner zur Personenkontrolle. Radare im niederen Frequenzbereich finden häufig Anwendung auf dem militärischen Gebiet, wo eine hohe Reichweite für die Entdeckung wichtig ist.

Ein Radar sendet dabei immer elektromagnetische Wellen aus, die von einem Objekt in viele Richtungen reflektiert und gestreut werden. Ein Teil der reflektierten Strahlen trifft auf einen Empfänger, der anhand des Signals und in Abhängigkeit des Radar-Typs Informationen über Position, Geschwindigkeit und Höhe liefert. Wie gut ein Objekt detektierbar ist, hängt im Wesentlichen neben Umwelteinflüssen auch von seinem Radarquerschnitt ab, die in den Angaben über Größe, Form und Material des Objekts einfließen und einen numerischen Vergleichswert ergeben. Das bedeutet, der eingesetzte Radar-Typ und das Frequenzband orientieren sich auch an den zu detektierenden Objekten, etwa Menschen und Fahrzeugen. Die Leistungsfähigkeit im Sinne der Detektierbarkeit beeinflusst außerdem die Tatsache, dass Radarstrahlen bestimmte Materialien durchdringen können. Metalle reflektieren Radarstrahlen am besten und sind generell nicht zu durchdringen. Das Gleiche gilt für Wasser. Trockenes Holz, Schäume, Kleidung, Regen und Kunststoffe sind dagegen gut bis sehr gut zu durchdringen. Menschen hingegen absorbieren und reflektieren Strahlen eher.

Die Allwetter-Lösung

Radare eignen sich aufgrund der physikalischen Eigenschaften der elektromagnetischen Wellen ideal für den Einsatz in Umgebungen, in denen andere Detektionssysteme wie Videoüberwachungslösungen eher Schwierigkeiten haben. Dunkelheit, ungünstige Lichtverhältnisse, Nebel oder Regen sowie Temperaturen spielen prinzipiell keine Rolle. Ebenso können Radargeräte Fehlalarme minimieren. Videoüberwachungslösungen etwa interpretieren die Bewegung eines Objekts als eine Anzahl der Pixeländerungen, die einen bestimmten Schwellenwert überschreiten muss. Schatten oder Lichtstrahlen können hier vermehrt Fehlalarme auslösen. Radarstrahlen erfassen nur rein physikalische Bewegungen und sind gegenüber obigen Phänomenen unempfindlich. Auch Verunreinigungen von Kameralinsen oder Insekten können für Videokameras ein Problem darstellen, wohingegen Radargeräte auch solche Störungen ignorieren können.

Ein weiterer Vorteil des Radars liegt in der beschriebenen Fähigkeit, Materialien zu durchdringen. Personen, die etwa hinter einem Baum stehen oder hinter ähnlichen Objekten sind damit trotzdem detektierbar. Videokameras können dagegen nicht durch Objekte hindurchsehen und sind auf klare, unbehinderte Sichtlinien angewiesen.

Auch zur Überwachung des öffentlichen Bereichs geeignet

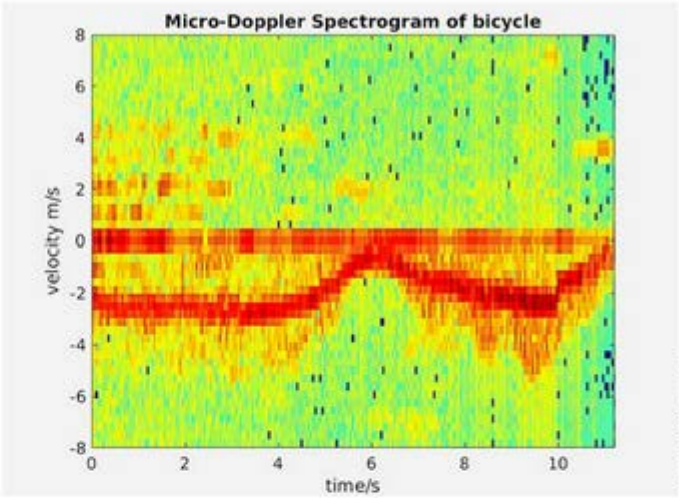
Radare sind in ihrer Funktionalität nicht neu und werden etwa seit Jahren im Bereich des (teil-) autonomen Fahrens und in der Industrie zur Objekt- und Personenerkennung eingesetzt. Vergleichsweise neu ist ihre Verwendung zur Überwachung öffentlicher Plätze und Räume in urbaner Umgebung. Hierzu bedarf es neben einem gut durchdachten Konzept für die Aufstellung der

Foto: Norbert Nagel CC-BY-SA

Ein typisches Radar zur Flugüberwachung am Frankfurter Flughafen.

Radargeräte auch für die Aufgabe entsprechend ausgewählte Systeme. Sollen innerhalb eines definierten Bereichs Personen „nur" erkannt werden oder auch, ob und wohin sie sich bewegen? Soll das System ferner sogar in der Lage sein, zwischen verschiedenen Objekten zu unterscheiden (Menschen, Gegenstände wie Fahrräder) und sogar einzelne Bewegungsmuster erfassen und interpretieren? Was auf den ersten Blick logisch klingt und wo die Videoüberwachung mittlerweile ein hohes technisches Lösungsniveau für diese Fragen erreicht hat, muss für vergleichbare Lösungen auf Basis von Radargeräten noch umfassend getestet werden.

Allein die Frage, ob eine Person stationär ist oder sich bewegt, muss eine dem Radargerät angeschlossene Software zuverlässig erkennen. Der Hintergrund hierfür ist der Doppler-Effekt, anhand dessen ein Radar die Bewegung (und Geschwindigkeit) ermittelt. Ein Objekt, dass sich tangential zum Radar, also im gleichen Abstand vorbei bewegt, würde theoretisch nicht erfasst werden. Daher ist es wichtig, dass etwa ein menschlicher Körper per Micro-Doppler-Signatur in „Bestandsteile" wie Arme und Beine „zerlegt" wird, denn diese sind Teil einer Körperbewegung und können als solche getrennt vom Rumpf erfasst werden und dienen damit als Merkmal einer Bewegung des gesamten Körpers. Auf diese mitunter kleinsten Bewegungen ist auch zu achten, wenn der Körper per se ruht und sich nicht bewegt, denn sonst könnte er theoretisch nicht erfasst werden. Wo bei klassischen Anwendungen wie in der Luftfahrt ein einzelnes Radar für eine Überwachung von sich bewegenden Objekten über große Entfernungen hinweg reicht, können für Personen auch mehr Geräte an mehreren Stellen installiert werden, um die Detektionsgenauigkeit zu erhöhen. Eine entsprechende Positionierung der Geräte kann damit die Lokalisierung in einer dreidimensionalen Umgebung verbessern – in Geschwindigkeit, Entfernung sowie die horizontale und vertikale Winkelauflösung der Objekte.



Hochschule Niederrhein

Ein Spektrogramm – hier das eines Fahrrades – kann charakteristische Merkmale eines Objekts darstellen.

„Radar und Video können in Kombination ihre Stärken ausspielen und die Schwächen des jeweils anderen kompensieren."

Das System muss lernen

Damit sich Radardaten sinnvoll interpretieren und auswerten lassen, muss das System per Mustererkennung unter Einbeziehung von KI und Neuronaler Netzwerke lernen, „was" von einer Radarsignatur real ist. Im vom Staat geförderten Projekt „Klara" geht es um eine solche Mustererkennung. Mithilfe von abgestrahlten Mikro-Doppler-Signalen lassen sich jedem Objekt in einem Geschwindigkeits-Zeit Diagramm bewegungscharakteristische Profile zuordnen (Mensch, Gerät, Tier). Diese Spektrogramme können mit parallel gewonnen Bildern aus einer Videokamera annotiert werden, sodass später eine Zuordnung eines Spektrogramms zu einem Objekt automatisiert erfolgt. „Dazu sind eine Vielzahl an Daten notwendig. Personen und Objekte müssen dabei auch aus verschiedenen Winkeln erfasst werden, um die entsprechenden Charakteristika dem System antrainieren zu können", erläutert Dipl.-Ing. Reinhard Kulke von der IMST GmbH.

Einen Schritt weiter geht das vom Land Nordrhein-Westfalen gefördertes Forschungsprojekt „Kirapol.5G". In diesem Projekt haben sich verschiedene Unternehmen und Institutionen zusammengeschlossen, um die Einsatzmöglichkeiten von Radaren zur Überwachung öffentlicher Plätze zu entwickeln und zu testen. IMST liefert hierfür die Radartechnik mit 77 GHz Geräten und die Auswertung. Für das Projekt erweitert die TAS Sicherheits- und Kommunikationstechnik den Sicherheitsrouter um ein intelligentes 5G-Kommunikationsmodul, um die Schnittstellen des Radar-Sensors in die 5G-Netzarchitektur einzubinden. Damit können die Möglichkeiten moderner 5G-Netzarchitektur (realisiert durch M3connect) für Ausfallsicherheit und eine sichere End-to-End-Übertragung genutzt werden, um die Bild- und Radardaten in die Cloud zu übertragen.

Die Hochschule Niederrhein ist verantwortlich für die Entwicklung der Klassifikationskonzepte und generiert die Trainingsdaten. Denn bevor ein solches System live erprobt werden kann, sind eine Vielzahl an Tests und Vorbereitungen zu treffen. So müssen nun die aufgenommenen Mik-

100

GHZ kommen in der Messtechnik zum Einsatz.

ro-Doppler-Spektren auch Situationen abbilden können, die etwa im Falle von Personengruppen oder außergewöhnlichen Umständen eintreten können. So müssen nun auch unabhängig vom Projekt Klara Muster für beispielsweise in Panik davonrennende Menschen erzeugt und verknüpft werden.

„Und schließlich gilt es, für einen Versuch, bei dem mehrere Radargeräte involviert sind, diese untereinander so zu vernetzen, dass die Spektrogramme aus verschiedenen Winkeln und verschiedenen Geräten demselben Objekt zuzuordnen sind", so Kulke. Aufgrund des für Kirapol.5G ausgewählten, hohen Frequenzbandes (bei 76 bis 77 GHz) sind die genutzten Geräte nicht in der Lage, Objekte durch Hindernisse hindurch, wie Bäume, zu erkennen.

Datenschutz und Akzeptanz

Ein großer Vorteil eines Radarsystems ist, dass die Spektrogramme datenschutzrechtlich erstmal unbedenklich sind. Zum einen setzt man hier auf bewährte Technik der Automobilindustrie, die Radare auf 77 GHz-Basis seit Jahren einsetzt. Zum anderen lassen die Spektrogramme keinen Rückschluss auf eine Person zu. Bei der Videoüberwachung erzeugt die Kamera ein Bild, das zwar durch technische Verfahren ganz- oder teilweise für die eigentliche Auswertung unkenntlich gemacht werden kann, es letztlich aber immer erstmal „existiert" und damit den Datenschutz auf den Plan ruft. Ein Spektrogramm erlaubt diese personenbezogenen Rückschlüsse nicht. Gleichwohl ist es wichtig, dass eine solche verhältnismäßig neue Anwendung auf Personen bezogen, entsprechend von der Bevölkerung akzeptiert wird, weswegen die ethische Seite von der Hochschule Niederrhein von Anfang an mit betrachtet wird.

Was akzeptieren die Bürger, wo haben sie Vorbehalte (etwa 5G-Technologie) und wie muss man kommunizieren? „Hinzu kommen Fragen, die die diskriminierungsfreie Anwendbarkeit neuer Technologien betreffen, beispielsweise, ob Männer und Frauen hiervon gleichermaßen betroffen sind", erklärt Dr. Monika Eigenstetter von der Hochschule Niederrhein.

Ob die Implementierung von Radar als neue Sensorik zur Erfassung von Personen und Situationen alleine sinnvoll wäre, ist eher unwahrscheinlich. Wie beim Perimeterschutz scheint die Kombination aus Video- und Radarsystemen den größten Nutzen zu bringen. Radardaten können einen ersten Aufschluss über Situationen und Personen geben, die im Gefahrenfall von Videodaten unterstützt werden, etwa zur Strafverfolgung. Beide Systeme können in Kombination ihre Stärken ausspielen und die Schwächen des jeweils anderen kompensieren. Insofern bleibt abzuwarten, ob künftig vielleicht hybride System auch auf öffentlichen Plätzen den Durchblick haben. ■

HENDRICK LEHMANN, FREIER MITARBEITER PROTECTOR

TYPISCHE RADARQUERSCHNITTE
Quelle: Wikipedia

Radarquerschnitt [m²]	Gegenstand
0,00001	Insekt
0,0002	Flugzeuge mit Tarnkappentechnik am Beispiel der Lockheed Martin F-22
0,01	Vogel
<0,1	Flugzeuge mit Tarnkappentechnik
≈0,1	Flugabwehrraketen
1,0	Mensch
2–3	Kleines Kampfflugzeug
5–6	Großes Kampfflugzeug
10	PKW
<100	Transportflugzeug
300–4.000	Küstenmotorschiff (55 m Länge)
5.000–100.000	Fregatte (103 m Länge)
10.000–80.000	Containerschiff (212 m Länge)

KIRAPOL.5G | RADAR UND KÜNSTLICHE INTELLIGENZ (KI), DIE KOMBINATION DER ZUKUNFT

KIRaPol.5G

Künstliche Intelligenz für Radarsysteme zur Unterstützung von polizeilichen Überwachungen auf öffentlichen Plätzen und Bahnhöfen

Kurzbeschreibung:

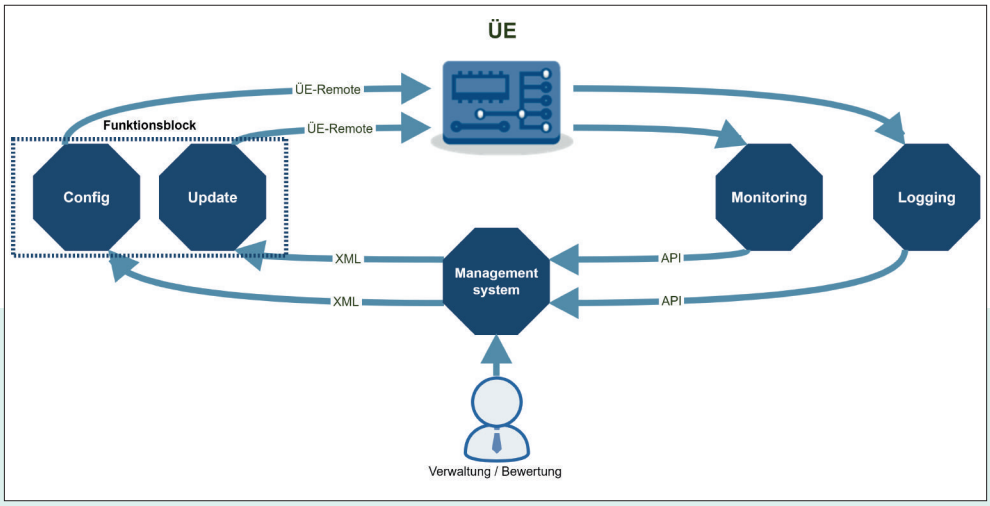
KIRaPol.5G ist ein vom Land Nordrhein-Westfalen gefördertes Forschungsprojekt. Es hat das Ziel, die polizeiliche Überwachung in öffentlichen Bereichen dort zu unterstützen, wo es möglicherweise zu Zwischenfällen kommen kann, die eine potentielle Gefahr für Bürger*innen darstellt. Unter bestimmten Voraussetzungen und innerhalb strenger Vorgaben ist es der Polizei erlaubt, Videotechnik zur Überwachung dieser öffentlichen Plätze einzusetzen. Die Partner im Projekt KIRaPol.5G wollen eine alternative Sensortechnik entwickeln und testen, die die Vorteile hat, dass die innovativen Radarsensoren anonymisierte Daten erfassen und unabhängig von Lichtverhältnissen und Wetterbedingungen arbeiten. Durch Künstliche Intelligenz (KI) unterstützte Algorithmen sollen trainiert werden, bestimmte gefahrenträchtige Situationen frühzeitig zu erkennen und die Polizei auf eine mögliche Gefährdung aufmerksam machen. Die Radarsensoren und Videokameras, die zum Trainieren der Neuronalen Netze (NN) notwendig sind, werden in Versuchsinstallationen in ein lokales 5G-Netz eingebunden, um die Radar- und Videodaten mit hoher Übertragungsrate und bestmöglichem Datenschutz zu einer Auswertungszentrale in der Cloud zu übertragen. Die technische Entwicklung, Installation und Erprobung wird von Experten für ethische, legale und soziale Aspekte (ELSA) begleitet und bewertet. Projektpartner aus Industrie, Wissenschaft und Sicherheitsbehörden erarbeiten gemeinsam diese Technologie. Tests und Demonstrationen werden in Bereichen der Stadt Mönchengladbach durchgeführt. Die IMST GmbH hat für KIRaPol.5G die Projektleitung übernommen und ist verantwortlich für die Radartechnologie. Das Projekt wird begleitet vom Competence Center 5G.NRW (CC5G.NRW). Partner und assoziierte Partner sind:

- IMST GmbH, Kamp-Lintfort (IMST, Projektleitung)
- Hochschule Niederrhein (HSNR), Krefeld
- Telefonbau Arthur Schwabe GmbH (TAS), Mönchengladbach
- M3-Connect GmbH (m3c), Aachen
- Polizeipräsidium Mönchengladbach (POLMG)
- Bundespolizei (BPOL), Potsdam (assoziiert)
- Bayrisches Landeskriminalamt (BLKA), München (assoziiert)

Automatische Konfiguration von Übertragungseinrichtungen als Lösung

Neue Anforderungen führen bisherige Prozesse an die Grenze des Leistbaren

AUTOR: DANIEL KAUMANNS



Device-Management-Kreislauf (Grafik: TAS)

Bisherige Prozesse zu Konfiguration und Aufschaltung stoßen an ihre Grenzen

Die bislang mehrheitlich manuellen Prozesse zur Konfiguration von Übertragungseinrichtungen (ÜE) und Aufschaltung der Übertragungsgeräte auf eine Alarmempfangsstelle (AES) stoßen angesichts komplexer werdender Anforderungen an ihre Grenzen. Errichter und Dienstleister, die die Übertragungseinrichtungen in Betrieb nehmen, warten und verwalten, stehen vor der Herausforderung, die verschiedenen Konfigurationsansätze und Funktionsumfänge der ÜE-Hersteller bei der Konfiguration der ÜE zu berücksichtigen.Daraus ergibt sich ein erheblicher Verwaltungs- und Schulungsbedarf bei den Unternehmen. Auch die expliziten Vorgaben der jeweiligen Alarmempfangsstellen hinsichtlich zu verwendender Übertragungsparameter und -modi für eine reibungslose und fehlerfreie Kommunikation sind zu berücksichtigen.

Hinzu kommen die entsprechenden Funktionsanforderungen sowie die normativ geforderten Überwachungen der Komponenten gemäß DIN EN 50136-1.

Dies führt zu einer Vielzahl an Problemstellungen:

- ❏ Manuelle Konfiguration vor Ort nur noch bedingt durch Servicetechniker vollständig leistbar.
- ❏ Unklare Aufschaltbedingungen: DP3 oder DP4 oder reicht auch SP4?
- ❏ Erhöhter Abstimmungsbedarf mit der AES.
- ❏ Heute sind teils keine Updates bzw. sofortigen Reaktionen auf Sicherheitsvorfälle möglich.

VdS 3886: Entlastung und einheitliche Strukturen

In Zukunft soll die herstellerunabhängige Konfigurationsschnittstelle der Richtlinien VdS 3886 den gestiegenen Anforderungen an die Konfiguration und Pflege der Übertragungseinrichtung gerecht werden.

Die Richtlinien VdS 3886 definieren eine einheitliche Struktur auf Basis von XML. Sie soll:

1. einheitliche Konfigurationsschnittstellen schaffen, sowohl auf Seiten der ÜE als auch der Alarmempfangsstelle, sowie
2. den Zugriff auf die ÜE auf Basis einheitlicher Standards ermöglichen.

Die beschriebenen Spezifikationen stellen allerdings lediglich eine Mindestfestlegung zwischen ÜE und AES dar. Aufgrund der abweichenden Funktionsumfänge der ÜEs wurde zudem ein herstellerspezifischer Teil in der VdS 3886 freigehalten, um herstellerspezifische Zusatzfunktionen konfigurieren zu können.

Dabei handelt es sich um die Beschreibung des Aufbaus dieser vereinheitlichten Konfigurationsstruktur und nicht um die Art der Übertragung oder die Art des Verbindungsaufbaus zur Konfigurationsübertragung. Genau diese Informationen werden jedoch für neuartige Dienstleistungen benötigt, auf einen möglichen Ansatz für solche Dienstleistungen kommen wir im letzten Abschnitt dieses Artikels.

Welche Akteure sind beteiligt?

Am Prozess zur Aufschaltung einer ÜE auf eine AES sind mehrere Parteien beteiligt.Zum einen sind dies der Errichter der Übertragungseinrichtung sowie die AES. Zum anderen ist in der DIN EN 50136-1 die Rolle des Alarm Transmission Service Providers (ATSP) verankert, der den gesamten Aufschaltprozess sowie die

Alarmkommunikation und die Überwachung der entsprechenden Leistungskriterien verantwortet. ATSP und AES-Betreiber können ein und dieselbe Instanz sein. In der Praxis übernehmen bereits viele AES die Dienstleistungen des ATSP.

Die Verantwortung für die fehlerfreie normkonforme Konfiguration einer ÜE liegt beim ATSP, dieser betreibt hierzu im Regelfall ein entsprechendes übergeordnetes Managementsystem, das als steuernde Instanz fungiert. Hier werden sowohl die für eine Aufschaltung notwendigen Daten (z. B. Verschlüsselungs- und Legitimationsinformationen) erzeugt und/oder verwaltet, als auch die Stammdaten der aufgeschalteten ÜE, des entsprechenden Betreibers respektive des Schutzobjekts verwaltet. Handelt es sich beim ATSP nicht um die AES, muss das Managementsystem entsprechende Schnittstellen zu den benötigten Daten für die Aufschaltung haben.

Abschied vom herstellerspezifischen Konfigurator?

So weit wird es noch nicht kommen, da eine Vielzahl von unterschiedlichen Übertragungseinrichtungen am Markt existieren, die allesamt unterschiedliche Möglichkeiten der Konfiguration aufweisen. Managementsysteme können allerdings keine universelle Konfiguration erzeugen, die von allen ÜE verstanden wird. Im Rahmen der VdS 3886 wurden hierzu entsprechende Konfigurationsdaten strukturiert, um sie für das Managementsystem als auch für die ÜE zu vereinheitlichen. Da die wenigsten ÜE die XML-Struktur verstehen können, wurde der Funktionsblock definiert. Der Funktionsblock ist als logische Komponente zu betrachten und dient als „Übersetzer" zwischen dem Managementsystem und der ÜE. Er ist also der herstellerspezifische Konfigurator, der die Konfiguration für das ÜE aufbereitet.

Komplett-Management von Übertragungseinrichtungen

Das Managementsystem kann das Übertragungsgerät mit korrekten Leitstellenzielen ausstatten – es lässt sich aber auch für weitere zukunftsweisende Dienstleistungen nutzen. Aus Sicht des Errichters kommen hier Anforderungen nach kontinuierlichen Updates, Sicherheits-Patches, Monitoring und Fernzugriff auf Anlagendaten hinzu. Diese Funktionen werden jedoch nicht von den VdS 3886 definiert, gehören aber zur vollumfänglichen Betrachtung für das Management einer Übertragungseinrichtung hinzu.

Der Fernzugriff auf technische Anlagen hat viele Vorteile und ist gängige Praxis. Auch bei Alarmsystemen setzen viele Unternehmen auf Remote Services, um z. B. teure Vor-Ort-Einsätze zu reduzieren und durch kontinuierliches Monitoring eine bessere Verfügbarkeit der Systeme zu gewährleisten. Hierunter zählen auch Dienste wie das Einspielen von einheitlichen Konfigurationen aus der Ferne, wozu wiederum die Anforderungen der VdS 3886 erfüllt werden müssen.

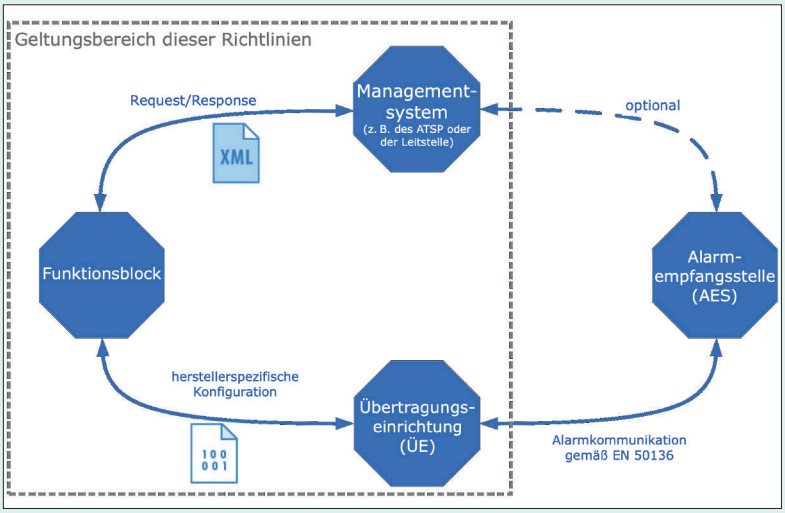
In der Praxis kann somit der Techniker vor Ort das Gerät installieren und muss die Konfiguration der AES Parameter nicht mehr aufwendig manuell eingeben. Ein Anruf beim ATSP oder beim zentralen eigenen Service-Center genügt, um das Aufspielen der korrekten Konfiguration zu veranlassen.

Solche Dienstleistungen müssen entsprechend der geltenden und entstehenden Normen durchgeführt werden, hierbei wird in der EN 50710 die Dienstleistung und in der prTS 50136-10 der Aufbau der technischen Infrastruktur und die Verantwortlichkeit für diese beschrieben. Sie obliegt dem Remote Access Infrastructure Provider (RAISP), lt. Definition „eine Person/Institution, die für die Gestaltung, den Betrieb, das Management und die Überprüfung der Leistungsmerkmale der Remote Access Infrastructure (RAI) verantwortlich ist". Ähnlich dem ATSP bedeutet dies: Der Service Provider, der die Infrastruktur für Remote Services zur Verfügung stellt, ist verantwortlich für die ständige Verfügbarkeit und IT-Sicherheit des Remote Access – unter Einhaltung der Datenschutz-Richtlinien. Diese zentrale Plattform muss nicht zwingend eine Leitstelle darstellen.

Fazit

Auch externe Dienstleister können die vereinheitlichte XML-Konfigurationsstruktur nutzen, um beispielsweise einen Fernzugriff über ein Fernwartungsportal aufzubauen, aber auch eine sichere Konnektivität für dahinter geschaltete Anlagen zu konfigurieren – abseits klassischer Alarmverbindungen. Diese Ansätze benötigen jedoch herstellerspezifische Funktionen, die sich bei den am Markt befindlichen Geräten im Leistungsumfang unterscheiden können.

Die VdS 3886 sind somit – neben den gültigen Normen, DIN EN 50136-1, EN50710, prTS50136-10 und weiteren Richtlinien – ein wichtiger Baustein im Umfeld der Digitalisierung der Aufschaltungs- und Fernwartungsprozesse von Übertragungseinrichtungen.



Geltungsbereich der Richtlinien VdS 3886 (Grafik: VdS)

Der Autor dieses Beitrags, ***Daniel Kaumanns, MBA***, ist Produktmanager für Übertragungstechnik und Remote Services bei TAS Sicherheits- und Kommunikationstechnik.

Kontakt: daniel.kaumanns@tas.de

PROTECTOR

1-2|2022
Januar / Februar
50. Jahrgang

ASW Bundesverband –
Allianz für Sicherheit in der Wirtschaft e.V.

schlütersche
www.sicherheit.info

Ansprechend

Netzwerk-Audio-Systeme im Einzelhandel zur Kundenansprache | **26**

Vernetzt

Sicherheitstechnik im Einzelhandel schützt Kunden und Waren | **34**

Verschlüsselt

Systemsicherheit von Zutrittskontrollsystemen erhöhen | **42**

Klug den Verkehr überwachen

Edge-basierte Videoanalyse von Hanwha Techwin erkennt Marke, Modell und Farbe | **18**

Foto: Hanwha Techwin

Foto: monticelllo - stock.adobe.com

Vernetzte Sicherheitstechnik im Einzelhandel sorgt nachhaltig für mehr Schutz von Kunden, Mitarbeitern und Waren.

Gut vernetzt und effizient

Wie sich durch sinnvolle Vernetzung von Sicherheitstechnik im Handel ein Plus an Sicherheit herstellen lässt – für Menschen und Waren.

TAS SICHERHEITS- UND KOMMUNIKATIONSTECHNIK

Auf Sicherheitstechnik im Handel kann heute kaum mehr verzichtet werden: Bedingt durch die Pandemie sind die Fallzahlen für Ladendiebstähle in 2020 etwas zurückgegangen, aber sie sind mit rund 304.000 Fällen nach wie vor auf einem hohen Niveau und verursachen der Wirtschaft einen jährlichen Schaden in Milliardenhöhe. Der Fokus der Diebstähle liegt schwerpunktmäßig auf Shops und Filialen, doch auch die Lager geraten zunehmend ins Visier der Täter, die zudem immer professioneller vorgehen und teilweise straff organisiert sind. Videoüberwachungslösungen für den Einzelhandel sind mittlerweile Standard im Kampf gegen Ladendiebe und Inventurdifferenzen, meist sind sie allerdings nur ein Teil der Gewerke, die sicherheitstechnisch ineinandergreifen.

Zentraler Baustein einer integrierten Sicherheitslösung für den Handel sind sie dennoch. Moderne Systeme in HD-Auflösung ermöglichen eine Strafverfolgung durch eindeutige Aufnahmen im Rahmen datenschutzrechtlicher Regelungen. Zudem können sie Täter bereits im Vorfeld abschrecken, vor allem dann, wenn sie keine Schlupflöcher lassen und auf Verkaufsflächen, im Warenlager und in den Außenbereichen installiert sind. Am Objekt selbst wird die Videoüberwachung in der Regel mit einer Einbruchmeldeanlage kombiniert. Sie sind ein weiterer wichtiger Bestandteil präventiver Maßnahmen, um Objekte wirkungsvoll zu schützen. Öffnungskontakte an Zutrittspunkten sorgen für eine sofortige Alarmierung während eines Einbruchversuchs. Innerhalb eines Objekts sichern Bewegungsmelder Räumlichkeiten und Zugänge zuverlässig ab. Sie helfen auch in den Fällen, in denen sich Täter vorher eingeschlichen und versteckt haben, um nach Ladenschluss loszuschlagen.

Gerade bei großen Warenlagern empfiehlt sich die Kombination der Videoüberwachung mit Perimeterschutz-Systemen. Hier kommen auch Flächenüberwachungen mit Laser oder Radartechnologie zum Einsatz. Mechanische Schutzvorrichtungen wie Zäune, Schranken und Tore sind optimal, um das Gelände einzufrieden und einen schnellen, einfachen Zugang zu verhindern. Ebenso wichtig ist eine geordnete Zutrittskontrolle, etwa wenn es um Lieferanten und Berechtigungen für die Warenlager geht. Solche Zutrittskontrolllösungen lassen sich ebenfalls mit der EMA für ein Maximum an Sicherheit verknüpfen.

Effizient und sicher: Fernzugriff auf Alarmsysteme

Gerade im Einzelhandel mit seinen Filialen und Ladenketten stehen Verantwortliche vor der Frage, wie sich sicherheitstechnische Anlagen effizient warten lassen. Eine Antwort darauf sind Wartungen, die aus der Ferne vorbereitet oder durchgeführt werden. Das bedeutet, dass sich ein Servicetechniker nicht zwingend in das Objekt begeben muss, um etwa Fehlerzustände eines Alarmsystems

zu analysieren. Eine einzelne Fernwartungslösung pro Gewerk kann allerdings den Effizienzgewinn durch Remote Services schnell wieder zunichtemachen. Zudem besteht die Gefahr von Sicherheitslücken aufgrund einer Vielzahl von Zugangsmöglichkeiten.

Viel effizienter ist hier eine Plattform, über die der Fernzugriff gewerkeübergreifend erfolgt. Ein solches System bietet das Unternehmen TAS Sicherheits- und Kommunikationstechnik mit seiner TAS Secure Platform. Darüber lässt sich ein sicherer Fernzugriff (Remote Access) auf Alarmübertragungseinrichtungen und nachgeschaltete Gefahrenmeldeanlagen realisieren. Über die TAS Secure Platform können zentral Software-Updates für eine Vielzahl an Systemen und Gewerken aufgespielt werden. Die Möglichkeit, bei Fehlerzuständen aus der Ferne auf das Gerät zuzugreifen, spart nicht nur Zeit und Geld, sondern vermeidet in Pandemie-Zeiten unnötige Kontakte. Servicetechniker müssen nur in „echten" Notfällen vor Ort sein und sind dann dank der Daten auch gleich optimal auf ihren Einsatz vorbereitet.

Cybersicherheit im Fokus von Einzelhändlern

Aus Sicht der Cyber Security ist es allerdings notwendig, höchste Sicherheitsanforderungen an die Fernzugriffspunkte zu stellen. Daher ist es nicht sinnvoll, eine Vielzahl an unreglementierten Zugriffspunkten zu betreiben. Cyberkriminelle könnten im Falle einer nicht ausreichend gesicherten Verbindung Zugang zum Netzwerk und damit auf die Gewerke selbst erhalten, diese in ihrem Sinne manipulieren und ausschalten. Mit der TAS Secure Platform bietet der Spezialist für Sicherheits- und Kommunikationstechnik einen ganzheitlichen Ansatz. Denn das Unternehmen stellt nicht nur die Infrastruktur für Leitstellen-Betreiber und Errichter zur Verfügung, sondern übernimmt als Remote Access Infrastructure Service Provider (RAISP) die Verantwortung für den Aufbau und die Sicherheit der Fernzugriffsinfrastruktur. Diese wird unter anderem durch Mehrfaktor-Authentifizierung, Verschlüsselungsverfahren, Mandantentrennung mit gesicherter zentraler System-/Kundendatenverwaltung und Pflege gewährleistet. All diese Maßnahmen ermöglichen einen sicheren Zugang über die TAS Secure Platform auf die angebundenen Gewerke. Durch die kontinuierliche Weiterentwicklung bleibt die Plattform stets auf aktuellem Stand und bietet nicht nur dem Einzelhandel mit der Zentralisierung wichtiger Wartungsfunktionen einen echten Mehrwert im Hinblick auf Kosteneffizienz und Sicherheit. ■

TAS Sicherheits- und Kommunikationstechnik:
www.tas.de