Quelle: Axis Communications

Expertendiskussion am Runden Tisch

Vernetzte Sicherheit im Smart Building

Beim ersten Round Table zum Thema »Vernetzte Sicherheit im Smart Building« setzten sich Errichter, Sachverständiger, IT-Experte, Fachverband und Hersteller gemeinsam an den virtuellen Diskussionstisch. Hier zeigte sich schnell, welche Sicherheitsrisiken durch fehlende Normen und eine große Komplexität der technischen Ausrüstung entstehen. Und dass eine gute Planung intelligenter Gebäudevernetzung immer erfordert, alle Beteiligten von Anfang an mit ins Boot zu holen.

Warum übereinander reden, wenn man auch miteinander reden kann? Frei nach diesem Motto trafen sich die Teilnehmer des ersten Round Tables »Vernetzte Sicherheit im Smart Building« Corona-bedingt zum Fachgespräch im virtuellen Konferenzraum. Hier nahmen Platz: *Peter Krapp* (Geschäftsführer Fachverband Sicherheit ZVEI), *Philipp Rothmann* (Cyber-Sicherheitsberater bei itsecurity-coach), *Sascha Puppel* (öffentlich bestellter und vereidigter Sachverständiger für Sicherheitstechnik und Sicherheitskonzepte), *Uwe Gleich* (Geschäftsführer Gleich GmbH Sicherheits- und Medientechnik) sowie *Jochen Sauer*, Business Development Manager beim Netzwerk-Video-Anbieter Axis Communications, der den Round Table organisiert hatte. Die Moderation übernahm Dr. *Clemens Gause* (Geschäftsführer VfS – Verband für Sicherheitstechnik e.V.).

Dr. Clemens Gause: Ich möchte die Diskussion zur vernetzten Sicherheit mit der Frage nach der aktuellen Lage der Sicherheitstechnik in der Verbandsarbeit eröffnen.

Peter Krapp: Beim ZVEI ist die vernetzte Sicherheit seit langem ein großes Thema. Wir sind ein vielschichtiger, diversifizierter Verband mit einer großen Community, der viele unterschiedliche Projekte betreut. Es gibt beispielsweise aktuell das Projekt »Sense«, das sich an Entwickler richtet, die der Frage nachgehen, wie ein Produkt mit dem eines anderen Herstellers kommunizieren kann.

Ein weiteres, weitaus größeres Projekt – »Foresight« – beschäftigt sich mit dem Thema Smart Home, erweitert um KI, und damit, wie dies richtig zu installieren ist und wie die »Total Cost of Ownership« dabei aussieht.

Zusätzlich spielt auch die 5G-Entwicklung in der Elektroindustrie eine große Rolle. Das Thema kommt aus der Automation, da die Industrie den Fertigungsprozess mittels 5G optimieren kann. Die Relevanz dieser Technologie ist hoch, denn darüber kann auch jedwede andere Peripherie vernetzt werden. Das beschäftigt in Zukunft daher auch die Sicherheitstechnik.

C. Gause: Ich sehe ein starkes Branchenwachstum in den letzten drei bis vier Jahren von sechs bis acht Prozent – auch im Jahr 2020 ist die Sicherheitstechnik sehr stark gewachsen. Was sind jedoch die Gefahren, die durch dieses Wachstum bedingt sind?

Philipp Rothmann: Das ist sehr vielschichtig. Die große Anzahl an Produkten und Dienstleistungen führt zu einer Fülle an Herstellern, Partnern, Errichtern und IT-Dienstleistern, die im Prozess eingebunden sind. Dadurch entsteht ein hoher Abstimmungs- und Standardisierungsbedarf. Die Gefahren, die sich ergeben, liegen also einerseits auf der Normenebene in der fehlenden Standardisierung und auf der Projekt- und Realisierungsebene in fehlenden Abstimmungen, zum Beispiel zum Datenschutz.

Außerdem hat sich die Angriffsfläche vergrößert: 5G bedeutet nämlich, dass große Datenmengen erzeugt werden. Diese Daten werden durch Cyberangriffe wie Denial of Service- und DDoS-Attacken bedroht. Errichter brauchen daher Know-how und vor allem kompetente Partner, die beispielsweise Abnahmeprüfungen wie Pen-Tests durchführen und die Schnittstellen im Auge behalten.

Sascha Puppel: Die Komplexität der Schnittstellen zwischen den Systemen ist sicher eine akute Gefahrenstelle. Aber auch die Schnittstellen in der Planungsphase können ein Hindernis sein – die Kommunikation und Vernetzung funktioniert bereits hier im Vorfeld der Umsetzung eines Projekts häufig nicht. Es gibt zwar zahlreiche, auch hilfreiche Normen. Die notwendigen Funktionen – insbesondere die Betriebsanforderungen – der jeweiligen Anlage werden aber vorab häufig nicht geklärt. Dabei ist die Kommunikation mit dem Kunden zentral.

Die aktuellen Regelwerke und Normen zu kennen ist das eine, sie auch anzuwenden und eine Anlage sauber durchzuplanen das andere. Der angesprochene boomende Markt tut sein Übriges: Planer und Errichter mit fragwürdigem Wissen erscheinen auf der Bildfläche. Um deren Qualifikation in der Praxis einzuschätzen, gibt es beispielsweise die DIN EN 16763, die als Entscheidungshilfe dienen kann.

Uwe Gleich: Ich kann mich da Herrn Puppel nur anschließen. Aus meiner Sicht wird in der Baubranche sehr viel »gepfuscht«. Die Errichter sind allesamt ausgelastet, das fördert weder Innovation noch Flexibilität. Noch dazu kommen die meisten Aufträge über die Generalunternehmer. Mit anderen Worten: der Nutzer des Gebäudes wendet sich für Sicherheitsanlagen an den Vermieter, der wiederum an einen Investor, der wendet sich wiederum an eine Baufirma und diese an einen Nachunternehmer – und so weiter. Zu viele Mitspieler, was nicht zu einer Transparenz der Kommunikation untereinander beiträgt, um mögliche Schwachstellen im Vorfeld aufzudecken und abzustellen.

Das bedeutet im Endeffekt, dass der Errichter für Sicherheitstechnik und der Nutzer des Gebäudes keine direkte Verbindung zueinander haben und der Nutzer durch diese lange Kommunikationskette fast keinen Einfluss mehr hat auf das, was gebaut wird. Auch die Sparmaßnahmen und die reine Vergabe nach Preis, ohne Rücksicht auf den Betrieb des Systems, stellen häufig eine Gefahrenstelle dar.

C. Gause: Welche Forderungen und Lösungsmöglichkeiten gibt es für diese komplexen Wege?

Quelle: Sachverständigenbüro Puppel

Sascha Puppel: *»Die aktuellen Regelwerke und Normen zu kennen ist das eine, sie auch anzuwenden und eine Anlage sauber durchzuplanen das andere.«*

S. Puppel: In der frühen Phase, d. h. am besten noch vor der genauen Planung, sollte die Abstimmung bereits zwischen den involvierten Parteien erfolgen. Dies sollte in ähnlicher Weise wie bei Brandmeldeanlagen erfolgen. Hier gibt es die normative Anforderung, noch vor der Planung ein Brandmelde- und Alarmierungskonzept zu erstellen. Es müssen dann die Fragen gestellt werden, was alles dazu gehört, welche Bedrohungen denkbar sind, welche Schutzziele es gibt, was die Anforderungen des Objektes sind, usw., um eine Risikobewertung zu erstellen. Daraus sollte dann ein Konzept, mithilfe der ISO-31000, entwickelt werden.

Diese typischen Planungsschritte vorherzusehen, spart am Ende viel Arbeit. Errichter müssen sich außerdem trauen, die eine oder andere Planung infrage zu stellen. Außerdem darf die Sicherheitstechnik nicht im

Quelle: itsecuritycoach

Philipp Rothmann: *»Eine intelligente Anwendung nutzt nichts, wenn zwei Drähte aus der Tür kommen, die man nur zusammendrücken muss, um die Tür zu öffnen.«*

Pool der Elektrotechnik untergehen. Stattdessen braucht die Sicherheitstechnik in Leistungsverzeichnissen bzw. Ausschreibungen ein eigenes Fachlos. Dies führt zu einer höheren Qualität und besserer Kommunikation.

U. Gleich: Nutzer müssen sich darüber hinaus für den Dienstleister entscheiden und sich unbedingt im Vorfeld Gedanken um den weiteren Betrieb machen, der erst im Anschluss erfolgt, nicht nur um die einmalige Investition. Bau und Betrieb lassen sich in dieser Form nicht voneinander trennen.

C. Gause: Auf welche Bedrohungen müssen sich Nutzer und Betreiber von Sicherheitsanlagen im vernetzten Gebäude denn einrichten? Gerade aktuell, wo 80 Prozent unseres Lebens in Gebäuden und Liegenschaften stattfindet?

S. Puppel: Es gibt keine statische Definition hierfür. Bedrohungen können sich schnell und dynamisch verändern. Das ist einer ihrer elementaren Bestandteile. Diese Dynamik bedeutet, dass auch zu Videosicherheitssystemen regelmäßige Begehungen durchgeführt werden sollten, um zu bewerten, inwiefern das Konzept weiterhin Sinn ergibt und wie sich baulich oder in der Nutzung ggf. seit der letzten Begehung Änderungen ergeben haben.

Diese Begehungen sind bereits für Gefahrenmeldeanlagen in der DIN VDE 0833-1 definiert. In der Praxis geschehen sie jedoch nur selten. Eine Begehung und Prüfung erfolgt meistens nicht, mögliche Bedrohungen werden schließlich zu spät festgestellt. Hier brauchen wir Betreiberpflichten. Im Bereich der Sicherheitstechnik würde ich mir persönlich diesbezüglich mehr Normenvorgaben wünschen.

C. Gause: Um nochmals genauer auch auf die vorhin angesprochenen Normen und Regeln einzugehen: Es gibt doch schon so viele davon. Können mehr Normen also die Lösung sein?

P. Krapp: Ein wichtiger Punkt. Es gibt bereits sehr viele Normen und Standards sowie Merkblätter und ähnliches zur Interpretation ihrer Umsetzung. Aber letztere ist oft schwierig. Ein Beispiel ist unser Merkblatt für Betreiber von Gefahrenmeldeanlagen. Häufig scheitert die Umsetzung an der Frage der Verantwortung – ist die Zentrale oder die Filiale für die Umsetzung verantwortlich? Keiner möchte sich wirklich darum kümmern.

Quelle: ZVEI/Maren Strehlau

***Peter Krapp:** »Vernetzen kann man im Prinzip alles, aber es gibt Geräte und Systeme, die wir – aus verschiedenen Gründen – nicht unbedingt vernetzen sollten.«*

Gleichzeitig erleben wir einen sich beschleunigenden, technologischen Fortschritt. Immer feiner ziselierte Normen sind hier aus meiner Sicht nicht unbedingt die Lösung. Vielmehr muss man Planer dazu bringen, aus den bestehenden Normen mehr herauszuholen und sie gezielter in der Praxis anzuwenden.

U. Gleich: Wir können gewisse Regeln auch umsetzen, selbst wenn es dazu keine offiziellen Normen gibt. Hinzu kommt, dass viele Normen nicht auf der Höhe der Zeit sind, da der Normierungsprozess so langwierig ist. Stattdessen müssen wir in der Industrie gemeinsame Standards definieren und uns an diese branchenweit dann auch entsprechend halten.

Jochen Sauer: Klar, wir sollten, können und müssen Standards zukünftig besser leben. Bauprojekte mit großen Verzögerungen und zusätzlichen Kosten wie der BER oder die Elbphilharmonie entstehen nicht dadurch, dass uns der Rahmen für die Standardisierung fehlt. Alle Projektbeteiligten müssen sich daher im Vorfeld die Frage stellen, welches Schutzziel besteht. In welche Richtung soll das Projekt laufen? Dafür müssen aber alle Stakeholder an einen gemeinsamen Tisch, um die Betriebsanforderung, die notwendig ist, zu erstellen. Die Gesamtkostenbetrachtung und der Nutzen der Anlage über die komplette Nutzungsphase hinweg müssen im Zentrum der Überlegungen stehen. Aktuell befinden wir uns leider oft in einer Situation, in der das Anforderungsprofil nicht genau genug gefasst wird.

S. Puppel: Mehr Normen sind vielleicht nicht die richtige Antwort. Vielmehr sollten wir die eine oder andere Norm besser spezifizieren. Ich stelle das immer wieder in der Praxis mit verbändeübergreifenden Infopapieren fest. Wenn der Errichter diese Papiere an der Hand hat, hat das eine ganz andere Wirkung auf die restlichen Stakeholder. Diesen Weg müssen wir forcieren, denn hier erhalten wir positive Rückmeldungen vom Markt. Es geht im Kern also darum, die Betreiber bereits in der Planungsphase informativ abzuholen, damit nicht Videosicherheitslösungen installiert werden und die IT-Sicherheit vergessen wird. Hier benötigt es mehr Aufklärungsarbeit.

C. Gause: Was muss in Sachen Aufklärung zum Smart Home gemacht werden?

P. Rothmann: Ich selbst habe beispielsweise erst seit vier Jahren Berührungspunkte mit dem Bereich Sicherheitstechnik und betreibe inzwischen ein kleines »Smart-Home-Labor«. In der Errichtung des Labors hat sich gezeigt, dass Hersteller schnittstellenübergreifend lange nicht viele Informationen an der Hand hatten. Das Gewerk war zusammen mit dem Know-how abgekapselt. Dadurch herrscht immer noch eine recht große Diskrepanz zwischen Sicherheitstechnik und Cybersecurity-Maßnahmen. Ich sehe das beispielsweise am Thema Verschlüsselungsmaßnahmen. Kunden kommen dabei mit der Frage auf mich zu, welche Funklösung sie für ihre Zutrittskontrolle verwenden sollen (RFID, etc.). Eine intelligente, informationssichere Anwendung nutzt allerdings nichts, wenn zwei Drähte aus der Tür kommen, die man nur zusammendrücken muss, um die Tür zu öffnen.

Es muss noch viel mehr Verständnis zwischen den einzelnen Disziplinen aufgebaut werden. Es braucht eine Kombination aus physischer Sicherheit und IT-Sicherheit. Wir müssen also eine Vertrauenskette im Planungsprozess integrieren, die die notwendige Qualitätssicherung schafft. Diese Vorgehensweise wird inzwischen punktuell umgesetzt. Ich bin beispielsweise in Kameraprojekte eingebunden, die in Hochsicherheitsbereichen eingesetzt werden, bei denen der Stress-, Schwachstellen- und Abnahmetest auch in Bezug auf Informationssicherheit gemacht wird. Solche Projekte gibt es, sie sind aber noch nicht flächendeckend umgesetzt.

U. Gleich: Außerdem sollte man den Errichtern, Betreibern und Nutzern aufzeigen, welche Kompetenzen aus den einzelnen Disziplinen vorhanden sind und wie diese gegenseitig genutzt werden können. Es gilt, ihnen die Diskrepanz zwischen einem offenen WLAN kombiniert mit einem Gitter vor dem

Fenster aufzuzeigen. Kombinierte Penetrationstests könnten eine Maßnahme sein.

C. Gause: Gibt es Geräte oder Dinge, die wir gar nicht vernetzen wollen?
U. Gleich: Aus meiner Sicht: nein. Es gibt keine Bereiche, die wir nicht vernetzen wollen, zumindest nicht, wenn die verwendete Technik auf dem neuesten Stand ist. In der Industrie kommt es immer mal wieder vor, dass beispielsweise Notausknöpfe oder ähnliches bewusst nicht vernetzt werden, aber diese Kategorie an Geräten oder Dingen bildet die Ausnahme.
P. Krapp: Es gibt Endgeräte, bei denen man die Safety-Funktion abkoppelt, also bewusst nicht vernetzt. Diese Abkopplung erfolgt einerseits zum Schutz des Menschen vor der Maschine oder zum Schutz der Maschine vor dem Menschen. Vernetzen kann man im Prinzip alles, aber es gibt Geräte und Systeme, die wir – aus verschiedenen Gründen – nicht unbedingt vernetzen sollten.

C. Gause: Wie soll man mit Anwendern umgehen, die nicht technikaffin sind?
J. Sauer: Dabei hilft ja gerade die Schnittstelle zwischen Mensch und Maschine. Am besten können wir das am Beispiel Autofahren heute und vor 30 Jahren vergleichen. Früher waren die Autofahrer mit Straßenkarten auf dem Schoß unterwegs und konnten Staus nicht präventiv umfahren. Heute gibt es smarte Navigationssysteme, die uns vor Staus und Gefahren auf der Autobahn warnen und die schnellsten Routen automatisch kalkulieren.

Quelle: Gleich GmbH

Uwe Gleich: *»Welcher Autofahrer checkt seinen Airbag wirklich, bevor er losfährt? Langfristig muss Sicherheitstechnik zu einer Selbstverständlichkeit werden.«*

U. Gleich: Um diesen Vergleich einmal aufzugreifen – welcher Autofahrer checkt seinen Airbag wirklich, bevor er losfährt? Nutzer müssen sich aktuell noch erst aktiv mit dem Thema Sicherheitstechnik beschäftigen wollen. Langfristig muss Sicherheitstechnik jedoch zu einer Selbstverständlichkeit werden.
J. Sauer: Genau, der Nutzer muss sehen und spüren, dass die Technik ihm das Leben erleichtert. Die Sicherheitstechnik muss den Nutzer nachts ruhig schlafen lassen. Dieses Verständnis und Bewusstsein muss nicht nur bei den Betreibern und Fachplanern tiefer verankert werden: Standardisierte Prozesse müssen Anwendung finden, beispielsweise, wenn sich eine Kamera mehrfach resettet, muss das über ein Störmeldemanagement erkennbar sein.

Das sind die Punkte, die auf dem Radar der Verantwortlichen sein sollten – dazu gehört auch im Wesentlichen Vertrauen. Vertrauen in den Fachplaner, den Hersteller, den Integrator, und auch in die Person, die meinen Cybersecurity-Test durchführt. Die fachmännische Beratung ist der Weg dorthin. Als Autofahrer muss ich auch nicht unbedingt wissen, wie viele Airbags im Auto installiert sind. Allerdings muss ich wissen, dass die Airbags im Notfall funktionieren, um mich entsprechend zu schützen.
S. Puppel: Ja, das ist richtig, aber dafür müssen regelmäßige Sicherheitsupdates zur Verfügung gestellt werden. In der Praxis wird das häufig vergessen, vor allem der betrachtete Zeithorizont, d. h. wie sieht die Situation in fünf oder zehn Jahren aus? Gerade für langlebige Produkte ist das ein wichtiger Punkt. Man muss sich Gedanken über die Sicherheitsaspekte in zehn Jahren machen, wenn wir Produkte, gerade im Videosicherheitsbereich haben, die entsprechend langlebig sind.
P. Rothmann: Wenn ich den Vergleich zum Auto aufgreife, vertrauen wir darauf, dass der Airbag funktioniert und nicht von außen, beispielsweise mit einem Smartphone, ausgelöst werden kann. Um das gleiche Vertrauen in intelligente, vernetzte Devices im Smart

Quelle: Axis Communications

Jochen Sauer: *»Es gibt drei Treiber der Sicherheitstechnik: Vertrauen in Planung, Unternehmen und Produkt, künstliche Intelligenz sowie Rechenleistung.«*

Home aufzubauen, ist es aus meiner Sicht noch ein steiniger Weg, da veraltete Technik und Protokolle noch vielerorts zum Einsatz kommen. Neben Vertrauen brauchen wir außerdem ein Gütesiegel für ganzheitliche Lösungen. Ein Beispiel ist für mich eine vernetzte Türanlage. Da möchte ich natürlich wissen, ob der Kontakt des Schließzylinders da ist und die Tür verschlossen ist, aber ich muss mich auch fragen, ob ich den letzten mechanischen Riegel wirklich motorisieren, also die letzte Bastion vor dem Hacker angreifbar machen möchte.

C. Gause: Wie sieht die Zukunft aus: Was sind die Treiber der Sicherheitstechnik?

J. Sauer: Für mich gibt es drei große Treiber der Sicherheitstechnik in der Zukunft. Einerseits ist es das Vertrauen in die Planung, das Unternehmen und das Produkt. Zweitens ist es die künstliche Intelligenz und drittens eine höhere Rechenleistung. Denn noch mehr Rechenleistung erhöht den Wert des Devices. Außerdem benötigen wir die Leistung »on the edge«. Die Lösungen müssen Kapazitäten bereitstellen, um eine bessere »Feind-/Freunderkennung« durchzuführen. Auch die Unterscheidung zwischen einer Szene, die Standard ist und einer Szene, die analysiert und bewertet werden muss, wird in der Zukunft wichtiger werden.

P. Rothmann: Auch ich sehe die KI als Treiber. Darüber hinaus stehen uns in der Videokameratechnik immer mehr Informationen aus unterschiedlichsten Sensoren, oder auch Wärmebildern, zur Verfügung. Wir können also beispielsweise Umgebungstemperaturen und Tag/Nacht-Analysen durchführen. All diese Informationen aus dem Device und den Sensoren können zukünftig zusammen aggregiert werden. In der IT-Security führt diese Fülle an Informationen dazu, dass auf Alarme schnell reagiert werden kann. Regelwerke lassen erkennen, was ein Standard, was eine Anomalie bzw. was kritisch ist. Wir haben somit bessere Analysewege und Entscheidungen, die uns einen großen Mehrwert bieten.

U. Gleich: Ich könnte provokant sein, und sagen, dass es in fünf Jahren keine Planer mehr geben wird, weil sie durch KI ersetzt wurden, aber ich glaube nicht, dass das passieren wird. Stattdessen wird sich viel konsolidieren, das Zusammenspiel zwischen Herstellern, Anwendern, Betreibern und Generalunternehmern wird zu neuen Netzwerken führen. Wir haben es zukünftig eher mit einem Wertschöpfungsnetzwerk statt einer Kette zu tun.

S. Puppel: Man könnte sich natürlich fragen, ob die Planer und Errichter auf der Strecke bleiben. Ich glaube nicht, denke aber, dass spezielles Know-how von Nöten sein wird, da die technische Entwicklung immer mehr an Fahrt aufnimmt.

P. Rothmann: Absolut. Wir haben es mit smarten Geräten zu tun und wir dürfen eine Videokamera nicht einfach als IP-Gerät betrachten, da sie viel komplexer ist als das. Deshalb kann man diese einem IT-Dienstleister nicht einfach übergeben und auf das Beste hoffen. Das Netzwerk aus Errichtern und der Austausch untereinander bleiben deshalb extrem wichtig – es darf nicht sein, dass es zukünftig einen Markt gibt, in dem nur noch Geräte miteinander sprechen. Es geht darum, Puzzleteile zusammenbringen. Das kann kein Thema für ein Gewerk sein, sondern muss im Netzwerk gelöst werden.

P. Krapp: Ein Trend ist ganz klar. Und zwar, dass jedes Gewerk gerne an die Fenster und Türen eines Gebäudes möchte, um dort Sensoren und Aktoren zu installieren. Die Frage, die sich daraus ergibt, ist die Verortung der Steuerungsintelligenz – wohin wandert diese? Die Steuerungsintelligenz ist nicht trivial und daher als Frage zu begreifen, wie viel Intelligenz in eine übergeordnete Steuerungssphäre gebracht werden kann und was vor Ort verbleiben sollte.

C. Gause: Bedeuten diese Trends also ein »wachse oder stirb« für die Errichter? Wie gehen die Hersteller damit um? Werden wir einen Trend sehen, in dem Hersteller Errichter aufkaufen?

J. Sauer: Das ist eine sehr gute Frage. Wir sehen solche Entwicklungen auf Herstellerseite beispielsweise im Bereich Lebensmittel, aber auch im Security-Bereich gibt es vereinzelt solche Tendenzen. Axis steht aber voll und ganz hinter dem dreistufigen Vertriebsmodell und fokussiert sich auf die eigene Kernkompetenz. Für uns ist das seit langem ein Weg, den wir auch weiter vertrauensvoll gehen werden. Unser seit langem etabliertes und gelebtes Partnerprogramm ist für uns wichtiger als die komplette Wertschöpfung im eigenen Hause zu haben.

U. Gleich: In anderen Ländern gibt es diese Entwicklung zur Konsolidierung eher. In Deutschland mit den vielen Mittelständlern bauen wir aber auf ein Wertschöpfungsnetzwerk.

P. Rothmann: Auch aus meiner Sicht sind die verschiedenen Hersteller in Projekten ein Pluspunkt, der die Flexibilität fördert.

FÜR SCHNELLLESER

Bedrohungen und Schutzziele sollten bereits vor einer detaillierten Planung von allen Beteiligten zusammengetragen werden

Langlebige Produkte wie Videolösungen benötigen vorausschauende Sicherheitskonzepte und regelmäßige Sicherheits-Updates

Künstliche Intelligenz und die Unterscheidung in Standard-Szenarien und abweichende Szenarien wird in Zukunft essenziell

Interview:
Dr. Clemens Gause, Geschäftsführer, VfS – Verband für Sicherheitstechnik e.V., Hamburg