DSD

3 | 2023

DER SICHERHEITSDIENST

Fachmagazin für die Sicherheitswirtschaft

75. Jahrgang

Bild: #1491317259/istockphoto.com

SICHERHEITSTECHNIK

Bild: #1408832606/istockphoto.com

Postvertriebsstück – DPAG – Entgelt bezahlt | DSA GmbH · Postfach 1201 · 61282 Bad Homburg

17. – 20. September 2024

SECURE YOUR BUSINESS

Die Leitmesse für Sicherheit

50 years

security essen

BUCHEN SIE JETZT!

www.security-essen.de

MESSE ESSEN

Weichen für das Sicherheitsgewerbe richtig stellen

Sehr geehrte Leserinnen,
sehr geehrte Leser,

vor bzw. in der parlamentarischen Sommerpause des Deutschen Bundestages wurden durch die Bundesregierung wichtige Weichen für die zukünftige nationale Sicherheitsstrategie, den Schutz Kritischer Infrastrukturen (KRITIS) und unser Sicherheitsgewerbe gestellt.

Mitte Juli 2023 wurde vom Bundesministerium des Innern und für Heimat (BMI) bereits zum KRITIS-Dachgesetz und nach langem Warten auch für das für unsere Branche wichtige Sicherheitsgewerbegesetz (SiGG) die Ressortabstimmung eingeleitet. Ende Juli wurde dann für beide Referentenentwürfe die Verbändebeteiligung begonnen. Da zum Redaktionsschluss dieser Ausgabe die Detailanalysen für unsere Verbandsstellungnahmen zu beiden Referentenentwürfen noch nicht abgeschlossen sind, kann an dieser Stelle nur eine erste Grundsatzbewertung vorgenommen werden.

Wir begrüßen, dass das BMI nach sehr langen Vorarbeiten, die bereits in die letzte Legislaturperiode zurückreichen, nun endlich Klarheit für unsere Branche schafft, wie die zukünftigen Rechtsgrundlagen für unsere wirtschaftliche Betätigung aussehen sollen. Das SiGG soll das Stammgesetz für das Sicherheitsgewerbe in Deutschland bilden. Insofern begrüßen wir, dass wir zukünftig nicht mehr als Bewachungsgewerbe tituliert werden. Dieser antiquierte Begriff entspricht bereits seit Jahrzehnten nicht mehr unserem Leistungsspektrum. Allerdings verwundert es dann, dass der Gesetzgeber zukünftig zwar auch von Sicherheitsmitarbeitern spricht, aber sich bei der Regulierung der Einsatzbereiche der Mitarbeiter – wie bisher – allein auf reine Bewachungstätigkeiten beschränkt. Wir erbringen aber als Sicherheitsgewerbe in Kombination von Mitarbeitern und Technik vielfältige integrierte Sicherheitsdienstleistungen. Grundsätzlich positiv ist, dass man entsprechend der von uns seit Jahren erhobenen Forderung nun erstmals im SiGG auch ein Regularium für die sog. Inhouse-Security schafft.

Allerdings wurden eine Reihe von wichtigen Forderungen des BDSW nicht aufgegriffen. Hierzu zählen u. a. die Vorstellungen des BDSW für nach Einsatzgebieten differenzierte gesetzliche Qualifizierungsvorgaben für Mitarbeiter. Der Gesetzgeber differenziert für nunmehr insgesamt drei Bewachungseinsatzkategorien bezüglich der Qualifizierung – wie bisher – allein zwischen Sachkunde und einer Schulung (vormals Unterrichtung). Beides soll weiterhin federführend durch die IHK-Kammerorganisation durchgeführt werden, was die bekannten „Warteschleifen" nicht verkürzen dürfte. Leider wurde vom BMI auch der Einstieg in eine Harmonisierung von „Zuverlässigkeitsüberprüfungen" nicht gewagt. Sehr kritisch sehen wir die Nichtbehandlung des Schutzes von KRITIS im SiGG. Nach BDSW-Vorstellungen sollten im SiGG verbindliche Basisqualitätsanforderungen für Sicherheitsunternehmen und deren Beschäftigte festgeschrieben werden, die im Bereich KRITIS zum Einsatz kommen.

Aber auch umgekehrt findet sich im Entwurf des KRITIS-Dachgesetzes, das der BDSW im Grundsatz begrüßt, da sich der Gesetzgeber in einem ganzheitlichen Schutzansatz von KRITIS nicht mehr allein auf die IT-Sicherheit fokussieren wird, leider keine Erwähnung des Sicherheitsgewerbes bzw. eine Verknüpfung zum SiGG. Das Sicherheitsgewerbe ist bereits heute faktisch integraler Bestandteil beim Schutz von sämtlichen KRITIS-Sektoren und systemrelevant für die Resilienz von KRITIS. Der nationale Gesetzgeber sollte daher die Systemrelevanz des Sicherheitsgewerbes für den Schutz von KRITIS festschreiben.

Insgesamt bleibt der SiGG-Entwurf an vielen Stellen hinter unseren Erwartungen zurück. Er sollte im Sinne unserer Forderungen im Rahmen der Verbändebeteiligung nachgebessert werden, damit die Weichen für das Sicherheitsgewerbe und die Sicherheit in Deutschland richtig gestellt werden.

Ihr
Gregor Lehnert

Gregor Lehnert

Präsident des Bundesverbandes der Sicherheitswirtschaft (BDSW)

Inhalt

Anmerkung der Redaktion:
Zur leichteren Lesbarkeit wurde auf zusätzliche Bezeichnungen in weiblicher Form verzichtet und nur die männliche Form verwendet. Angesprochen sind natürlich alle Geschlechter.

Der Katastrophe voraus

Von Thomas Pecher-Wagner

Hinterher ist man immer schlauer. Manche sind es aber auch schon vorher. Im Juli 2021 schrillten in der Kreisverwaltung Bernkastel-Wittlich alle Alarmglocken. Man war auf die schlimmsten Überflutungen aller Zeiten eingestellt. Handlungs- und Kommunikationsabläufe waren minutiös geplant. Doch das Gros des Unwetters zog weiter und die Katastrophe trat 100 Kilometer nördlich im Ahrtal ein. Die Region Bernkastel-Wittlich kam mit einem blauen Auge davon – und hat sich für die Zukunft dennoch viel vorgenommen.

„Achtung, Achtung! Hier spricht Ihre Feuerwehr. In der nächsten Stunde ist in Ihrem Bereich mit Überflutung zu rechnen. Bitte räumen Sie die Wohnung!“ Am Mittwoch, dem 14. Juli 2021, fahren acht Einsatzwagen der freiwilligen Feuerwehr durch die Straßen von Wittlich und Bernkastel. Gleichzeitig warnt der Deutsche Wetterdienst vor „extremem Unwetter“ mit Dauer- und Starkregen in weiten Teilen von Nordrhein-Westfalen und Rheinland-Pfalz. In den Straßen von Wittlich ist alles ruhig, zu ruhig. Vor den Häusern türmen sich Sandsäcke, keine Autos parken in den Straßen, die Laternen sind abgeschaltet. Drüben am Mosel-Zufluss Lieser steigt der Pegel, steigt und steigt.

Tag und Nacht im Einsatz

In der Kurfürstenstraße 16 sitzt Brand- und Katastrophenschutzinspekteur Jörg Teusch auf dem Platz des Stabsleiters. Links außen sitzt der Zuständige des Sachgebiets S6 für Information und Kommunikation, daneben reihen sich 14 weitere Sachgebietsfunktionen. Bereits am Montagmorgen hat die Katastrophenschutzdienststelle in ihren Räumlichkeiten die Stabsstrukturen hochgefahren. Auf allen Ebenen wird kommuniziert, Handlungsabläufe werden durchgesprochen. Der Stab ist in ständigem Austausch mit den anderen Landkreisen, mit dem THW und der Feuerwehr, mit dem Schifffahrts- und Umweltamt. Alles wird vorbereitet auf die Flutkatastrophe, die in der Nacht von Dienstag auf Mittwoch eintreten soll: sieben Meter Hochwasser. Ausgelöst von einem Wolkenband, das 80–120 l/m² je Stunde mit sich bringt. So viel Regen, wie sonst in ein bis zwei Monaten fällt.

„Am 14. Juli um 11 Uhr fing es an zu regnen, und am Mittwochnachmittag schwammen bereits die ersten Autos durch die Straßen“, erinnert sich Teusch. Er ist einer von sieben hauptamtlichen Katastrophenschutzinspekteuren des Bundeslandes Rheinland-Pfalz und angestellt in der Kreisverwaltung Bernkastel-Wittlich. „Wir haben früh angefangen mit der Räumung. Zu einem Zeitpunkt, als das Wasser noch nicht da

Thomas Pecher-Wagner

Director Product Management beim Softwarehersteller C4B. Er ist zuständig für die strategische Weiterentwicklung der UCC-Lösung XPhone Connect.

www.c4b.com

war." Er erzählt, wie sie eine zentrale Evakuierungsstelle im Gymnasium in Wittlich einrichteten. Wie sie die Schadensnacht durchgearbeitet haben, um der schlimmsten Unwetterkatastrophe, die Teusch in seiner 35-jährigen Dienstzeit erlebt hat, bestmöglich zu begegnen. „Wir hätten Todesfälle gehabt, wenn wir nicht geräumt hätten. Dabei waren es letztendlich ‚nur' 3,65 Meter Hochwasser." Von den prognostizierten sieben Metern blieb die Region verschont. Denn das Wolkenband zog weiter und ergoss sich mit 200 l/m² je Stunde im Ahrtal.

Schnelle Interimslösung als Testfeld

Nach einer derartigen Katastrophe wird zurückgeblickt: Was hätte anders laufen müssen? Wie stellt man sich für die Zukunft auf? Teusch war vier Wochen lang im Ahrtal im Einsatz, um zu helfen und auch um wichtige Erfahrungen zu sammeln. Danach sortierte sich die Kreisverwaltung Bernkastel-Wittlich komplett neu. Interimsmäßig wurde ein Gebäude angemietet und mit 16 festen Arbeitsplätzen für den Katastrophenfall eingerichtet. Teusch trat mit Jürgen Könen, IT-Administrator der Behörde, in Kontakt. „Wir haben zusammen mit unserem Betreuer NTA unseren Bauchladen an IT-seitigen Möglichkeiten angeschaut, um die Kommunikation für den Ernstfall zu optimieren. Und da kam unsere Telefonie-Software XPhone ins Spiel", erzählt Könen. Als Unified-Communications-Lösung vereint XPhone die Kommunikationsdienste in einer einheitlichen Anwendungsumgebung. Neben der Telefonie werden also auch ERP, CRM und E-Mail in die IT-Infrastruktur eingebunden. Bestmögliche Vernetzung für bestmögliches Handeln – so lautet der Anspruch der Behörde für die Zukunft.

„In der Telefonie nutzen wir XPhone, um wichtige Zeit zu sparen: keine Rufnummern abtippen, Telefonverzeichnisse hinterlegen, relevante Daten zur Verfügung haben." Dank Softphone konnte Könen jedem Stabsmitarbeiter eine eigene Nummer zuordnen, unabhängig von dessen Arbeitsplatz. Außerdem legten Könen und Teusch Wert auf eine intuitive Telefonie-Software, mit der die Kollegen direkt umgehen können ohne vorherige Schulung. Gerade im Katastrophenschutz sei die einfache Bedienung ganz entscheidend. „Wir brauchen ein Tool, das anspruchslos die Leistung erfüllt und in der Katastrophe nicht selbst eine Katastrophe ist. Das haben wir mit XPhone gefunden", so Teusch. Intuitiv sei XPhone auch hinsichtlich der Administration, welche überwiegend von der IT-Abteilung der Behörde vorgenommen werden kann. Nur bei speziellen Themen unterstützt die NTA Saar.

Optimale Kommunikation im Katastrophenschutzzentrum

Mittlerweile ist die Kreisverwaltung in der Planungsphase für ein neues Gebäude. Dort soll eine Unify-Telefonanlage mit XPhone eingerichtet werden. Die Interimslösung dient derweil als Testfeld. „Wir üben alle 14 Tage und setzen Handlungsabläufe unter Last", sagt Teusch. 999 Rufnummern sind für das Katastrophenschutzzentrum reserviert. Die Server werden im Falle eines Stromausfalls über ein Notstromaggregat versorgt. Damit wird die interne Kommunikation sichergestellt. Hinsichtlich der internen Kommunikation ist Teusch ein Fan vom Team-Panel, das XPhone bietet: Dank der Telefoniestatus-Anzeige ist auf einen Blick sichtbar, welcher Kollege besetzt oder frei ist.

Für die Kommunikation von außen wird je nach Bedarf eine zentrale Notfall-Rufnummer installiert. Jürgen Könen bildet diese über das in XPhone integrierte Hotline-Management-Tool „TeamDesk" ab. Die TeamDesk-Gruppe mit den zugehörigen Nummern hat er selbst eingerichtet. „Es ist sehr wertvoll, dass die Hotline ohne größeren Aufwand ad hoc scharf geschaltet werden kann." Auch möchte Könen die Hotline über eine API-Schnittstelle mit dem Ticketsystem verbinden, welches für jeden Anrufer ein Ticket aufmacht. Vorteil: Der Anrufer gibt bereits wichtige Informationen an, um noch schneller ins Gespräch einzusteigen.

In Schadenslagen ist Jörg Teusch viel unterwegs. Über die XPhone-App hat er Zugriff auf sämtliche Rufnummern wichtiger Institutionen. „Bei einem Einsatz muss ich nicht daran denken, das Diensttelefon umzustellen und habe zudem sämtliche Kontakte datenschutzkonform dabei. So kann ich jederzeit agieren."

Und agieren ist das, was für Teusch an oberster Stelle steht. „Wir brauchen für die Zukunft tragfähige Strukturen. Und die Kommunikationswege müssen klar sein." Nur so könne man weitestgehend vermeiden, dass man am Ende in die Zuschauerrolle gedrängt wird, in der man machtlos zusieht, wie einem die eigene Heimat entgleitet; sondern zielgerichtet mit Maßnahmen aufwarten, um einer Katastrophe zuvorzukommen.

Fernwirk-
Sicherheitssysteme
Oldenburg

FSO

www.fso.de

Ihr Security-Provider.
Zukunft sichern.

Alarmprovider VdS 3138

Clearingstelle für Konzessionäre

Störungsannahme für EVU's

FSO Fernwirk-Sicherheitssysteme Oldenburg GmbH
Am Patentbusch 6a I 26125 Oldenburg
Telefon 0441-69066 I Telefax 0441-939001-939
Email info@fso.de I www.fso.de

Einsatz von mobiler Videoüberwachung und Versicherungsschutz

Eine Bestandsaufnahme aus Sicht der Haftpflichtversicherung

Von Bernd Michael Schäfer

Bernd Michael Schäfer

Geschäftsführer der ATLAS Versicherungsmakler für Sicherheits- und Wertdienste GmbH, Köln

www.atlas-vsw.de

Zwei Faktoren beeinflussen die Entwicklung der Sicherheitsdienstleistungen erheblich. Zum einen gibt es immer weniger verfügbare Mitarbeiter. Zum anderen führt die technologische Entwicklung zu immer leistungsstärkeren Kameras und besserer Software für die Auswertung der Bilder. Als Kombination von beidem erscheint der Einsatz von mobilen Videotürmen zur Überwachung von Freiflächen eine perfekte Lösung zu sein. Zunächst ist festzuhalten, dass mobile Videotürme einfach nur ein anderes Instrument sind, mit dem der Sicherheitsdienstleister seine Bewachungstätigkeiten ausübt. Ob er dies mit Personal, stationärer Videotechnik oder eben mit mobilen Videotürmen (Cams) macht, ist in Bezug auf die von ihm geschuldete Dienstleistung und die damit übernommene Haftung unerheblich. So ist auch in dem Bewachungshaftpflichtvertrag nichts Besonderes zu regeln, wenn Cams eingesetzt werden.

Allerdings ist die Schadensituation deutlich anders als sonst. Cams werden vor allem dort eingesetzt, wo es sich um temporäre Risiken mit Bewegung handelt, also auf Baustellen. Diese erfreuen sich immer größerer Beliebtheit bei den Tätern. Gestohlen wird alles, was sich auf den Baustellen befindet, bevorzugt jedoch Kupferkabel, die dutzende Meter lang von der Kabeltrommel abgewickelt, abgeschnitten und abtransportiert werden. Baucontainer werden aufgebrochen, der Inhalt bis zur letzten Hilti entwendet. Die reklamierten Schäden der Auftraggeber sind erheblich.

Die Gründe für die deutlich höhere Schadeneintrittswahrscheinlichkeit sind vielgestaltig.

a) Leichte Umwandlung von Material in Geld

Die Nachfrage nach Kupfer ist hoch, die Schrotthändler aufnahmebereit für Diebesgut, es wird nicht groß danach gefragt, woher die Kabel kommen. Das ist ein starker Anreiz für die Täter.

b) Veränderungen durch den Auftraggeber

Auf Baustellen ist immer alles in Bewegung. Sachen, die heute noch im videoüberwachten Bereich stehen, werden morgen aufgrund von baulogistischen Gründen in einen nicht überwachten Bereich verbracht, ohne dass es eine Abstimmung mit dem Sicherheitsdienstleister gibt.

c) Technische Mängel

Eine häufige Schadenursache ist, dass fehlenden Routinemeldungen zu wenig Aufmerksamkeit gewidmet werden. So werden Cams manchmal mehrere Tage lang ohne Routinemeldung geführt, weil der Mitarbeiter in der NSL dafür eine gute Erklärung hat: Mal „kennt er die Situation, der kommt schon wieder", mal ist „Vodafone in dem Bereich aus Erfahrung schwach", mal ist kein Personal verfügbar, um im Objekt Klarheit zu schaffen. In allen Fällen sind dies Ausreden, die lediglich planvollem Nichtstun eine rationale Begründung liefern sollen.

d) Gestiegene Aggressivität der Täter

Zunehmend sind gezielte Angriffe auf Cams zu verzeichnen, die die Überwachung schlicht stilllegen. So wurden in einem Fall vier von fünf Cams sabotiert.

e) Fehlende Ermittlungserfolge der Polizei

In erschreckend wenigen Fällen werden die Täter gefasst. Es drängt sich der Eindruck auf, dass auf systematisches, evtl. auch überregionales Ermitteln von Täterstrukturen verzichtet wird. Die schnelle Verfügbarkeit von eingestellten Ermittlungsakten spricht hier eine klare Sprache. Die Kriminalität wird verwaltet, nicht bekämpft.

Gibt es zur Frage der Deckung dieser Schäden über die Bewachungshaftpflichtversicherung kein Problem, weil diese praktisch immer gegeben sein wird, so sieht dies bei der Haftung des Sicherheitsdienstleisters vollkommen anders aus. Regelmäßig möchten Auftraggeber nicht verstehen, dass sie eine Dienstleistung einkaufen, dass aber der Dienstleister keinen Erfolg

schuldet. Bedeutet: Wenn die geschuldete Leistung (Überwachung durch Cams) fehlerfrei erbracht wurde, gibt es keine Haftung durch den Dienstleister und der Versicherer wird den Schadenersatzanspruch zurückweisen.

Fatal wird es jedoch bei der Feststellung des Schadenersatzanspruches der Höhe nach. Regelmäßig erhält der Sicherheitsdienstleister eine seitenlange Aufstellung über das entwendete Material und die gestohlenen Werkzeuge. Gehört das Material üblicherweise dem Auftraggeber (Generalunternehmer), so ist dies bei dem Inhalt der Baucontainer und den Hiltis nicht der Fall; diese gehören regelmäßig den Nachunternehmern des Auftraggebers. Und diese haben keinen Anspruch gegen den Sicherheitsdienstleister, weder aus Vertrag noch aus Verschulden. Im Ergebnis gehen diese Ansprüche komplett ins Leere. Und der Auftraggeber hat den Nachweis zu führen, wie viel Kabel er gekauft, gelagert und bereits vor dem Schaden verbaut hat, alles machbar, aber aufwendig. Das Zusenden von Fotos mit leeren Kabeltrommeln und einer behaupteten Meterzahl ist dafür nicht ausreichend; leider werden regelmäßig keine Inventuren nach erfolgtem Diebstahl gemacht, sondern einfach Behauptungen aufgestellt.

Bei Kabeldiebstahl unbeachtlich, aber bei allen anderen Diebstählen ein Thema ist der Zeitwert. Es reicht eben nicht, die Rechnung über eine neue Hilti einzureichen, die nach dem Schaden beschafft wurde. Es muss der Nachweis geführt werden, wie alt die gestohlene Hilti war. Und eine vier Jahr alte Hilti hat eben keinen Wert mehr, da sie komplett abgeschrieben ist.

Zur Verbesserung der für alle Beteiligten schwierigen Situation bieten sich folgende Ansätze an:

- Abläufe und Interventionsmaßnahmen mit erhöhter Priorität festlegen;
- häufigere Kontrolle der Funktionalität der eingesetzten Systeme (Routinemeldung!);
- schnellere Reaktion auf Störungen, nicht abhaken als Normalfall („Das wird schon wieder“);
- strikte Haftungsbegrenzung auf niedrige Summen für Abhandenkommen (z. B. 25.000 Euro);
- vertraglicher Hinweis darauf, dass
  - keine Haftung für Sachen der Nachunternehmer besteht;
  - bei Diebstählen am Tag danach die Fehlmenge durch eine Inventur festgestellt werden muss und
  - dass nur für den Zeitwertschaden geleistet wird;
- Eindecken einer Versicherung für alle Schäden während des Bauvorhabens durch den Generalunternehmer. Hier wären dann die Nachunternehmer mitversichert.

Grundsätzlich sind Cams ein gut geeignetes Instrument zu Sicherung vieler Situationen. Um sie effektiv einzusetzen, müssen jedoch vertraglich wie tatsächlich sinnvolle Maßnahmen zur Schadenprävention ergriffen werden.

Drohnen im Bereich Kritischer Infrastruktur – Inspektion und Gefahrenabwehr

Von Achim Friedl

Achim Friedl

Präsident des europäischen Dachverbandes JEDA – Joint European Drone Associations

Er befasst sich seit Mitte der 90er-Jahre mit unbemannten Luftfahrzeugen. Nach dem Studium war er in Führungsfunktionen und als Hubschrauberberufspilot im Flugdienst der Bundespolizei tätig. Danach wechselte er in das Bundesministerium des Innern und war für die technische Ausstattung der deutschen Bundespolizei und der Bereitschaftspolizeien der Länder verantwortlich.

Seit dem Eintritt in die Pension im Jahr 2016 betätigt er sich in Fachverbänden der Luftfahrt.

Bild: mit freundlicher Genehmigung der Vereinigung Cockpit

Unbemannte Luftfahrzeuge/Drohnen bringen Nutzen für die Bevölkerung. Ebenso besteht ein Gefährdungspotenzial, das von diesen wendigen und in niedriger Höhe operierenden Fluggeräten ausgeht.

Unbemannte Luftfahrzeuge

Unbemannte Luftfahrzeuge – im professionellen Bereich als Unmanned Aircraft Systems (UAS) und umgangssprachlich auch als Drohnen bezeichnet – erfreuen sich im Sport- und Freizeitbereich großer Beliebtheit und haben aufgrund ihrer vielfältigen gewerblichen Einsatzmöglichkeiten große Bedeutung und Nutzen für unsere Gesellschaft. Sie werden als „Aerial Operations" täglich in immer mehr Wirtschaftszweigen eingesetzt, wie Landwirtschaft, Bauwesen, Vermessung, Überwachung, Filmproduktion, Gesundheitsversorgung, medizinische Notfalldienste, Energie, Umwelt, öffentliche Sicherheit sowie innere und äußere Gefahrenabwehr. UAS sind technisch ausgereift und leistungsfähig. Aufgrund mikroelektronischer Unterstützung sind sie leicht zu fliegen, was jedermann ermöglicht, UAS zu steuern und somit am Luftverkehr teilzunehmen.

Nutzen und Missbrauch

UAS/Drohnen haben die sprichwörtlichen zwei Seiten einer Medaille.

Die gute: Hoher Nutzen bei Dienstleistungen für die Bevölkerung, insbesondere auch bei der Überwachung von Industrieanlagen und der Inspektion Kritischer Infrastrukturen.

Die schlechte: Nicht bestimmungsgemäße Verwendung, d. h. missbräuchliche Verwendung, die erhebliche Gefahren hervorrufen und große Schäden verursachen kann.

Flugbetrieb

Der Betrieb von UAS ist in Deutschland umfassend geregelt und in Bereichen beschränkt, in denen Drohnen eine Gefahr für die öffentliche Sicherheit oder Ordnung darstellen. In der „offenen" Kategorie ist der Betrieb innerhalb der Sichtweite des Fernpiloten, unter 120 Metern über Grund und mit ausreichendem Sicherheitsabstand zu Personen zulässig. Können die genannten Eckpunkte nicht eingehalten werden, z. B. beim automatisierten Betrieb außerhalb der Sichtweite, dann findet der Betrieb in der „speziellen" Kategorie statt. Es wird eine behördliche Betriebsgenehmigung gebraucht, die nur erteilt wird, wenn in einem UAS-Betreiberkonzept die sichere Flugdurchführung nachgewiesen wurde.

Industrieanlagen

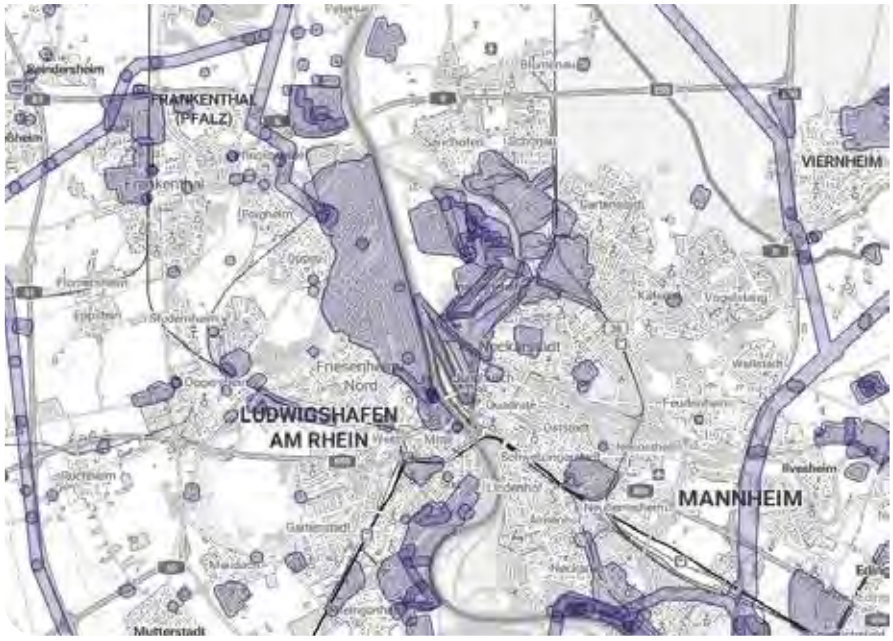
Die Betreiber von Industrieanlagen müssen für die Sicherheit und Funktionsfähigkeit ihrer Anlagen und Einrichtungen sorgen. Für den Objektschutz, die schnelle Reaktion auf Störungen, die Beseitigung von Schäden sowie den Brandschutz und die Brandbekämpfung bedienen sie sich eines Werkschutzes bzw. einer Werkfeuerwehr. Videoüberwachung, Einbruchmeldeanlagen, Brand- und Störmeldeanlagen sind heutzutage Standard. Zusätzlich können UAS eingesetzt werden, um das Industriegelände und technische Anlagen regelmäßig zu überwachen.

Im Alarmfall können UAS schnell vor Ort sein und aussagekräftige Lagebilder (Luftaufnahmen, Gefahrstoffdetektion) liefern. Dazu werden an der Sicherheitszentrale oder strategisch günstigen Positionen auf dem Werksgelände Drohnenhangars errichtet, in denen UAS für den Einsatz bereitgestellt werden. Auf Knopfdruck kann das UAS in „Marsch" gesetzt werden. Die Daten des Zielortes werden automatisch aus einer Alarmanlage übernommen. Schon bevor Personal vor Ort sein kann, bekommt der Einsatzleiter die ersten Lageinformationen von dem UAS. Vorteilhaft ist auch, dass sich Personen zunächst nicht in den Gefahrenbereich begeben müssen.

Inspektion von Freileitungen und Windenergieanlagen (WEA)

Die Anlagen der elektrischen Energieerzeugung und -verteilung liegen als Kritische Infrastruktur

im überragenden öffentlichen Interesse. Die Stromnetzbetreiber sind zur regelmäßigen Inspektion und Wartung gesetzlich verpflichtet, um ein sicheres, zuverlässiges und leistungsfähiges Energieversorgungsnetz zu gewährleisten. Drohnen sind bei der Inspektion von 18.000 Kilometern überregionaler Freileitung, 38.000 Strommasten und fast 30.000 WEA eine wertvolle Hilfe. Sie fliegen automatisiert Stromfreileitungen ab und erkennen dabei Fehlerstellen und Fremdkörper, die sich in den Stromleitungen verfangen haben. Drohnen können an Strommasten und WEA sehr dicht heranfliegen (mit speziellem Training des Fernpiloten) und detailgenaue Inspektionen durchführen, die sogar für die Früherkennung von Schäden geeignet sind.



Geografische Gebiete an Industrieanlagen/-gebieten im Raum Ludwigshafen, in denen Drohnen nur mit Genehmigung des Anlagenbetreibers fliegen dürfen

Gefahren und Gegenmaßnahmen

Bedauerlicherweise sind immer wieder Meldungen wie „Schock in über 1.000 Metern Höhe: Drohne behindert Piloten beim Landeanflug“ oder „Drohne auf Irrwegen: Berliner Fernsehturm wird gesperrt“ zu lesen.

Die Medienberichterstattung darf nicht den Anschein erwecken, die Masse der Drohnenpiloten verhalte sich gefährlich oder rechtswidrig. Es sind nur wenige, die das tun und damit den guten Ruf von unbemannten Luftfahrzeugen opfern. In beiden oben genannten Fällen handelt es sich um Straftaten, die repressiv verfolgt werden müssen. Um derartigem Missbrauch präventiv zu begegnen, sind verschiedene Maßnahmen ergriffen worden:

Generalprävention

Die gravierenden Missbrauchsfolgen für Personen und Sachen am Boden oder bei Kollision mit anderen Luftfahrzeugen müssen aufgezeigt werden, um bei potenziellen Tätern die Einsicht zu erzeugen, sich regelgerecht zu verhalten (erzieherischer Effekt).

Kompetenznachweise

Fernpiloten müssen Kenntnisse und Fähigkeiten zum UAS-Flugbetrieb nachweisen („Drohnenführerschein“). Darüber soll auch das Verantwortungsbewusstsein für die Luftfahrt gestärkt und Missbrauch vorgebeugt werden.

Registrierung

Registriert werden alle UAS-Betreiber, die UAS mit einer Abflugmasse von mehr als 250 Gramm fliegen wollen. Die eindeutige Registriernummer ist an jeder Drohne anzubringen. Für havarierte oder sichergestellte Drohnen können darüber Rückschlüsse auf den verantwortlichen Betreiber bzw. Eigentümer gezogen werden.

Fernidentifizierung

Ein „Feature“, das die Drohnendetektion erleichtert, stellt die ab dem 1. Januar 2024 gesetzlich vorgeschriebene direkte Fernidentifizierung dar. Während des gesamten Fluges werden Daten des UAS (u. a. die Position im Luftraum, die Betreibernummer und die geografische Position des Fernpiloten) so abgestrahlt, dass sie von Mobilfunkgeräten direkt empfangen werden können. Das nimmt dem Piloten die Anonymität und schafft Ansatzpunkte, um ihn ggf. „auf frischer Tat“ anzutreffen.

Flugbeschränkungen und -verbote

Es gibt Bereiche, dort haben Drohnen ohne Genehmigung einfach nichts zu suchen. Das europäische Luftrecht räumt den EU-Mitgliedstaaten ein, den Betrieb von UAS über bestimmten Gebieten aus Gründen der öffentlichen Sicherheit, des Schutzes der Privatsphäre oder der Umwelt einzuschränken oder zu untersagen. Die sog. „geografischen UAS-Gebiete“ haben auch eine Schutzwirkung gegen missbräuchliche Verwendung von Drohnen. In Deutschland gibt es derzeit Beschränkungen für UAS über und in der Nähe von: Wohngrundstücken, Bundesverkehrswegen, Naturschutzgebieten, Industrieanlagen, Anlagen der Energieerzeugung und -verteilung, Justizvollzugsanstalten, militärischen Einrichtungen, Krankenhäusern, Unglücksorten und Katastrophengebieten, Regierungs- und Sicherheitsbehörden, diplomatischen Vertretungen und natürlich in der Nähe von Flugplätzen (Abstand 1 bis 1,5 Kilometer). Geflogen werden darf dort nur mit Genehmigung des Anlagenbetreibers oder der zuständigen Luftfahrtbehörde.

Fazit

Der wirtschaftliche und umweltfreundliche Einsatz von unbemannten Luftfahrzeugen sollte weiter gefördert werden, insbesondere zur Inspektion Kritischer Infrastrukturen. Missbrauch muss mit den genannten Instrumentarien unterbunden werden. Dabei ist die Detektion/Feststellung von gefährlichen Drohnen jedermann erlaubt, während die Abwehr, bis auf Notwehr- und Notstandsituationen, den Behörden vorbehalten bleibt.

UFOs ergänzen klassischen Wachdienst

Kontakt
Kooi Security Deutschland GmbH
Olympiastr. 1, Geb. 5
26419 Schortens
www.247kooi.de

Immer mehr Baustellen müssen vor Diebstahl und Sabotage gesichert werden, doch der Bewachungswirtschaft fehlt das Personal. Der Einsatz mobiler Videoüberwachung hilft, mehr Sicherheit mit weniger Personal zu schaffen.

Solarmodule, Kupferkabel, Baumaschinen, Diesel: Diebstahl, Vandalismus und Sabotage sind auf Baustellen allgegenwärtig. Neben den Kosten für die Wiederbeschaffung fürchten Projektleiter vor allem Verzögerungen, wenn die Baustelle wegen fehlendem Gerät oder langen Lieferzeiten von speziellen Komponenten tage- oder sogar wochenlang stillsteht. Im schlimmsten Fall drohen Konventionalstrafen und steigende Versicherungsprämien. Betroffen sind praktisch alle Baustellen, vom Hochbau über Verkehrswege bis hin zu dringenden Infrastrukturprojekten an Straßen und Schienenwegen, Wind- und Solarparks sowie Strom-, Gas-, Wasser- und Kommunikationsleitungen, die alle zur Kritischen Infrastruktur gehören.

Aufgrund der hohen Kostenrisiken wächst der Sicherheitsbedarf auf Baustellen seit Jahren. Angesichts des wachsenden Personalmangels in der Bewachungswirtschaft – schon heute sind laut BDSW bis zu 10.000 Stellen unbesetzt – können klassische Wachdienste alleine diesen Bedarf nicht decken. Zumal sich die Kosten für eine permanente Sicherheitskraft vor Ort oft nicht abbilden lassen und weniger kostenintensive Revierdienste mit Patrouillengängen keine lückenlose Sicherheit bieten.

„Wie in anderen Bereichen empfiehlt sich auch für die temporäre Baustellensicherung eine Kombination aus klassischem Wachdienst und intelligenter Technik", sagt Mike Jürgens, Geschäftsführer von Kooi Security Deutschland. Kooi, seit Ende 2022 Mitgliedsunternehmen im BDSW, zählt als Pionier in mobiler Videoüberwachung zu den europaweit führenden Anbietern und ist mit einer Mietflotte von mehr als 5.000 Systemen und eigenen zertifizierten Alarmzentralen in über 20 Ländern aktiv. „Die Lösung für optimale Baustellensicherheit ist eine mobile Videoüberwachung in Verbindung mit einer Alarmzentrale, die Vorfälle per Livestream einschätzen und Unbefugte vom Tatort vertreiben kann. So muss der Wachdienst vor Ort nur noch ausrücken, wenn es wirklich erforderlich ist."

Mobile Kamerasysteme

Die Kooi-Systeme unter der Bezeichnung „UFO" (Unit for Observation) sind je nach Ausführung mit hochauflösenden PTZ-Kameras mit 360-Grad-Funktion, Bewegungsmeldern und Infrarottechnik zur Detektion bei Nacht ausgestattet. Für Einsatzbereiche ohne vorhandene Stromversorgung stehen außerdem eigene Power Units für den autarken Betrieb zur Verfügung, wahlweise mit Generator, Solarpaneelen oder hybrid.

Die UFOs werden in sicherheitskritischen Bereichen positioniert. Das sind typischerweise Stellplätze von Containern, Lagerplätze von Baugerät und Material, Starkstromleitungen von Kränen sowie Zufahrten. Durch die richtige Wahl von Standort und System lassen sich unterschiedlichste Areale bis hin zu Großbaustelle oder auch Solarparks mit Videoüberwachungstürmen absichern. Zwei diagonal gegenüber aufgestellte UFOs mit Bewegungsmeldern reichen aus, um eine Fläche von der Größe eines Fußballfeldes zu überwachen.

Ein entscheidender Vorteil der mobilen Technik ist auch, dass die Systeme entsprechend dem Baufortschritt problemlos umpositioniert werden können, beispielsweise wenn Container oder Freiflächenlager verschoben werden, Streckenabschnitte bei Infrastrukturprojekten fertig sind oder neue Baukörper entstehen. Die Umpositionierung kann problemlos mit der Alarmzentrale abgestimmt werden, damit die Kameras auch am neuen Standort in dem festgelegten Sicherungsbereich detektiert.

Hand in Hand mit dem Wachdienst

Entscheidend für die effiziente Überwachung ist nicht allein die Technik, sondern das Zusammenspiel mit der Alarmzentrale. Die UFOs sind auf die Kooi-eigene 24/7-Alarmzentrale in Schortens bei Wilhelmshaven aufgeschaltet. Mithilfe künstlicher Intelligenz werden typische Fehlalarmquellen bereits im Vorfeld herausgefiltert. Dabei profitieren die UFOs davon, dass Kooi über eine eigene Softwareentwicklung verfügt und in den Systemen mehr als zehn Jahre Erfahrung mit Tausenden von Projekten steckt.

Bei einem verifizierten Alarm kann das Leitstellenpersonal über die UFO-Kameras die Situation vor Ort einsehen und per Sprachansage und Sirene intervenieren. Unbefugte und Gelegenheitstäter schreckt das in 98 Prozent der Fälle ab. Erst wenn potenzielle Täter dennoch auf dem Gelände bleiben, setzt der Zentralist eine vorher vereinbarte Meldekette in Gang, beispielsweise das Hinzuziehen des lokalen Wachdienstes. „Je nach Lage und Beschaffenheit des Areals ist ein lokaler Wachdienst unverzichtbar, um vor Ort eingreifen zu können“, erklärt Mike Jürgens. „Das gilt insbesondere dann, wenn in dünn besiedelten Regionen die nächste Polizeistation weiter entfernt ist und die Interventionszeit zu lang wäre. In jedem Falle kann der Wachdienst mithilfe der mobilen Videoüberwachung wesentlich zielführender eingesetzt werden, das heißt wirtschaftlicher und weniger personalintensiv.“

Das gilt auch für die Interventionszeit. „Anders als bei einigen Anbietern üblich ist der Vorfall für unsere Alarmzentrale nicht erledigt, wenn die Meldekette abgearbeitet ist“, so Jürgens. „Unsere Zentralisten bleiben mit den UFOs bis zum Eintreffen der Sicherheitskräfte an der Situation dran. So entsteht während der Interventionszeit vor Ort keine Sicherheitslücke und wir können dem Wachdienst beim Eintreffen oft wertvolle Hinweise auf die aktuelle Lage geben.“

Schnell eingerichtet

Der praktische Ablauf beim Einsatz der mobilen Videoüberwachung ist einfach. „Wir haben eine große Flotte von UFOs und können jederzeit kurzfristig das passende System an den Einsatzort bringen“, so Mike Jürgens. „Aufstellung und Inbetriebnahme dauern in der Regel nicht mehr als eine Stunde. Dabei prüft unsere Alarmzentrale sofort, ob alles einwandfrei funktioniert und die Kameras richtig ausgerichtet sind.“

Gemäß der datenschutzrechtlichen Bestimmungen wird die Baustelle nur während einer

vereinbarten Bewachungszeit außerhalb der Arbeitszeiten überwacht. Öffentlicher Raum im Sichtfeld der Kamera wird durch eine Maskierung von der Überwachung ausgeschlossen, und es erfolgt auch kein permanenter Videostream. Erst im Alarmfall werden die Bilder bis zur Klärung der Situation vorübergehend gespeichert.

Falls erforderlich, lässt sich die Bewachungszeit kurzfristig per App anpassen, beispielsweise wenn außerhalb der üblichen Arbeitszeiten Großgeräte angeliefert oder besondere Arbeiten ausgeführt werden. Über die 247kooi-App können auch Projektinformationen und Vorfallsberichte eingesehen werden, außerdem lassen sich Bildaufnahmen der UFOs auf dem Gelände anzeigen. Die Nutzung der App ist im festen wöchentlichen Mietpreis für die Überwachungslösung enthalten. Das gilt bei Kooi auch für die 24/7-Alarmbearbeitung, und zwar unabhängig von der Anzahl der Alarme.

Individuelle Zusammenarbeit

Der Schulterschluss von klassischem Wachdienst und mobiler Videoüberwachung macht immer mehr Schule. „Wir arbeiten bundesweit wie regional mit einer Reihe von namhaften Sicherheitsdienstleistern zusammen“, berichtet Mike Jürgens. „Wie die Zusammenarbeit aussieht und welche Leistungen sie einschließt, lässt sich individuell gestalten. Wie auch immer das am Ende aussieht: Mithilfe unserer UFOs kann die Bewachungswirtschaft Baustellen und andere Objekte wesentlich effizienter überwachen und ihren Kunden mit geringerem Personalaufwand eine für alle Beteiligten wirtschaftliche 24/7-Lösung anbieten. Das ist angesichts des wachsenden Personalmangels ein besonderer Vorteil.“

SafeNow revolutioniert Sicherheitsbranche

Immer mehr Unternehmen vertrauen auf eine App, um Sicherheitsgefühl zu steigern

Von Tilman Rumland

Tilman Rumland

Gründer und Geschäftsführer der SafeNow GmbH

www.safenow.app

Eine Gruppe Jugendlicher verprügelt einen Jungen im Untergeschoss eines Bahnhofs, während sich die Sicherheitskräfte im Obergeschoss befinden. Eine Frau wird von zwei Männern auf der Damentoilette eines Nachtclubs sexuell belästigt, während die Securitys oben an der Tür stehen. Eine Joggerin wird nachts auf der Ostseite eines Parks verfolgt, während die Nachtwache auf der Westseite patrouilliert. Das ist traurige Realität. Denn obwohl Sicherheitskräfte meist direkt vor Ort sind, bekommen sie oft zu spät oder gar nicht mit, wenn ihre Hilfe benötigt wird. Areale sind zu groß, zu unübersichtlich oder können aufgrund des Schutzes der Privatsphäre, wie zum Beispiel auf Toiletten, nicht überwacht werden. Wie ist es möglich, diese kritische Lücke in unserer bestehenden Sicherheitsstruktur zu schließen?

SafeNow – ein neuer Sicherheitsstandard

Für fast alle Bereiche des Lebens gibt es heutzutage sogenannte „Smart Matching"-Apps. Das Prinzip ist sehr ähnlich: A hat ein Bedürfnis, B ein Angebot und eine Plattform organisiert, beide Seiten zusammenzubringen. Für Mobilität gibt es Uber, für die Liebe Tinder, für Essen Wolt und für das Wohnen AirBnB. Aber was ist, wenn es um die persönliche Sicherheit geht? Bisher war die einzige Option, bei der Polizei anzurufen. Wir bei SafeNow haben uns zum Ziel gesetzt, das zu ändern: Mit unserer App können Hilfesuchende mit einem Klick einen Alarm an das lokale Sicherheitspersonal schicken. Möglich wird dies durch sogenannte „SafeNow-Zonen". In diesem vom Veranstalter oder Betreiber eines Geländes definierten Bereich, können Helfer und Hilfesuchende über die SafeNow-App schnell zusammenfinden.

Das Sicherheitspersonal vor Ort erhält im Ernstfall einen Alarm und bekommt sofort mit, wer Hilfe benötigt. Dank präziser Ortungstechnologie erhalten sie einen metergenauen Standort und wissen so genau, wo sie hinmüssen. So lassen sich sogar Stockwerke und Räume innerhalb von Gebäuden präzise zuordnen. Dies ermöglicht eine beispiellose Geschwindigkeit, um Helfer und Hilfesuchende zusammenzuführen. Zusätzlich können sich SafeNow-Nutzer in der App – unabhängig von SafeNow-Zonen – mit Freunden und Familie in privaten Gruppen vernetzen, um so in Notsituationen besser aufeinander aufpassen zu können. Alle Gruppenmitglieder sind so in der Lage, einen lauten Alarm abzusenden, der sich auch über „Nicht stören" und „Lautlos" hinwegsetzt. Da es sich nicht um eine Standard-Textnachricht oder einen Telefonanruf handelt, ist allen in der Gruppe sofort klar, dass es ernst ist, und sie wissen sofort, wer wo ihre Hilfe benötigt.

Ein Paradigmenwechsel zur selbstbestimmten Sicherheit

Viele Menschen kennen das beklemmende Gefühl, in einer MRT-(Kernspintomografie-)Röhre zu liegen: Es ist eng, laut und angstauslösend. Früher mussten viele MRT-Scans abgebrochen werden, bis die Patienten einen einfachen Notfallknopf in die Hand bekamen. Das Ergebnis? Es wurden drastisch weniger Scans abgebrochen. Es ist bemerkenswert: die gleichen Menschen mit den gleichen Ängsten in der gleichen Situation – was sich geändert hatte, ist, dass die Menschen jetzt ein Gefühl der Kontrolle hatten, in ihrer eigenen Hand. SafeNow hat quasi die digitale Variante dieses Drückers entwickelt und um

das Smart Matching ergänzt: Der Alarmknopf passt sich automatisch an die Umgebung an (und das ohne sich irgendwo einloggen zu müssen!) und alarmiert im Notfall bei Betätigung die zuständigen lokalen Helfer vor Ort.

Wir bei SafeNow glauben an einen selbstbestimmten Sicherheitsansatz, bei dem Menschen befähigt werden, eine aktive Rolle in modernen Sicherheitskonzepten einzunehmen. Innerhalb von SafeNow-Zonen erhöhen die Nutzer der App auch die Sicherheit vor Ort, da jeder für sich und andere schnell und unauffällig Hilfe organisieren kann. Gäste, Reinigungskräfte, Mitarbeiter und alle, die sich in der Zone aufhalten, werden direkt zu Augen und Ohren des Sicherheitspersonals. Sie helfen so, die Sicherheit auf dem Gelände zu erhöhen: Alle Personen werden eingebunden und sind Teil der Lösung. SafeNow setzt so auf einen lokalen und dezentralen Sicherheitsansatz, weg von einem „Big Brother is Watching You" hin zu einem „Big Brother is There for You". Menschen sollten auf diese Weise selbstbestimmt und frei entscheiden können, wann sie Hilfe benötigen – ohne dabei mehr überwacht zu werden.

Branchenübergreifendes Interesse an SafeNow nimmt spürbar zu

Immer mehr Geschäftsbereiche und Industrien schlagen neue Wege ein, ihren Mitarbeitenden ein sicheres Gefühl bei der Arbeit zu ermöglichen. Dieses „WeCare"-Bewusstsein geht hier weit über die Grenzen des Unternehmens hinaus, da sie SafeNow auch privat und in anderen SafeNow-Zonen nutzen können. Die Deutsche Bahn führt SafeNow am Hamburger Hauptbahnhof für Gäste und Mitarbeitende ein, das Schottenhamel-Festzelt nutzt SafeNow während des diesjährigen Oktoberfests, das Düsseldorfer Hotel Breidenbacher Hof für sein Zimmerpersonal. Das Medienunternehmen ProSiebenSat.1 setzt SafeNow sowohl auf dem Campus in Unterföhring ein als auch für Firmenfeiern und Auslandsproduktionen. Das Wannda-Festival verwendet SafeNow auf Outdoor-Veranstaltungen. Es gibt dazu tägliche Anfragen von neuen Anwendungsbereichen wie Flüchtlingsheimen, Freibädern, Universitäten, Schulen etc. SafeNow wird zusätzlich tatkräftig von gemeinnützigen Organisationen wie TERRE DES FEMMES oder dem Verband der Münchner Kulturveranstalter oder Kein Opfer e. V. unterstützt.

94 Prozent der Fahrgäste fühlen sich sicherer: eine Studie, die überzeugt

Die Deutsche Bahn hat in Zusammenarbeit mit der Bundespolizei und SafeNow die Effekte des SafeNow-Sicherheitssystems auf die reale und gefühlte Sicherheit von Fahrgästen, Mitarbeitern und Gewerbetreibenden am Bahnhof Berlin Südkreuz untersucht. Das Projekt wurde von einem unabhängigen Institut wissenschaftlich begleitet und ausgewertet. Innerhalb der SafeNow-Zone wurde allen Menschen eine niederschwellige Möglichkeit geboten, das lokale Sicherheitspersonal rund um die Uhr alarmieren zu können, und zwar auf dem gesamten Bahnhofsgelände inkl. Toiletten und anderen schwer zu schützenden Bereichen.

Die Ergebnisse sind eindeutig: 94 Prozent der befragten Reisenden und Mitarbeiter fühlen sich mit der SafeNow-App sicherer, die Zeit bis zum Eintreffen des Sicherheitspersonals verringerte sich am Bahnhof auf 2 Minuten 36 Sekunden im Durchschnitt. Das Sicherheitspersonal berichtete von einer deutlichen Arbeitserleichterung und einer höheren Wertschätzung durch Fahrgäste. Notsituationen von Beleidigungen über Diebstählen bis hin zu Suizidversuchen konnten nachweislich schneller gelöst und sogar ganz verhindert werden. „Da hätte man damit rechnen müssen, dass da Fahrgäste schwer verletzt, wenn nicht sogar getötet worden wären. Also da war die App der absolute Knaller" (O-Ton Mitarbeiter DB Sicherheit/Bundespolizei). Die Hemmschwelle, in Gefahrensituationen professionelle Hilfe zu rufen, wurde durch die SafeNow-App nachweislich gesenkt. 49 Prozent der Alarme wurden durch Zeugen für andere Hilfsbedürftige ausgelöst. Diese Statistik ist besonders erwähnenswert: In der Gesellschaft wünscht man sich zwar mehr Zivilcourage, dennoch gestaltet sich das beispielsweise bei einer gewalttätigen Auseinandersetzung zwischen Dritten schwierig. Mit SafeNow konnten Menschen direkt helfen, ohne sich selbst in Gefahr zu bringen. Sie wurden so zu „Silent Heroes".

Über 100.000 App-Downloads in unter zwei Monaten

Die SafeNow-App gibt es mittlerweile in mehr als zehn Sprachen und ist im Apple Store (iOS) oder Google Play Store verfügbar. Das Interesse an der App steigt rasant an: So wurde die App mittlerweile mehr als 150.000-mal heruntergeladen. Die Social-Media-Videos von SafeNow bekamen innerhalb weniger Wochen über 7 Mio. Aufrufe, mehr als 700.000 Likes und wurden knapp 200.000-mal gespeichert. Die SafeNow-App war kurzzeitig sogar auf Nummer 1 in der Kategorie Lifestyle im App Store.

Das Geschäftsmodell: SafeNow-Partner finanzieren Sicherheit für alle

SafeNow schaltet keine Werbung und verdient auch kein Geld mit persönlichen Daten. Stattdessen wird SafeNow durch Betreiber öffentlicher SafeNow-Zonen finanziert. Wir sind allen unseren Partnern sehr dankbar, da sie einen direkten Beitrag für eine sicherere Welt machen, der weit über die Grenzen ihres Verantwortungsbereichs hinausgeht. So können z. B. Frauen in einem Frauenhaus im Südosten der Türkei als Gemeinschaft und mit ihren Familien SafeNow nutzen – finanziert von deutschen Unternehmen. Wir sind davon überzeugt, dass jeder Mensch das Recht hat, sich überall sicher und frei zu fühlen. Deshalb ist und bleibt die SafeNow-App für Endnutzer kostenlos, für immer.

Hochsicherheits-Tresorschlösser: Immer gut geschützt!

Von Thomas von Polheim

Thomas von Polheim

Business Development Manager Safe Locks Germany • Austria • BeNeLux bei dormakaba SAL GmbH

www.dormakaba.com

Hochsicherheits-Tresorschlösser sind speziell entwickelte Produktlösungen, die ein besonders hohes Maß an Sicherheit, Robustheit und Widerstandsfähigkeit bieten. Sie verfügen über fortschrittliche, zeitgemäße Sicherheitsmechanismen, die Manipulationsversuche, wie zum Beispiel Picking oder Manipulation der Schließmechanismen verhindern. Diese erfüllen bestimmte Zertifizierungen und Standards, die ihre Sicherheitsmerkmale und -leistungen bestätigen. Beispiele hierfür sind die EN 1300 oder VdS-Klassifizierungen.

dormakaba kann auf eine 160-jährige Geschichte von Sicherheitslösungen zurückblicken und ist stolz darauf, als einer der marktführenden Hersteller auf global etablierte Tresorschlossmarken wie Paxos, Axessor, Mauer, Cencon, Auditcon und La Gard aufzubauen. Die bewährte Qualität und Zuverlässigkeit der dormakaba-Produkte sorgen dafür, dass Ihre Werte in jeder Hinsicht sicher sind.

Für Effizienz im ash-Handling sorgt die Netzwerkintegration, welche die Verwaltung von Tresorschlössern (IP) über eine Softwareschnittstelle ermöglicht. Die Software kann Zugriffsrechte für einzelne Benutzer verwalten, Zeitpläne für den Zugang festlegen und Ereignisprotokolle verfolgen. Diese Systeme bieten eine erhöhte Flexibilität und Kontrolle über die Zugriffsberechtigungen. Durch die Integration einer Netzwerksoftware können Tresorschlösser von einem zentralen Standort aus ferngesteuert, programmiert, zur Öffnung freigegeben oder gesperrt und überwacht werden.

Einmalcode-Tresorschlösser bieten ein erhöhtes Maß an Sicherheit, da die generierten Öffnungscodes nur einmalig und zeitlich begrenzt verwendet werden können. Dadurch wird das Risiko von unbefugtem Zugriff oder Missbrauch reduziert. Dank der Schnittstellenoptionen werden Einmalcode-Tresorschlösser nahezu ausschließlich in bestehende Kundenapplikationen integriert und sorgen durch parallel verfügbare Öffnungsmodi für eine hohe Flexibilität im Rahmen des Code-Managements. Einsatzorte sind Bereiche, in denen temporärer Zugriff auf gesicherte Bereiche oder Gegenstände benötigt wird.

Nachfolgend stellen wir Ihnen eine Auswahl unserer innovativen Tresorschlösser vor:

Cencon: die elektronische Einmalcode-Tresorschloss-Lösung

Das speziell zur Sicherung von Geldausgabeautomaten entwickelte System arbeitet mit einem sich stetig ändernden Einmalcode und kontrolliert, registriert und quittiert jeden Schlosszugriff. Jedem Mitarbeiter kann ein persönlicher Schlüssel (Smart Key) und ein individuelles Profil zugewiesen werden und somit können Insiderdelikte wirkungsvoll verhindert werden. Mit inzwischen weltweit über 1,6 Mio. verkauften Stückzahlen ist Cencon das führende Einmalcode-Tresorschloss.

Mit der Cencon-Software können von einem zentralen Punkt weltweit Tausende von Cencon-Schlössern kontrolliert werden – ohne Kabelverbindung. Durch die Eigenstromversorgung der Schlösser sind weder Batterien noch andere externe Spannungsquellen erforderlich.

Das Cencon-2000-System beinhaltet drei unabhängige Betriebsarten. Dadurch erhalten die verschiedenen Anspruchsgruppen wie das Bankpersonal, Wertlogistikunternehmen (WTU) und Service-Techniker individuellen Zugang zum Wertbehältnis.

Die Axessor-Serie: das elektronische Motorschloss für alle Fälle

Das Axessor CIT ist ein modulares, ausbaufähiges Netzwerkschloss-System (IP) mit bis zu 14 Schlössern, das sowohl im Einzelbetrieb als auch im Verbund mit mehreren Tausend Schloss-Systemen betrieben werden kann: ob Stand-alone, netzwerkfähig, einmalcodefähig! Die gesamte Systemintelligenz befindet sich im gesicherten Bereich.

Die Einmalcode-Funktion des Axessor CIT zeichnet sich durch sein patentiertes interaktives Code-System (ICS) aus: Im ICS-Modus registriert sich der Benutzer mit seiner persönlichen ID am Schloss. Das ICS stellt die Anwesenheit vor Ort sicher und generiert eine temporäre, personen- und situationsspezifische Einmalfrage. Erst nach Weiterleitung dieser Frage via Mobile-App-Applikation etc. an die Einsatzzentrale und Verifizierung der Daten erhält der Benutzer von der Einsatzzentrale einen Einmalcode zum Öffnen des Schlosses. Jedes Ereignis wird aufgezeichnet, um eine maximale Transparenz zu gewährleisten.

Paxos advance IP: das redundante, elektronische Hochsicherheits-Tresorschloss

Paxos ist als redundantes, motorisiertes Tresorschloss die erste Wahl, wenn es um höchste Zuverlässigkeit bei gleichzeitig einfacher und intuitiver Bedienung geht. In Millionen Betriebsstunden haben diese Systeme ihre außergewöhnlich hohe Verfügbarkeit unter Beweis gestellt.

Paxos advance IP ist die zeitgemäße Generation dieser zuverlässigen und bewährten Familie. Es verbindet höchste Zuverlässigkeit mit Bedienerfreundlichkeit und erlaubt die einfache Verbindung von mehreren Schloss- und Eingabeeinheiten zu einem Schließsystem.

Zudem kann das Schließsystem mittels einer Programmiersoftware via einem IP-Netzwerk aus der Ferne überwacht und konfiguriert werden. Auch der Fernzugriff auf Audit-Daten ist möglich.

- Doppelte Sicherheit: Alle Komponenten im gesicherten Bereich sind doppelt ausgeführt.
- Höchste Zuverlässigkeit und Verfügbarkeit: Das Funktionieren ist garantiert, auch bei Fehlerdetektion.
- Gesamte Systemintelligenz befindet sich im gesicherten Bereich.
- EN 1300 B, C, D / VdS Hochsicherheitsschloss Kl. 2, 3, 4

LA GARD 700 – die neue Tresorschloss-Serie für den täglichen Standard

LA GARD ist seit fast einem halben Jahrhundert Branchenführer im Bereich Tresorschlösser. Die LA-GARD-700-Serie verkörpert die bewährten Originalfunktionen und die lange Tradition der LA-GARD-Hochsicherheitsfunktion zusammen mit fortschrittlichen technologischen Merkmalen.

Die Modelle LA GARD Basic, ComboGard Pro und AuditGard wurden weiterentwickelt und sind nun in die neuen LA-GARD-700-Modelle integriert worden. Die 700-Serie verfügt über eine moderne Benutzeroberfläche sowohl im Aussehen als auch in der Technologie mit und ohne OLED-Display.

Ideal für gewerbliche Branchen, Finanzen, Recht, Pharmaindustrie, Einzelhandel, Tresorlager, Behörden (HSL und Strafverfolgung) und Privathaushalte/Privatpersonen. Mit fünf zur Auswahl stehenden Modellen bietet die Serie eine Reihe von Funktionen und Optionen für nahezu jeden Bedarf an Tresorschlössern.

Weitere Informationen über unsere effizienten Lösungen im Bereich der Hochsicherheits-Tresorschlösser finden Sie über den nachfolgenden Link: https://www.dormakaba.com/de-de/produkte-loesungen/produkte/hochsicherheitsschloesser.

Elektronische Schlüsselverwaltung – mehr Sicherheit für alle

Von Patrizia Opitz

Patrizia Opitz
Marketingleiterin der KEMAS GmbH

Kontakt:
KEMAS GmbH
security@kemas.de
www.kemas.de

Wie komplex die Schlüsselverwaltung ist, zeigt sich in einer Konzernzentrale ebenso wie in einem mittelständischen Unternehmen. Wie lässt sich an einem Standort der geregelte Zugang von Mitarbeitenden, Besuchern und Dienstleistern zu Büros, Besprechungsräumen, Lager- und Rechenzentren, sensiblen und weniger sensiblen Gebäudeteilen sicherstellen? Und wie lassen sich weitere Schlüssel – etwa für Fahrzeuge oder andere technische Einrichtungen des Gebäudes – sicher und effizient verwalten?

In vielen Unternehmen werden Schlüssel immer noch persönlich zugewiesen. Die Mitarbeiterinnen und Mitarbeiter behalten sie in der Regel bei sich und nehmen sie am eigenen Schlüsselbund mit nach Hause. Damit ist jeder für seine Schlüssel selbst verantwortlich. Dienstleister oder Fremdfirmen erhalten ihren Zugang meist am Empfang. Die Übergaben werden von den Mitarbeitenden in ein Schlüsselbuch oder eine Excel-Tabelle eingetragen. Auf diese Weise ist eine große Anzahl von Schlüsseln im Umlauf. Es ist fraglich, ob der Überblick behalten werden kann. Problematisch ist es auch, wenn Schlüssel verloren gehen oder nicht zurückgebracht werden. Dann ist es an der Zeit, die Schlösser auszutauschen und über eine elektronische Schlüsselverwaltung nachzudenken.

Kernstück der KEMAS-Lösungen ist die Informations- und Managementplattform KEMAS NET® für Ressourcenverfügbarkeit und Prozesssicherheit. Das Berechtigungsmanagement trägt der Tatsache Rechnung, dass nicht alle Räumlichkeiten eines Unternehmens von allen Mitarbeitenden betreten werden dürfen. Je nach Berufsgruppe oder Aufgabe vergibt der Administrator Zutrittsberechtigungen. Diese können befristet und jederzeit angepasst werden. So kann an allen Standorten eines Unternehmens ein allgemeingültiges Berechtigungskonzept für Schlüssel und Zutrittsmedien umgesetzt werden.

In Schlüsselverwaltungssystemen werden Schlüssel oder Zutrittsmedien je nach Größe und Anzahl eindeutig einem (beleuchteten) Steckplatz, einem Schubfach oder einem Fach zugeordnet. Über einen Leser können sich die Mitarbeiterinnen und Mitarbeiter identifizieren, Schlüssel entnehmen und zurückgeben. Für besonders sensible Bereiche kann auch ein Vier-Augen-Prinzip eingeführt werden. Das bedeutet, dass z. B. bei der Ausgabe eines übergeordneten Schlüssels ein weiterer Mitarbeiter oder Vorgesetzter anwesend sein muss.

Wird ein Schlüssel nicht rechtzeitig zurückgegeben, erhält der Administrator automatisch eine Erinnerungs- oder Alarmmeldung.

Aufgrund der Größe des Geländes oder Gebäudekomplexes ist es oft sinnvoll, mehrere Systeme einzusetzen. Die Terminals werden häufig in den Eingangsbereichen des Geländes und in den Fluren der Gebäude aufgestellt. Durch die Vernetzung untereinander können Schlüssel auch an anderen Stellen abgegeben werden. Bei der Rückgabe wird der mit dem Schlüssel verbundene RFID-Transponder im Depot erkannt, woraufhin das System das Vorhandensein des richtigen Objekts meldet. Über die Systemstatusanzeige der Software erhält der Sicherheitsverantwortliche auf einen Blick eine grafische Übersicht über die Belegungszustände.

Die Vorteile liegen auf der Hand: Durch die lückenlose, revisionssichere Protokollierung von

Modulares System für die Objektaufbewahrung

Schlüssel wird im Schubfach überwacht

Schlüsselverwaltung ohne Fachüberwachung

Berechtigungen, Entnahmen und Rückgaben von Schließmedien wird die Schlüsselverwaltung deutlich sicherer. Die Anzahl der im Umlauf befindlichen Schlüssel wird erfasst und kann schließlich durch entsprechende Auswertungen reduziert werden. Das Verlust- und Missbrauchsrisiko sinkt. Fehler in der Dokumentation werden durch die zentrale Datenhaltung erheblich reduziert und der interne Genehmigungsprozess deutlich vereinfacht. Auch für Dienstleister und Fremdfirmen wird das System komfortabler und schneller. Sie können nun unabhängiger und flexibler agieren und sind nicht mehr auf Öffnungszeiten oder besetzte Pforten angewiesen.

Nicht zuletzt entlastet die elektronische Schlüsselverwaltung die Mitarbeiterinnen und Mitarbeiter. Denn wird der Schlüssel nicht mehr benötigt, landet er einfach wieder im Terminal und der Nächste kann ihn nutzen. So ist die Verfügbarkeit bei Bedarf rund um die Uhr gewährleistet.

Die modularen Systeme von KEMAS dienen aber nicht nur der Schlüsselausgabe und der sicheren Aufbewahrung von Schlüsseln, sondern können für alle prozess- und diebstahlrelevanten Gegenstände eingesetzt werden. Dazu gehören Arbeitsmittel wie Laptops und Mäuse, teure Werkzeuge und Messgeräte oder auch Dokumente. Die verschiedenen Standardmodule lassen sich nach dem Baukastenprinzip beliebig kombinieren.

Beleuchtete Depotstellen nach Inhaltsstatus **Bilder: KEMAS**

„Viele unserer Kunden nutzen zu Beginn nur die elektronische Schlüsselverwaltung und buchen im Laufe der Zeit weitere Funktionen wie z. B. eine Besucherverwaltung oder auch eine Fahrzeugschlüsselverwaltung dazu“, so Patrizia Opitz, Marketingleiterin bei KEMAS. „Die Möglichkeit der kontaktlosen und zeitunabhängigen Bestellung und Übergabe von Schlüsseln und anderen firmeninternen Objekten möchten viele nicht mehr missen.“

Softwarelösungen für Sicherheitsdienste

Kontakt
Bite AG
Im Köller 3
70794 Filderstadt
www.bite.de

In der heutigen digitalen Zeit spielt Software eine entscheidende Rolle in vielen Branchen. Auch Sicherheitsdienstleister profitieren von maßgeschneiderten Softwarelösungen, um ihre Effizienz zu steigern, Arbeitsabläufe zu optimieren und Fehler zu vermeiden. Die Personaleinsatzplanung ist ein entscheidender Faktor für den Erfolg eines Sicherheitsdienstleisters. Die richtige Anzahl qualifizierter Sicherheitskräfte zur richtigen Zeit am richtigen Ort zu haben, ist von entscheidender Bedeutung, um die Sicherheit von Objekten, Veranstaltungen oder öffentlichen Einrichtungen zu gewährleisten.

Seit vielen Jahren ist die Software DISPONIC, ein Produkt der Bite AG, am Markt etabliert. Die Software ist eine spezialisierte Softwarelösung, die Unternehmen bei der effizienten Planung und Verwaltung ihres Personaleinsatzes unterstützt. Die Software bietet verschiedene Funktionen und Module, um den gesamten Prozess der Personalplanung sowie der Berechnung des Bruttolohns und die Fakturierung gegenüber dem Kunden zu optimieren. DISPONIC ist speziell auf die Anforderungen der Personaleinsatzplanung in Sicherheitsunternehmen ausgerichtet.

Die Hauptmodule von DISPONIC umfassen die Dienstplanung, den Bruttolohn und die Faktur. DISPONIC ermöglicht es Unternehmen, den Personaleinsatz auf der Grundlage von Arbeitszeitmodellen, Mitarbeiterverfügbarkeiten, Qualifikationen und anderen relevanten Faktoren zu planen. Die Software berücksichtigt dabei auch gesetzliche Vorgaben, Tarifverträge und individuelle Arbeitsvereinbarungen.

DISPONIC: effiziente Personaleinsatzplanung und mehr

Moderne Sicherheitsunternehmen stehen vor der Herausforderung, ihren Personaleinsatz effizient zu planen und zu verwalten, um einen optimalen Service für ihre Kunden zu gewährleisten. In diesem Zusammenhang hat sich eine Software als unverzichtbares Werkzeug erwiesen. Eine solche Softwarelösung wie etwa DISPONIC bietet zahlreiche Funktionen, die die Personaleinsatzplanung optimieren und das gesamte Sicherheitsteam unterstützen.

DIENSTPLAN – immer und überall einsehbar

Ob Smartphone, Tablet oder Notebook – der Mitarbeiter kann jederzeit seinen Dienstplan einsehen und alle relevanten Daten eines Auftrags abrufen. Dienstzeiten, Aufgaben, Adressen und Besonderheiten – alles immer auf einen Blick.

Verfügbar – Freiwunsch – oder Urlaubsantrag

Diese Module bringen echten Mehrwert. „Verfügbar" zum Beispiel ist cool für Aushilfen. Sie melden selbstständig ihre verfügbaren Arbeitszeiten. Diese Informationen werden direkt in der Planung berücksichtigt. Hinter „Freiwunsch" steckt ein ähnlicher Gedanke: Statt zahlreicher Anfragen in Form von E-Mail oder Whatsapp können Mitarbeiter den Wunsch nach freien Tagen ganz einfach an den Einsatzleiter übermitteln. Dieser hat allerdings das letzte Wort – kann diese Wünsche berücksichtigen oder überplanen.

Kein Papier, kein Ausdrucken oder Ausfüllen von Formularen. Die Mitarbeiter geben ihren Urlaubsantrag sofort über DISPONIC online ab. Genehmigt oder leider abgelehnt – der urlaubsreife Mitarbeiter sieht es direkt im Portal.

Mobile Zeiterfassung

Genial bei großen Events. Wie lässt sich bei Events wie Konzerten oder Fußballspielen die Security zuverlässig und schnell erfassen? Mit einem Dienstausweis mit integriertem NFC-Chip in Kombination mit der DISPONICApp. Alle Informationen werden erfasst und automatisch in DISPONIC übernommen.

Was erleichtert noch die tägliche Arbeit?

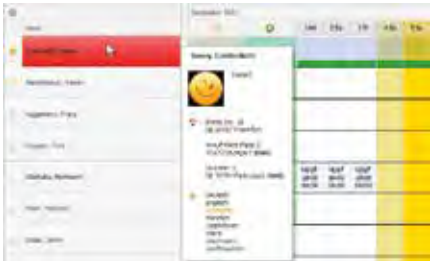
Mit DISPONIC können Schichtpläne erstellt und verwaltet werden. Die Software berücksichtigt dabei die Anforderungen an Arbeitszeiten, Pausenregelungen und Schichtwechsel. Die Planer können mühelos Schichten zuweisen und sicherstellen, dass zu jeder Zeit ausreichend Sicherheitspersonal verfügbar ist. Mitarbeiter haben die Möglichkeit, ihre Schichten einzusehen und gegebenenfalls Änderungen beim Einsatzplaner zu beantragen, was die Flexibilität erhöht und die Zufriedenheit der Mitarbeiter sicherstellt. „Die Einführung von DISPONIC bedeutet in erster Linie Zeitersparnis, also ein besseres Zeitmanagement für meine gesamte Verwaltung. Außerdem sind die unbesetzten Dienste mehr wahrnehmbar und können rasch besetzt werden. So werden Fehler vermieden", sagt Margarete Landertshammer, Geschäftsführende Gesellschafterin der HEL-WACHT HOLDING GMBH, Wien.

Faktur

Die Rechnungstellung hat einen zentralen Stellenwert. Die Kunden der Sicherheitsunternehmen brauchen Transparenz und genaue Stundenabrechnungen mit individuellen Preisen. Die flexible Schnellerfassung mit DISPONIC spart enorm viel Zeit. Rechnungen werden aus der Einsatzplanung generiert. Es gibt flexible Abrechnungsmodelle und selbstverständlich den Rechnungsversand per E-Mail.

Bruttolohn

Das Modul macht die Bruttolohnabrechnung komfortabel und schnell. Grundlegende Informationen wie Grundlohn, Zuschläge und Zulagen werden einmal hinterlegt. Den Rest macht die Software.



Schon bei der Einsatzplanung wird der Bruttolohn sofort automatisch berechnet.

DISPONIC bietet eine zentrale Datenbank zur Verwaltung von Mitarbeiterinformationen. Hier können Mitarbeiterprofile, Qualifikationen, Arbeitszeiten, Urlaubs- und Krankheitszeiten sowie weitere relevante Informationen hinterlegt werden. Diese Daten dienen als Grundlage für die Einsatzplanung. Die zentrale Erfassung und Verwaltung dieser Informationen erleichtern den Planern die Auswahl der geeigneten Sicherheitskräfte für bestimmte Aufgaben und Standorte. DISPONIC bietet Sicherheitsunternehmen eine leistungsstarke Softwarelösung, um interne Prozesse zu optimieren und ihre Leistung gegenüber ihren Kunden effizient und zuverlässig zu gestalten.

Unterschiedliche Reports und Auswertung als Instrument der Unternehmenssteuerung sind Teil der Software. DISPONIC bietet verschiedene Berichts- und Auswertungsfunktionen, um Informationen über Personaleinsatz, Arbeitszeiten, Abwesenheiten und andere relevante Kennzahlen darzustellen. Dadurch können Unternehmen Trends erkennen, Ressourcen besser planen und die Effizienz steigern.

Die integrierte Einsatzplanung, mobile Einsatzsteuerung und Automatisierung von Routineaufgaben sind nur einige der vielen Vorteile, die DISPONIC bietet. Durch die Nutzung dieser Software können Sicherheitsunternehmen ihre Effizienz steigern, die Qualität ihrer Dienstleistungen verbessern und gleichzeitig eine höhere Qualität für ihre Kunden gewährleisten.

DISPONIC ist skalierbar und kann an die spezifischen Anforderungen verschiedener Sicherheitsunternehmen angepasst werden. Egal ob es sich um ein kleineres Unternehmen mit wenigen Mitarbeitern oder ein großes Sicherheitsunternehmen mit vielen Standorten handelt, die Software kann entsprechend skaliert werden, um den individuellen Bedürfnissen gerecht zu werden.

Insgesamt ermöglicht die Sicherheitsdienst-Software wie DISPONIC eine effiziente, transparente und gut organisierte Personaleinsatzplanung. Sicherheitsunternehmen profitieren von optimierten Abläufen, erhöhter Sicherheit, zufriedenen Mitarbeitern und einer gesteigerten Kundenbindung. Die Software ist zu einem unverzichtbaren Instrument geworden, um den wachsenden Anforderungen der Sicherheitsbranche gerecht zu werden und den Schutz von Menschen und Eigentum bestmöglich zu gewährleisten.

Wie Online-Wächterkontrollsysteme die Sicherheitsbranche verändern

Von Jarmo Voegt

Jarmo Voegt

Digital Sales & Marketing Specialist bei SequriX

SequriX ist Anbieter einer Softwareplattform für die Sicherheitsbranche mit über 150 Kunden in Europa.

www.sequrix.com

Die Digitalisierung verändert alle Wirtschaftszweige und macht auch vor der Sicherheitsbranche nicht halt. Unternehmen sollten davor jedoch nicht zurückschrecken, da die Vorteile unverkennbar sind. Im Fokus stehen dabei Online-Wächterkontrollsysteme. Was solche Softwareanwendungen leisten, welche Chancen sie für Sicherheitsunternehmen bieten und wie sie als Teil einer ganzheitlichen Plattformlösung genutzt werden können, zeigt dieser Beitrag.

Automatisierte Gesichtserkennung, intelligente Alarmbewertung oder Drohnenüberwachung: Neue Technologien sind in der Sicherheitsbranche längst Wegbereiter und revolutionieren die Arbeitsweise des Sicherheitsdienstes. Allerdings haben vor allem kleine Sicherheitsunternehmen immer noch massive Defizite, wenn es um das Thema Digitalisierung geht. Ein Problem, schließlich kommt es beim Digitalisierungswettlauf auf Schnelligkeit an, denn Technologien entwickeln sich stetig weiter und die Konkurrenz schläft nicht. Doch Sicherheitsunternehmen stehen nicht nur vor der Herausforderung, abzuwägen, welche Innovationen sich langfristig rentieren und bei welchen sie eher zurückhaltend bleiben sollten. Zusätzlich müssen sie dem gestiegenen Wettbewerbsdruck innerhalb der Branche standhalten und sehen sich mit zunehmenden Qualitätserwartungen und Forderungen nach mehr Transparenz seitens der Kunden konfrontiert. Eine primär manuelle Operative und Verwaltung können dem nicht mehr gerecht werden. Denn manuelle Prozesse und der Einsatz von Papierlisten bedeuten einen hohen Verwaltungsaufwand. Und damit auch eine nicht zu unterschätzende personelle und finanzielle Belastung. Gerade hier machen sich Defizite in der Digitalisierung bemerkbar.

Aber wie können Sicherheitsdienstleister diesen Rückstand aufholen und sich im Wettbewerb behaupten? Der Anfang ist oft einfacher als gedacht und beginnt mit dem Schritt weg von papierbasierten Arbeitsprozessen. Ein Schlüsselwort in diesem Zusammenhang sind Online-Wächterkontrollsysteme (WKS).

Wie kann ein Online-WKS Sicherheitsunternehmen bei geschäftlichen Herausforderungen unterstützen?

Ein modernes Online-Wächterkontrollsystem ist eine Softwarelösung, mit der Sicherheitsdienstleister ihre Prozesse umfassend digitalisieren und automatisieren können. Sie bietet die Chance, alle Kundeninformationen an einem zentralen Ort bündeln und verwalten zu können. Auch Revierfahrten und Rundgänge können im WKS geplant und technologiegestützt ausgeführt werden. Dies spart Zeit und Geld. Dabei bietet eine solche Lösung nicht nur den Sicherheitsfirmen selbst, sondern auch Kunden einen großen Vorteil, denn ein WKS ermöglicht eine optimale Dokumentation, Nachweisführung und Berichterstattung an den Vertragspartner.

Um von den Vorteilen eines WKS zu profitieren, muss dieses mit Daten gefüttert werden: Kunden, Mitarbeiter, Fahrzeuge, Objekte, Aufgaben, Schichten – all diese Aspekte können miteinander verknüpft werden, um Geschäftsabläufe perfekt steuern und dokumentieren zu können.

Die Funktionen eines Online-WKS

Laut der Lünendonk-Studie von 2021 erwarten Kunden von Sicherheitsunternehmen eine hohe Transparenz der erbrachten Leistungen. Im Speziellen geht es hier um die genaue Nachvollziehbarkeit in Form von Protokollen und GPS. Wächterkontrollsysteme erhöhen die geforderte Transparenz durch das Scannen von Kontrollpunkten auf Rundgängen. Mögliche Kontrollpunkte sind dabei:

- NFC-Tags
- GPS-Tags
- Bar- und QR-Codes
- Händische Kontrollpunkte

Mittels Echtzeit-Synchronisation ist es möglich, den aktuellen Bearbeitungsstand von Rundgängen ein-

zusehen und auf Vorfälle zu reagieren. Sollte es zu besonderen Ereignissen oder Auffälligkeiten kommen, kann dies in der App vermerkt werden. Neben einer rein textbasierten Ereigniserfassung bieten vollumfassende Online-WKS-Systeme auch eine Fotofunktion. Möchte der Mitarbeiter beispielsweise ein zerbrochenes Fenster melden, kann dieses einfach auf einem Foto markiert werden, was den Meldeprozess stark vereinfacht und eventuelle Sprachbarrieren umgeht.

Nach Abschluss eines Rundgangs bieten bestimmte Online-WKS-Lösungen eine automatische Berichterstellung und Versand an den Kunden. Auch die Auslieferung von Sammelberichten zu einem vom Kunden gewünschten Zeitpunkt ist möglich. Eine Funktion, welche den Verwaltungsaufwand und die Kosten massiv reduziert. Die Daten müssen während des Rundgangs lediglich mit dem Smartphone erfasst werden und stehen direkt für den Bericht zur Verfügung. Ein Abtippen von Papierlisten ist damit nicht mehr nötig und die Gefahr von Übertragungsfehlern ausgeschlossen.

Vorteile für die Belegschaft

Auch die Mitarbeiter profitieren von einer solchen Anwendung. Mithilfe eines integrierten Dokumentenmanagements haben sie alle benötigten Informationen zur Hand. Dienstanweisungen, Alarmanlageninformationen und -codes des jeweiligen Objekts können in der App verschlüsselt und auch offline eingesehen werden. Welcher Mitarbeiter welche Dokumente und Codes einsehen kann, kann über ein Rechtesystem festgelegt werden. Eine ausgedruckte Einsatzmappe ist nicht mehr notwendig und das Risiko, einzelne Dienstanweisungen zu vergessen oder zu übersehen, auf ein Minimum reduziert.

Auch der Alleinarbeiterschutz ist stets sichergestellt. Hier existieren verschiedenste Möglichkeiten:

- Intelligente Totmann-Funktion
- Panikalarm
- Routinemeldung
- „Zu-Spät“-Meldung

Mit Online-Wächterkontrollsystemen zukunftssicher aufgestellt

Der Schritt weg von manuellen Prozessen im Revierdienst hin zu einem Online-WKS ist eine logische Konsequenz der genannten Vorteile: finanzielle und zeitliche Einsparungen, geringerer Verwaltungsaufwand und erhöhte Benutzerfreundlichkeit. Ohne ein Online-WKS tolerieren Unternehmen eine unzureichende Nachvollziehbarkeit der geleisteten Dienste, ebenso wie Fehleranfälligkeiten bei der Digitalisierung von papierbasierten Listen. Auch die Dokumentation an Kunden ist ohne WKS vergleichsweise zeitaufwendig und teuer. Dokumentenmanagement und Alleinarbeiterschutz sind manuellen Lösungen ebenfalls klar überlegen.

Plattform statt isolierter Lösung

Wächterkontrollsysteme sind allerdings längst nicht mehr nur nützlich für das Scannen von Kontrollpunkten, sondern oftmals in umfassendere Softwareplattformen eingebettet. All-in-one-Lösungen, wie die von SequriX, beinhalten neben dem klassischen WKS für den Revierdienst auch Objektschutz, Alarminterventionen, Berichterstellung und -versand, Auftragsmanagement und Schichtplanung. Statt viele verschiedene Softwarelösungen zu verwenden, bei denen es immer wieder zu Schnittstellenproblemen und Datenverlusten kommt, kann so der gesamte Umfang der geschäftlichen Tätigkeiten aus einem System heraus durchgeführt werden. Und genau darin besteht die große Stärke einer Plattformlösung: Sie unterstützt und entlastet Sicherheitsunternehmen in sämtlichen Bereichen ihrer administrativen und operativen Tätigkeiten. Mit den freigewordenen Kapazitäten kann sich somit voll auf das geschäftliche Wachstum des Unternehmens fokussiert werden.

Die Digitalisierung als Chance begreifen

Wie zu Beginn bereits erwähnt, schreitet die Digitalisierung in der Sicherheitswirtschaft stark voran. Damit die firmeninterne Digitalisierung von Erfolg gekrönt ist, muss zeitgleich auch ein Umdenkprozess stattfinden. Wer Digitalisierung als lästige Pflicht betrachtet, wird früher oder später daran scheitern. Stattdessen muss sie als Chance gesehen werden – eine Chance zur Optimierung von Prozessen sowie zur Erhöhung von Effizienz und Qualität. Unternehmen, die den Wandel frühzeitig erkennen und sich an die veränderten Gegebenheiten und Anforderungen des Marktes anpassen, sind zukunftssicherer aufgestellt und damit der Konkurrenz einen Schritt voraus.

Sie sind neugierig geworden und würden gerne mehr über die konkreten Funktionen und Vorteile von SequriX erfahren? Kontaktieren Sie uns gerne jederzeit für einen persönlichen Austausch.

Weniger Falschalarme in der Videoüberwachung

Die KI-gesteuerte Revolution der Sicherheitsbranche durch promiseQ

Kontakt
promiseQ GmbH,
c/o The Drivery GmbH,
Mariendorfer Damm 1,
12099 Berlin
www.promiseq.com

In einer Zeit zunehmender Sicherheitsbedenken sind Videoüberwachungssysteme zu einem unverzichtbaren Instrument für die Gewährleistung von Schutz in verschiedenen Umgebungen geworden. Die Zunahme von Falschalarmen stellt jedoch eine große Herausforderung für Sicherheitsunternehmen und Überwachungszentralen dar. Diese Falschalarme verschwenden nicht nur wertvolle Ressourcen wie Zeit und Geld, sondern führen bei echten Bedrohungen zu verzögerten Reaktionen bei den Mitarbeitenden und einer gleichgültigen Einstellung.

Das Technologieunternehmen promiseQ aus Berlin hat sich diesem Problem angenommen und bietet mit seinem Vorzeigeprodukt Threat Detect eine bahnbrechende Lösung für die Sicherheitsbranche. Durch die Entwicklung von KI-gestützter, digitaler Filterung ist es dem Start-up gelungen, Falschalarme deutlich zu reduzieren und Sicherheitsunternehmen eine effiziente und kostengünstige Lösung für den Schutz von Öffentlichkeit, Infrastruktur und Privateigentum zu bieten.

Die Geburt von promiseQ

Die Geschichte hinter promiseQ wurzelt in den gemeinsamen Erfahrungen der beiden Gründer Elias Kardel und Tolga Ermis. Nach ihrer gemeinsamen Arbeit bei HELLA Aglaia, einer Volkswagen-Tochtergesellschaft, die sich auf Computer Vision für Autos spezialisiert hat, erkannten Elias und Tolga das Potenzial von künstlicher Intelligenz, wenn sie mit menschlicher Verifikation in Echtzeit gepaart wird.

Elias Kardel (links) und Tolga Ermis

Angetrieben von dem Wunsch, etwas zu bewirken, gründete das Duo promiseQ. Das Technologieunternehmen erlangte schnell Anerkennung für seinen bahnbrechenden Ansatz und wurde auf renommierten Techkonferenzen wie der VivaTech in Paris und der South by Southwest Techkonferenz in Austin, Texas, vorgestellt. promiseQs Engagement für herausragende Leistungen brachte dem Unternehmen auch eine Nominierung für einen Preis bei den renommierten Deep Tech Awards 2022 ein.

Die Epidemie der Falschalarme: Innovation ist notwendig

Die enorme Zahl an Falschalarmen zeigt den dringenden Bedarf an innovativen Lösungen, die echte Bedrohungen von harmlosen Vorfällen unterscheiden können. Herkömmliche Videoüberwachungssysteme verlassen sich oft ausschließlich auf die Überwachung durch Menschen, was zu erheblichen Kosten in Verbindung mit Arbeitskräften und menschlichen Fehlern führt. promiseQ erkannte diese Ineffizienz und machte sich daran, einen zuverlässigen und kostengünstigen Ansatz zu entwickeln.

KI-Filterung: So funktioniert Threat Detect

Das Herzstück von promiseQ ist Threat Detect, ein hybrides KI-System, das die Möglichkeiten der digitalen Filterung nutzt, um Falschalarme zu eliminieren, die Sicherheitsnetzwerke überlasten und Notfallmaßnahmen behindern. Konventionelle Überwachungszentren sind auf menschliches Personal angewiesen, um unzählige Video-Feeds zu analysieren. Im Gegensatz dazu automatisiert

Threat Detect diesen Prozess durch fortschrittliche KI-Algorithmen.

Der digitale Filterprozess umfasst die Analyse von Videodaten von IP-Kameras in Echtzeit und die Erkennung potenzieller Bedrohungen. Außerdem können historische Daten und vordefinierte Bedrohungsmodelle abgeglichen werden.

Das Besondere für die Sicherheitsbranche ist, dass Threat Detect hardwareunabhängig funktioniert, sodass Sicherheitsunternehmen mit Kunden arbeiten können, die jede Art von Kamera oder Überwachungssystem verwenden. Sicherheitsfirmen müssen nicht in verschiedene Videomanagementsysteme investieren. promiseQ reicht aus.

Durch die Reduzierung von Falschalarmen ermöglicht promiseQ den Sicherheitsunternehmen, sich auf echte Bedrohungen zu konzentrieren. Dadurch können die Unternehmen schneller und effektiver auf Notfälle reagieren. Dies erhöht nicht nur die öffentliche Sicherheit, sondern spart auch beträchtliche Ressourcen, die sonst für die Untersuchung von Falschalarmen verschwendet worden wären.

In einer Analogie, die jeden anspricht, macht Tolga Ermis auf die Frustration aufmerksam, die durch Falschalarme verursacht wird und zu einer Desensibilisierung führen kann. „Ungenaue Videoüberwachungs- und Alarmsysteme sind wie der Junge, der in den Fabeln von Äsop‚Wolf' rief. Die Gefahr dieser Desensibilisierung bei echten Bedrohungen besteht darin, dass sie zu verzögerten Reaktionen und verschwendeten Ressourcen führen. Dank der Entwicklung von Threat Detect, dem Falschalarmfilter von promiseQ, können wir nun diese Bedenken beheben und Falschalarme im Zusammenhang mit Videoüberwachung reduzieren."

„Im Moment haben wir Funktionen wie Geofencing, Livebildübertragung und Referenzbildprüfungen", fügt er hinzu. „Aber wir arbeiten an weiteren KI-Funktionen wie der forensischen Suche à la ChatGPT und der Erkennung verdächtiger Aktivitäten. Eine solche Technologie könnte zum Beispiel im Fall der jüngsten Geldautomatensprengungen eingesetzt werden."

Elias Kardel betont auch, dass das Produkt bereits in andere Bereiche vorstößt. „Wir entwickeln uns stetig weiter zu einer umfassenden Videomanagement-Plattform, die sich mit den Themen Integration, Vernetzung, Bandbreite und GDPR auseinandersetzt. Unser nächster Plan sieht die Einführung eines Edge-KI-Servers bei unseren Kunden vor Ort vor, der eine holistische Sicherheitslösung verspricht."

promiseQ hat erkannt, wie wichtig es ist, ein menschliches Element in seinen KI-Diensten zu erhalten und die Privatsphäre des Einzelnen zu schützen.

In außergewöhnlichen Situationen oder komplexen Bedrohungsszenarien können externe Analysten in den KI-Prozess hinzugezogen werden. Diese helfen, die genaue Bestimmung von Bedrohungen zu gewährleisten. KI-gesteuerte Technologien bieten eine hohe Effizienz, dennoch ist es wichtig, dass menschliches Fachwissen in die Entscheidungsprozesse integriert bleibt. Diese Funktion hilft dabei, ein Gleichgewicht zwischen Automatisierung und verantwortungsvoller Entscheidungsfindung sicherzustellen.

Dadurch gibt es Threat Detect in zwei Versionen: Threat Detect Classic, das nur auf der KI beruht, und Threat Detect Premium, das ein menschliches Element enthält.

Einer der wichtigsten Vorteile von Threat Detect ist das Potenzial, die Betriebskosten für Sicherheitsunternehmen zu senken. Das traditionelle Modell, sich auf arbeitsintensive und kostspielige Überwachungszentren zu verlassen, ist in der heutigen, schnelllebigen Welt nicht mehr tragbar. Mit der automatisierten KI-Filterung von promiseQ können Sicherheitsunternehmen die Personalkosten senken und gleichzeitig ein hohes Maß an Überwachung aufrechterhalten.

Der Erfolg eines zertifizierten Pilotprojektes: der Weg bis zur Akzeptanz in der Industrie

Der Erfolg des Start-ups ist in der Branche nicht unbemerkt geblieben. Das Unternehmen hat kürzlich Partnerschaften mit prominenten Akteuren der Branche angekündigt, darunter Sitasys, INSOCAM, Dr. Pfau Fernwirktechnik GmbH, Ajax Systems und Hikvision. Diese Partnerschaften unterstreichen die wachsende Anerkennung der innovativen Technologie und das Potenzial, die Sicherheitsbranche zu verändern.

Mit der steigenden Nachfrage nach Sicherheit und Überwachung steigt auch die Dringlichkeit, das Problem der Falschalarme anzugehen. promiseQs Threat Detect, angetrieben von KI-gesteuerter digitaler Filterung, bietet eine fortschrittliche Lösung, um Falschalarme um bis zu 95 Prozent zu reduzieren.

Mit der Weiterentwicklung des Unternehmens sieht die Zukunft der Sicherheitsbranche vielversprechender, genauer und sicherer aus, da promiseQ die Innovation auf dem Markt vorantreibt.

Einführung der Body-Cam leicht gemacht – neue Netzwerkplattform für Sicherheitsdienste

Kontakt
NetCo Professional Services GmbH
Am Mönchenfelde 13
38889 Blankenburg (Harz)
www.netco.de

Mitarbeiterschutz, Unfallverhütung und Prävention – das sind große Schlagworte in der Sicherheitsbranche. Besonders Sicherheitsunternehmen müssen sich in einer Zeit, in der die Gewaltbereitschaft in der Bevölkerung weiter zunimmt, mit dem Schutz des eigenen Personals befassen. Eine Maßnahme, um Angriffen und Arbeitsunfällen vorbeugen zu können, sind die nachweislich deeskalierend wirkenden Body-Cams. Die Kameras an der Dienstkleidung erfüllen vorwiegend den Zweck, Konfliktsituationen zu beruhigen. Das Hauptziel ist folglich nicht, eine eskalierte Lage aufzuzeichnen, sondern sie zu deeskalieren und es erst gar nicht so weit kommen zu lassen, dass Aggressoren aufgenommen werden müssen.

Stufenmodell zur Deeskalation

Bei Body-Cams mit Display gibt es für diese Vorgehensweise sogar ein spezielles Stufenmodell zur Deeskalation: Zunächst weist das Sicherheitspersonal auf die Möglichkeit, eine Aufnahme starten zu können, hin. Entspannt sich der Konflikt nicht, kann nun das Display eingeschaltet werden, in dem sich der Aggressor spiegelt. Erst im letzten Schritt soll die Body-Cam-Aufnahme gestartet werden, nachdem alle weiteren Maßnahmen zur Beruhigung der Lage nicht gewirkt haben.

Stefan Bisanz, Mitgründer und Geschäftsführender Gesellschafter der Consulting plus Holding GmbH, die sich auf Sicherheitsberatung und -management spezialisiert hat, findet, dass das Display der Body-Cam „die Psyche des Menschen austrickst – auf einmal ist nicht mehr mein Gegenüber der Gegner, sondern ich selbst, weil ich mich sehe, vielleicht auch mit einem Gesichtsausdruck, den ich so von mir ja gar nicht kenne. Die Body-Cam ist wie ein Spiegel. Deshalb glaube ich, dass sich der ein oder andere über sich selbst erschreckt. Und dann begreift der Aggressor, dass das, was er gerade sieht, nun aufgenommen werden könnte. Diese Schockwirkung hilft bei der Prävention einer Straftat."

Straftaten und dadurch entstandene Arbeitsunfälle vorzubeugen, ist auch ein großes Anliegen der gesetzlichen Unfallversicherungen, die eine Vielzahl von Unternehmen aus der Sicherheitswirtschaft zu ihren Kunden zählen. Dabei wird die Body-Cam als Einsatzmittel für die Unfallverhütung immer gefragter. Für viele Sicherheitsunternehmen verbirgt sich hinter der Einführung eines Einsatzmittels wie der Body-Cam ein hoher Aufwand an Zeit und Bindung von Ressourcen, was besonders in kleineren Niederlassungen eine Herausforderung darstellen kann.

Einführung der Body-Cam – das gilt es zu beachten

Nicht jedes Unternehmen kann intern auf einen Datenschutzexperten oder eine Rechtsabteilung zurückgreifen. Somit stellt sich die Informationsbeschaffung und Eruierung einer rechtssicheren Vorgehensweise oft als sehr zeitintensiv heraus. Daher bieten einige (Unfall-)Versicherer ihren Mitgliedsunternehmen Leitfäden mit allen Schritten auf dem Weg zur erfolgreichen Body-Cam-Nutzung an. Doch auch Body-Cam-Entwickler wie die NetCo Professional Services GmbH geben interessierten Unternehmen Hinweise zur Vorgehensweise und unterstützen den kompletten Prozess der Implementierung mit einem fachlich versier-

ten Team. Das Unternehmen stellt einen Leitfaden mit allen Maßnahmen zur DSGVO-konformen Nutzung von Body-Cams auf seiner Unternehmenshomepage bereit. Darin wird Schritt für Schritt erklärt, wann der Body-Cam-Einsatz erlaubt ist, was man bzgl. der Datenspeicherung beachten muss und wie man ein für die Einführung benötigtes Einsatzkonzept erstellt.

Dieses Einsatzkonzept besteht aus mehreren Dokumenten, wie u. a. dem Nachweis des berechtigten Interesses. Die Erforderlichkeitsprüfung, ob ein Body-Cam-Einsatz berechtigt ist, beinhaltet auch die Abwägung von alternativen Maßnahmen. Beispiele hierfür können die personelle Zweitbesetzung oder alternative technische sowie organisatorische Möglichkeiten sein. Unfallversicherungen geben den Tipp, Unfallberichte für den Nachweis des berechtigten Interesses zu sammeln und als Begründung hinzuzufügen.

Weitere Bestandteile des Einsatzkonzeptes stellen ein Verarbeitungsverzeichnis und einen Auftragsverarbeitungsvertrag dar. Falls vorgeschrieben, muss darüber hinaus eine Datenschutzfolgeabschätzung hinzugefügt werden. Auch die Konfiguration der einzusetzenden Body-Cams, eine Erklärung zur Transparenz- und Informationspflicht sowie die technischen und organisatorischen Maßnahmen sollten niedergeschrieben werden. Es ist zudem empfehlenswert, alle Vorhaben mit dem Datenschutzbeauftragten abzustimmen; falls vorhanden, ist auch die Einbindung des Betriebsrates im Sinne der Mitbestimmung wichtig.

Des Weiteren muss der Sicherheitsdienstleister die technischen Anforderungen an die Body-Cams definieren und einen passenden Hersteller wählen. NetCo berät seine Kunden nicht nur zu den technischen Kameraqualifikationen, sondern auch zum Thema Halterung, die an der Dienstkleidung des Sicherheitspersonals befestigt wird. Zudem können Anbieter von Mitarbeiterschulungen zur Verwendung von Body-Cams vermittelt werden. Die Firma LOGO Bochum, Gesellschaft für Schulung und Beratung GbR, bietet beispielsweise speziell auf Bodycams ausgerichtete Deeskalationsschulungen an.

Expertise und Network – die Body-Cam-Konferenz sorgt für wertvollen Austausch innerhalb der Branche

Deeskalation statt Dokumentation – unter diesem Motto kamen Referenten und Beschäftigte aus der Sicherheitswirtschaft, darunter Sicherheitsdienste, aber auch Verkehrsgesellschaften, Ordnungsämter, Polizeien und Vertreter aus dem Einzelhandel, auf der diesjährigen Body-Cam-Konferenz Mitte Juni in Köln zusammen. Schwerpunktthemen der Veranstaltung waren neben der DSGVO-konformen Body-Cam-Nutzung auch die Implementierung sowie Einsatzmöglichkeiten der Kameras in den Sicherheitsunternehmen. Dieses Jahr ließ sich sogar eine verstärkte Teilnahme von privaten Sicherheitsdiensten vernehmen, die an der Einführung von Body-Cams interessiert waren oder von ersten Nutzungserfahrungen berichten konnten. Die Unternehmen profitierten nicht nur von dem vielseitigen Programm und den Expertenvorträgen, die das Thema „Body-Cam“ aus unterschiedlichen Perspektiven beleuchteten, sondern vor allem auch vom Austausch untereinander. Viele Unternehmen konnten ihr Netzwerk erweitern und nutzten diese Kommunikationsplattform, um Erfahrungen bei der Body-Cam-Anwendung zu teilen.

Neue Struktur für die Body-Cam-Konferenz 2024

Bei der diesjährigen Konferenz waren die Nachfragen und Themenwünsche aus der Sicherheitsbranche so groß, dass die Veranstaltung im nächsten Jahr eine neue Strukturierung mit verschiedenen Gruppen bekommen soll. Für die Sicherheitswirtschaft ist sogar eine eigene Kommunikationsplattform geplant, um das Netzwerk fördern und auf Fragestellungen besser eingehen zu können. Weitere Informationen zur dritten Body-Cam-Konferenz können auf der Website von NetCo ab Anfang 2024 eingesehen werden.

Mobile Videoüberwachung von LivEye macht Werks- und Firmengelände sicher

Kontakt
LivEye GmbH
Europa Allee 56b
54343 Föhren
www.liveye.com

Diebstähle haben im vergangenen Jahr in Deutschland deutlich zugenommen. Waren es 2021 noch rund 1,5 Millionen polizeilich erfasste Fälle, stieg die Zahl in 2022 laut Kriminalitätsstatistik auf rund 1,8 Millionen. Das ist eine Steigerung um 20 Prozent (Quelle: Bericht der Innenministerkonferenz). Unter diesen Voraussetzungen wird eine professionelle Videoüberwachung immer wichtiger.

Die Zahlen zeigen eine bedenkliche Entwicklung und stellen eine Herausforderung für die Strafverfolgungsbehörden und die Gesellschaft dar, da sie sowohl wirtschaftliche Schäden als auch Sicherheitsbedenken mit sich bringen. Doch Sicherheit bedeutet für Unternehmen nicht nur die Abwehr von Diebstahl und Vandalismus, sondern auch den Schutz der Reputation. Entscheider haben es deshalb mit einer komplexen und angespannten Sicherheitslage zu tun, bei der sie proaktiv reagieren müssen, um den vielfältigen Herausforderungen angemessen begegnen zu können. So erfordern die unterschiedlichen Bedrohungen wie Diebstähle, Vandalismus, Aktivisten und terroristische Aktivitäten spezifische Sicherheitsmaßnahmen und -strategien. Hier ist das frühzeitige Erkennen von Anzeichen einer Gefährdung oder von ungewöhnlichem Verhalten entscheidend, um rechtzeitig geeignete Maßnahmen einleiten zu können. Angesichts der komplexen Bedrohungen sollten Unternehmen in moderne Sicherheitstechnologien investieren, die eine effektive Überwachung, Alarmierung, Intervention und Dokumentation gewährleisten.

Einbrecher auf Baustellen-Klo gestellt

Betriebsgelände befinden sich häufig in abgelegenen Industriegebieten, was für Einbrecher einen Vorteil darstellt. Umso wichtiger ist es, diese entsprechend zu schützen. Mobile Videoüberwachungssysteme bieten hier bei Bedarf rund um die Uhr Schutz und sind eine kosteneffiziente Alternative bzw. Ergänzung zum konventionellen Wachschutz.

So konnte jüngst eine Straftat auf einem großen und unübersichtlichen Betriebsgelände in der nordrhein-westfälischen Kreisstadt Unna durch LivEye verhindert werden. Zwei verdächtige Personen wurden nachts mittels Kameraüberwachung als Eindringlinge identifiziert. Das 24 Stunden besetzte LivEye Video Monitoring & Alarm Center beobachtete, wie Täter über den Zaun des Unternehmensgeländes kletterten. Der diensthabende Operator informierte die Polizei. Die konnte die Eindringlinge wenig später auf dem Gelände stellen – insbesondere weil der gut geschulte Operator dank der eingesetzten Technik genau mitteilen konnte, dass sich eine der Personen auf einem Baustellen-Klo versteckt hielt.

Individuelle Überwachung in Echtzeit

Durch ein persönliches Sicherheitsaudit vor Ort, wird ein individuelles Sicherheitskonzept erarbeitet, sodass die eingesetzte Videoüberwachungslösung das gesamte Unternehmensgelände abdeckt. Auch sogenannte „tote Winkel" werden erfasst und bieten so eine lückenlose Sicherheitsabdeckung. Durch die Übertragung in Echtzeit und die eigens entwickelte KI, ermöglicht die Videoüberwachung das sofortige Erkennen von Sicherheitsvorfällen oder verdächtigem Verhalten. Das Sicherheitspersonal kann unmittelbar reagieren, potenzielle Bedrohungen identifizieren und entsprechende Maßnahmen ergreifen. Da sich die Anforderungen der Überwachung je nach Gelände stark unterscheiden können, lässt sich die Sicherheitsdienstleistung von LivEye individuell anpassen. Das ermöglicht es, auch bei

veränderten Sicherheitsanforderungen, flexibel zu reagieren.

Baustellenüberwachung – eine besondere Herausforderung

Baustellen sind dynamische Umgebungen mit verschiedenen Sicherheitsrisiken, die eine sorgfältige Planung und Implementierung von Überwachungssystemen erfordern. LivEye bietet dazu mobile Videoüberwachungssysteme, die individuell auf die Baustellenbegebenheiten angepasst werden. Unvorhersehbare Umgebung, Stromversorgung, Witterungsbedingungen, weitläufige Flächen – zu all dem wird ein umfassendes Sicherheitskonzept erarbeitet, das auch alle Bauphasen abdeckt. Die Lösungen ermöglichen eine sichere Überwachung zu jeder Tages- und Nachtzeit. Eine orangefarbene Beleuchtung wirkt in der Nacht abschreckend sowie präventiv und Bewegungen werden von der intelligenten Analysesoftware zuverlässig erfasst. Diese kann zwischen Menschen, Tieren, Fahrzeugen und wiederkehrenden Bewegungen unterscheiden und verringert somit die Fehlerquote auf ein Minimum. Im Verdachtsfall wird umgehend das durchgehend in Deutschland besetzte Video Monitoring & Alarm Center alarmiert. Der diensthabende Operator reagiert sofort und leitet entsprechende Maßnahmen ein. Über das integrierte Lautsprechersystem sprechen sie die identifizierten Personen individuell an und fordern sie dazu auf, das Gelände zu verlassen. Wird dieser Forderung nicht nachgekommen, wird die Polizei oder der hinterlegte Wachdienst informiert. Sollte es zu einer Unterbrechung der Stromversorgung kommen, werden die LivEye-Überwachungssysteme mit Energie aus einem bis zu 80-stündigen Akkuspeicher versorgt. So ist eine kontinuierliche Videoüberwachung gewährleistet. Im Falle einer Straftat hilft das gesicherte Videomaterial dabei, die Täter zu identifizieren und zu überführen. Systeme der LivEye können auch unter widrigsten Bedingungen eingesetzt und autark, ohne Stromanschluss, betrieben werden.

Kompetenz durch Erfahrung

LivEye ist ein führender Anbieter für die Bewachung von temporären Risikozonen mit mobilen Videoüberwachungsanlagen. Mit aktuell rund 1.500 Videotürmen, einem eigenen 24/7-Alarmcenter sowie über 60 Mitarbeitern ist LivEye einer der größten Anbieter in Deutschland. Mit dem Slogan „SECURE by NIGHT & SMART by DAY" steht LivEye für KI-gestützte Sicherheitssysteme, die außerhalb der Scharfzeiten Mehrwerte liefern. So schützt LivEye vor Gefahren wie Eindringlingen mittels Videoanalyse und Intervention über die hausinterne Leitstelle.

Zum anderen steht dem Kunden ein Webportal zur Bilddokumentation zur Verfügung, welches ihn mit Stand- und 360-Grad-Bildern aus der Ferne Objekte mit Leichtigkeit managen lässt. Mit den datenschutzkonformen LivEye-Systemen sind Objektverantwortliche immer informiert und können in Echtzeit Projekte steuern und neue Risiken erkennen. Die LivEye-Lösungen sind vielseitig einsetzbar und finden Anwendung in Bereichen wie Energieversorgung, Telekommunikation, Industrieanlagen und der Bauwirtschaft.

Die LivEye GmbH ist ein führendes Unternehmen im Bereich der mobilen Videoüberwachung für temporäre Risikozonen, wie kurzfristig errichteter Infrastruktur oder Baustellen.

Weitere Informationen finden Sie unter: **www.liveye.com**.

Anzeigen

Who is Who der Sicherheitswirtschaft

– nach Postleitzahlen geordnet –

Dussmann
FACILITY MANAGEMENT

Dussmann Service Deutschland GmbH

Friedrichstraße 90 • 10117 Berlin

www.dussmann.de

teamflex

Teamflex Solutions GmbH

Thüringer Allee 12/Haus 4 • 14052 Berlin

www.teamflex-solutions.de

GATE AVIATION

GATE Aviation GmbH

Heidenkampsweg 74–76 • 20097 Hamburg

www.gate-aviation.de

Hamburger Wachunternehmen & Personalservice GmbH

Damm 33 • 25421 Pinneberg

www.hwp-sicherheit.de

Anzeigen

W.I.S. Sicherheit + Service GmbH & Co. KG

Industriestr. 171 • 50999 Köln

www.wis-sicherheit.de

Pond Security Service GmbH

Rückinger Str. 12 • 63526 Erlensee

www.pond-security.com

INDUSTRIE-BEWACHUNG
Bruno Wachtmeister GmbH & Co. KG

Bellingweg 14 • 70372 Stuttgart

www.industrie-bewachung.de

Securiton Deutschland
Alarm- und Sicherheitssysteme

Von-Drais-Str. 33 • 77855 Achern

www.securiton.de

ZIEMANN SICHERHEIT GmbH

Gewerbestr. 19–23 • 79227 Schallstadt

www.ziemann-gruppe.de

Dussmann

FACILITY MANAGEMENT

Ein Sicherheitskonzept, das sitzt wie ein Maßanzug

Für eine einwandfreie Umsetzung von Sicherheitskonzepten ist ein harmonisches Zusammenspiel von Qualität, Sicherheitspersonal, Dokumentation, Organisation und Technik unerlässlich. Nur so kann größtmögliche Sicherheit garantiert werden. Ein Full-Service-Anbieter, der im Bereich der Sicherheitstechnik umfassend aufgestellt ist, ist Dussmann. Von Beratung über Analyse bis hin zum Bau und Wartung sicherheitstechnischer Anlagen bietet Dussmann alle Leistungen aus einer Hand. Das Technikportfolio reicht dabei von elektronischen Zutrittslösungen sowie mobilen Videotürmen über Sicherheitsroboter bis hin zu Gefahrenmeldesystemen. Die Aufschaltung der Gefahrenmeldeanlagen erfolgt über eine nach DIN EN 50518 zertifizierte Alarmempfangsstelle. Der Alarmdienst wird mit einer eigenen, nach VdS 3138 zertifizieren Notruf- und Serviceleitstelle abgesichert.

Gefahrenmeldeanlagen errichtet Dussmann u. a. in

- Außenanlagen
- öffentlichen Einrichtungen und Sportzentren
- Industrie- und Gewerbeobjekten
- Forschungs- und Kultureinrichtungen
- Baustellen
- militärischen Anlagen

Der Einsatz modernster Sicherheitstechnik verlangt zudem qualifiziertes Personal. So bildet Dussmann seine Sicherheitsfachkräfte stets weiter. Eine eigene Abteilung für integrierbare Sicherheitssysteme ist verantwortlich dafür, dass die Sicherheitstechnik zuverlässig arbeitet und konstant auf aktuellem Stand bleibt.

Kontakt:
Dussmann Service Deutschland GmbH
Friedrichstraße 90 · 10117 Berlin
Tel.: +49 30 2025-2719
Mail: vertrieb@dussmann.de
Web: www.dussmann.de/

teamflex

Teamflex Solutions GmbH Sicherheit und Service

Die **Teamflex** Solutions GmbH ist ein spezialisiertes Fachunternehmen für komplexe Sicherheitsdienstleistungen. Unser Leistungsportfolio bedient die Schwerpunkte Großveranstaltungen, Messen und Kongresse, Gala Events, Konzerte, Sport- und Open-Air-Veranstaltungen sowie Objektschutz in Asyl- und Flüchtlingseinrichtungen. Die enge sowie partnerschaftliche Zusammenarbeit mit unseren Kunden ist für uns der Schlüssel zu einer bedarfsgerechten, qualitativ hochwertigen und effizienten Leistungserbringung.

Neue Projekte bedürfen neuer Strategien und Ausrichtungen. Hierbei ist es unser Anspruch, durch den Einsatz von qualifiziertem Personal eine 100 %ige Zufriedenheit bei unseren Auftraggebern zu erzielen. Teamwork hat bei uns oberste Priorität und wird durch ein professionelles Personalmanagement gefördert. Die Absicherung verschiedenster Großevents setzen einen bis ins Detail konzeptionierten Maßnahmenkatalog voraus. Dieser wird in Abstimmung mit den jeweiligen Kunden individuell und auf deren Bedürfnisse angepasst. Die professionelle Umsetzung erfolgt in den Bereichen der Sicherheits- und Servicedienstleistungen. Der Einsatz von unseren kunden- und serviceorientierten Mitarbeitern stellt für uns hierbei einen wichtigen Erfolgsfaktor dar.

Gezielte Trainings-/Weiterbildungsmaßnahmen sind für die Teamflex selbstverständlich und unterstreichen sowohl die Wertschätzung für unsere Mitarbeiterinnen und Mitarbeiter als auch unseren eigenen Qualitätsanspruch.

Teamflex – innovativ / kompetent / flexibel

Kontakt:
Marc Böttger, Geschäftsführer
Teamflex Solutions GmbH
Thüringer Allee 12 · 14052 Berlin
Tel.: +49 30 86 800 11 00
Mail: info@teamflex-solutions.de
Web: www.teamflex-solutions.de

Anzeigen

GATE AVIATION

GATE Aviation – Ihr zuverlässiger Partner für Luftsicherheit

Bild: # 1069567532/istockphoto.com

GATE Aviation mit Sitz in Hamburg ist deutschlandweit marktführend im Bereich „Qualifizierungsmaßnahmen für Luftsicherheit". Als operative Schnittstelle zwischen den Anforderungen der Luftsicherheit und dem Arbeitsmarkt an Flughäfen stehen wir seit mehr als zehn Jahren für die qualitativ hochwertige Schulung von Luftsicherheitsassistenten und Luftsicherheitskontrollkräften gemäß §§ 5 und 8. Hauptakteure für Rekrutierung und Ausbildung dieser Flughafenfachkräfte schätzen dabei insbesondere unsere Flexibilität, Zuverlässigkeit, Nachhaltigkeit und Kompetenz.

Durch unser zielgerichtetes und mittlerweile digitalisiertes Eignungsfeststellungsverfahren werden geeignete Kandidaten schnell und zuverlässig identifiziert. Die anschließende Schulung ist methodisch und didaktisch auf die Anforderungen der zukünftigen Arbeitsplätze am Flughafen und die individuellen Bedarfe des zukünftigen Arbeitgebers abgestimmt. Unsere Lehrkräfte verfügen neben pädagogischer Qualifikation über langjährige Erfahrung im Bereich Luftsicherheit. Darüber hinaus beraten wir Unternehmen bei weitgehenden Flughafendienstleistungen, u. a. im Hinblick auf nachhaltige Optimierung und Qualitätssicherung.

Mit uns auf gutem Kurs.
Wir freuen uns auf Ihre Kontaktaufnahme:

Kontakt:
GATE Aviation GmbH
Heidenkampsweg 74–76 · 20097 Hamburg
Tel.: +49 40 298 484 88-0
Mail: info@gate-aviation.de
Web: www.gate-aviation.de

HWP Sicherheit – nicht mehr und nicht weniger!

Ein Hamburger Dienstleister mit optimalem Preis-Qualitäts-Verhältnis bietet Ihnen ohne Umwege sein Dienstleistungsportfolio an: Wir liefern schnell und zuverlässig just-in-time benötigte Dienstleistungen in Berlin, Bremen, Hamburg, Niedersachsen, Mecklenburg-Vorpommern und Schleswig-Holstein: Sicherheitsdienste mit speziellem Fokus auf Veranstaltungen jeglicher Art!

Qualitäten, mit denen wir seit Jahren unsere Kunden überzeugen:

- Hohe Flexibilität, auch bei kurzfristigen Anfragen
- Zuverlässige Betreuung: vom Angebot über die Personalbereitstellung bis zur Ausführung – preisgünstige Dienstleistungen bei hoher Qualität
- Ein junges Team, das Sie rundum kompetent betreut

Wir haben uns als H.W.P GmbH in den vergangenen Jahren in der Sicherheitsbranche einen Namen gemacht und sind seit 2021 sehr stolz, gem. ISO:9001 zertifiziert zu sein. Dies entspricht unserem Leistungsanspruch – sowohl an unsere betreuten Projekte als auch an uns selbst. Sämtliche Dienstleistungen werden zudem den hohen Ansprüchen der DIN 77200 gerecht, was als starkes Signal an die Ansprüche sowie an das QM zu verstehen ist, um Ihnen als Kunden gegenüber die Qualität unserer Dienstleistungen sicherzustellen.

Mit der H.W.P GmbH wählen Sie einen starken und zuverlässigen Partner! Mit unserer eigenen Akademie schulen wir zudem unsere Mitarbeiter auf die speziellen Anforderungen der Veranstaltungsbranche, um hier für unsere Kundenprojekte bestens gewappnet zu sein!

Senden Sie uns gern Ihre Anfrage!

Kontakt:
Hamburger Wachunternehmen & Personalservice GmbH
Damm 33 · 25421 Pinneberg
Tel.: +49 4101 820 5170
Mail: kaymaz@hwp-sicherheit.de
Web: www.hwp-sicherheit.de

Anzeigen

Mobile Baustellen-überwachung von Kooi

Kooi Security ist ein Pionier in der temporären, mobilen Videoüberwachung und als einer der europaweit führenden Anbieter mit einer Mietflotte von mehr als 5.000 Systemen und eigenen zertifizierten Alarmzentralen in über 20 Ländern aktiv. Das Unternehmen ist in Deutschland und Österreich mit eigenen Ländergesellschaften, einer deutschen Alarmzentrale sowie mehreren regionalen Standorten vertreten.

Die temporäre Videoüberwachung mit Kooi UFOs (Units for Observation) ist eine wirksame und wirtschaftliche Lösung, um insbesondere Baustellen vor den hohen Folgeschäden von Diebstahl, Vandalismus und Sabotage zu schützen. In Verbindung mit künstlicher Intelligenz zur Minimierung von Fehlalarmen und der Aufschaltung auf die 24/7 Kooi-Alarmzentrale werden Vorfälle zuverlässig detektiert, Täter durch Ansprache und Sirene abgeschreckt und bei Bedarf entlang einer abgestimmten Meldekette agiert. Die zielführende Überwachung vermeidet unnötiges Ausrücken und entlastet lokale Wachdienste. Typische Einsatzbereiche sind Hoch- und Tiefbaustellen, Wind- und Solarparks, Kritische Infrastrukturen wie Strom-, Gas-, Wasser- und Kommunikationsleitungen, aber auch Lagerflächen, Leerstände und andere Objekte.

Kontakt:
Kooi Security Deutschland GmbH
Olympiastraße 1 · Geb. 5 · 26419 Schortens
Tel.: +49 4421 5001 66
Mail: sales.de@247kooi.de
Web: www.247kooi.de

Ihr flexibler Partner für Sicherheit

Die Schmalstieg GmbH Sicherheitsdienste ist ein renommiertes Traditionsunternehmen in Hannover und der Region. Mit einer langen Geschichte und einer etablierten Reputation bietet das Unternehmen ein breites Spektrum an Sicherheitslösungen.

Die Kernkompetenz des Unternehmens liegt im Bereich von Flüchtlings- und Asyleinrichtungen sowie im Objektschutz und Empfangsdienste. Mit langjähriger Erfahrung und eigens entwickelten Schulungen bereitet die Schmalstieg GmbH ihr Personal optimal auf die spezifischen Anforderungen vor. Sie bietet zahlreiche Fort- und Weiterbildungsmöglichkeiten für ihre Mitarbeitenden an und legt Wert auf ein familiäres Umfeld.

Ein weiterer Schwerpunkt der Schmalstieg GmbH Sicherheitsdienste liegt auf dem Revier- und Interventionsdienst. Sie haben sich auf besonders sicherheitsbedürftige Objekte und kritische Infrastruktur spezialisiert. Mit ihrer Fachkompetenz und ihrem geschulten Personal gewährleisten sie einen effektiven Schutz und intervenieren bei Vorfällen schnell und professionell.

Die Sicherheitsdienste zeichnen sich durch maßgeschneiderte Sicherheitskonzepte aus, die in enger Zusammenarbeit mit dem Kunden entwickelt werden. Gemeinsam werden mögliche Schwachstellen und Risiken identifiziert und passende Sicherheitsmaßnahmen und -technologien ausgewählt und implementiert.

Die Schmalstieg GmbH Sicherheitsdienste sind zertifiziert nach DIN 77200, sodass höchste Standards eingehalten werden und alle Sicherheitsmaßnahmen den geltenden Vorschriften entsprechen.

Kontakt:
Schmalstieg GmbH Sicherheitsdienste
Zeißstraße 82 · 30519 Hannover
Tel.: +49 511 9859115
Mail: security@schmalstieg.net
Web: www.schmalstieg-sicherheitsdienste.de

Anzeigen

NetCo Body-Cam – Deeskalation statt nur Dokumentation

WE LOVE TECHNOLOGY! NetCo ist ein inhabergeführtes IT-Unternehmen mit 50+ Mitarbeitenden und Standorten in Blankenburg (Harz) und Magdeburg. Das Unternehmen entwickelt innovative Hard- und Softwarelösungen für die DSGVO-konforme Nutzung von Body-Cams & Kamerasystemen zur Baustellendokumentation. 1997 gegründet, hat sich NetCo mit seiner Body-Cam mit großem, deeskalierend wirkendem Frontdisplay vor allem erfolgreich in der Sicherheitsbranche etabliert.

Die NetCo Body-Cam wird zusammen mit der NetCo Suite in unserem Standort Blankenburg entwickelt, produziert und vertrieben und ist damit ein echtes „Made in Germany"-Produkt. Das große Frontdisplay der NetCo Body-Cam mit seiner Spiegelfunktion setzt bereits vor einer Eskalation an. Aggressive Personen werden unmittelbar mit ihrem eigenen Verhalten konfrontiert. Es folgt die Chance zur Reflexion und Wahrnehmung möglicher Konsequenzen. So werden Straftaten verhindert, statt nur dokumentiert. Das schätzen nicht nur immer mehr Polizei- und Ordnungsbehörden, sondern auch ÖPNV-Unternehmen wie die Kölner Verkehrsbetriebe, die Wiener Linien und die Deutsche Bahn.

Für Unternehmen, die bei der Anschaffung noch zögern oder die Technik erst einmal testen möchten, bietet NetCo ein monatliches Mietkonzept an. Interessierte Unternehmen erhalten Body-Cam und SmartHub kostenfrei und zahlen nur für die Softwarenutzung 50 Euro/Monat.

Mehr Infos unter www.netco.de/body-cam

Kontakt:
NetCo Professional Services GmbH
Am Mönchenfelde 13 · 38889 Blankenburg (Harz)
Tel.: +49 3944 950-0
Mail: info@netco.de
Web: www.netco.de

120 Jahre Sicherheit digital, innovativ und individuell

Seit 1902 leisten die Mitarbeiterinnen und Mitarbeiter der Wach- und Schließgesellschaft einen enorm wichtigen und spürbaren Beitrag an subjektiver und objektiver Sicherheit. Mittlerweile ist das drittälteste Sicherheitsunternehmen Deutschlands mit mehreren Hundert qualifizierten Fachkräften einer der leistungsstärksten Dienstleister in NRW. Als anerkannter Ausbildungsbetrieb hat sich die WSG als zertifiziertes Sicherheitsunternehmen mit einem umfassenden Qualitätsmanagement kontinuierlich und erfolgreich auf dem Markt durchgesetzt. Eine grundsolide Ausbildung der Mitarbeiter sowie die kontinuierliche Investition in zukunftsorientierte Technik sind die Basis einer erfolgreichen Geschäftspolitik.

Neben den üblichen Objektschutzdiensten sind die sicherheitsrelevanten Themen der Cybersecurity, der Drohneneinsatz, die Erstellung von Sicherheitsanalysen bis hin zur Installation von Sicherheitstechnik und Videotürmen obligatorische Aufgaben der WSG.

Die WSG betreibt eine der modernsten und EU-konformen Alarmempfangszentralen in Deutschland. Die Alarmverfolgung sowie Alarmbearbeitung von Alarmmelde- sowie Videoüberwachungsanlagen verstehen sich als obligatorisch. Sämtliche Leistungen der WSG unterliegen den Qualitätsnormen der Zertifizierung nach DIN EN ISO 9001 sowie DIN 77200. Bestehende Geschäftsbeziehungen seit über 70 Jahren bestätigen die erfolgreiche Geschäftspolitik der WSG.

Mehr über die Wach- und Schließgesellschaft erfahren Sie auf unserer Homepage.

Kontakt:
Wach – und Schließgesellschaft
Nachf. Herkströter GmbH & Co. KG
Deutscher Ring 88 · 42327 Wuppertal
Tel.: +49 202 27457- 0
Web: www.wsg-wuppertal.de

Anzeigen

KÖTTER Security

Ganzheitlicher Schutz durch Smart Security Solutions

Wirtschaftsspionage, organisierte Kriminalität und Infrastrukturrisiken sind nur einige Bedrohungen, denen Unternehmen und öffentliche Einrichtungen immer öfter gegenüberstehen. Mit der veränderten Sicherheitslage wächst das Bedürfnis nach Sicherheit. Die Lösung: ein ganzheitliches Sicherheitskonzept basierend auf einer individuellen Risikoanalyse.

KÖTTER Security hat im aktuellen Lünendonk-Ranking erneut seine Position als größtes Familienunternehmen der Sicherheitsbranche in Deutschland bestätigt. Kunden aus unterschiedlichen Branchen vertrauen auf die Smart Security Solutions, die die physische Sicherheit eines Objekts genauso wie die Cybersecurity umfassen. Gefragt sind hybride Lösungen bestehend aus personellen Dienstleistungen (u. a. Pforten-, Empfangs- und Revierwachdienste) und leistungsstarker Sicherheitstechnik (z. B. Videosysteme und -Sensorik), die auf die rund um die Uhr erreichbare Hightech-Notruf- und Serviceleitstelle (NSL) aufgeschaltet wird. Weitere Maßnahmen im Bereich Risiko- und Krisenmanagement, Brandschutz sowie Arbeitssicherheit und Gesundheitsmanagement leisten wichtige Präventionsarbeit und sichern für den Ernstfall ab.

Ganzheitliche Sicherheit bietet KÖTTER Security auch im Betreibermodell an: Neben der Konzeption und Umsetzung einer individuellen Sicherheitsstrategie übernimmt der Sicherheitsspezialist auch die Investition in neu zu installierende technische Systeme, den Betrieb sowie die Wartung aller Komponenten.

Kontakt:
KÖTTER Security
Wilhelm-Beckmann-Straße 7 · 45307 Essen
Tel.: +49 201 2788-388
Mail: info@koetter.de
Web: koetter.de

Stölting SECURITY SERVICE

Security with a Smile

Die Stölting Security & Service GmbH gehört zu den zehn leistungsstärksten Dienstleistern der privaten Sicherheitswirtschaft in Deutschland. Mit rund 4.000 Mitarbeitern, die durch unsere eigene Bildungsakademie kontinuierlich geschult und weitergebildet werden, stehen wir für nachhaltige Dienstleistungserbringung, Kompetenz und Qualität.

Unser inhabergeführtes Unternehmen hat sich in den letzten zwei Jahrzehnten zu einem der Marktführer in den Bereichen der stationären und mobilen Sicherheitsdienstleistungen entwickelt und sorgt mit qualifiziertem Personal und modernster Technik zuverlässig für den Schutz unserer Kunden.

Zudem hat sich mit der Stölting Eventsecurity & Service GmbH in den letzten Jahren ein bundesweit operierender Veranstaltungsdienstleister entwickelt, zu dessen Kundenkreis renommierte Veranstalter und Fußballvereine der 1. und 2. Bundesliga zählen.

Mit der Aufschaltung auf eine der modernsten Notruf- und Serviceleitstelle Europas sowie dem Einsatz von KI-basierter Video- und Verarbeitungstechnik bieten wir unseren Kunden kompromisslose Sicherheit.

Verlassen Sie sich auf Qualität und Erfahrung – Stölting Sicherheitsdienstleistungen

Zertifiziert nach DIN 77200, SCC-VAZ 2021, ISO 9001, ISO 50001 und ISO 14001.

Kontakt:
Stölting Security & Service GmbH
Johannes-Rau-Allee 11 · 45889 Gelsenkirchen
Tel.: +49 209 70279-0
Mail: info@stoelting-gruppe.de
Web: www.stoelting-gruppe.de

Anzeigen

Piepenbrock

Ihr Sicherheitsdienstleister

Wir geben Sicherheit – überall und rund um die Uhr

Ihre Sicherheit ist bei uns in besten Händen: Wir bieten zuverlässigen Schutz für Gebäude, Einrichtungen, Anlagen, Veranstaltungen und Personen. Sie suchen nach einem Partner für Empfangs- und Pförtnerdienste, Zugangskontrollen oder Revier- und Streifendienste? Profitieren Sie von unserem exzellenten Service, individuellen Sicherheitslösungen und langjähriger Erfahrung. Sowohl in der Privatwirtschaft als auch im öffentlichen Sektor sind wir für Sie da. So vertrauen zum Beispiel oberste Bundesbehörden auf unsere Expertise für Kritische Infrastrukturen – und zählen schon lange zu unseren zufriedenen Kunden.

Unsere Dienstleistungen schneiden wir genau auf Ihre Bedürfnisse zu. Basis dafür ist unser gut ausgebildetes Personal – kontinuierlich weitergebildet in unserer eigenen Akademie. Neben der Unterrichtung oder Sachkundeprüfung nach § 34a Gewerbeordnung sind viele unserer Mitarbeiter geprüfte Schutz- und Sicherheitskräfte oder haben eine Ausbildung als Fachkraft für Schutz und Sicherheit absolviert. Wir bilden unsere Mitarbeiter für speziell auf Sie zugeschnittene Wünsche aus: zum Beispiel in der Bedienung von Röntgenkontrolltechnik in Anlehnung an das Luftsicherheitsgesetz. So garantieren wir Ihnen höchste Qualität und Flexibilität.

Sie möchten von unseren maßgeschneiderten Sicherheitslösungen profitieren? Dann nehmen Sie noch heute Kontakt mit uns auf!

Kontakt:
Nicole Oppermann, Geschäftsführerin Sicherheit
Piepenbrock Sicherheit GmbH + Co. KG
Hannoversche Straße 91–95 · 49084 Osnabrück
Tel.: +49 541 5841-441
Mail: sicherheit@piepenbrock.de
Web: www.piepenbrock.de

ATLAS

ATLAS – Der Spezialmakler der Sicherheitswirtschaft

Für Sicherheitsunternehmen kann fehlender oder mangelhafter Versicherungsschutz zum existenzgefährdenden Risiko werden. Die Tätigkeiten in Krankenhäusern, Kernkraftwerken, Flughäfen, Museen, Fußballstadien oder auch bei Geldtransporten stellen hohe Anforderungen an den Deckungsschutz der verschiedenen Versicherungen. Gerade in der Betriebshaftpflichtversicherung gehen diese weit über die gesetzlichen Anforderungen oder die DIN 77200-1 hinaus.

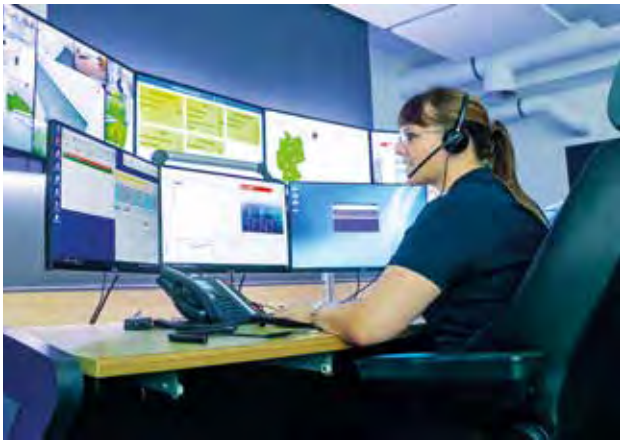
Unsere Aufgabe ist es, die Haftungssituation der Sicherheitsdienstleister schon bei der Ausschreibung zu prüfen und den erforderlichen Versicherungsschutz zu besorgen. Gerade Sicherheitsdienstleister sind aufgrund der teilweise hochsensiblen Daten in der NSL oder der AIS ein interessantes Ziel für Cyberattacken. Die Analyse des IT-Sicherheitsstandards sind die Basis für die immer wichtiger werdende Cyberversicherung, um die wir uns auch kümmern.

Seit 21 Jahren ist ATLAS ist der einzige Versicherungsmakler in Deutschland, der ausschließlich auf Sicherheitsunternehmen spezialisiert ist. Wir sind Teil der GGW Group, die mit mehr als 1.400 Mitarbeitern die drittgrößte Versicherungsmaklergruppe in Deutschland ist. Durch unsere Mitgliedschaften im BDSW, in der BDGW und im VSW gestalten wir das Umfeld der Sicherheitswirtschaft aktiv mit.

Kontakt:
Bernd M. Schäfer, Geschäftsführer
ATLAS Versicherungsmakler für Sicherheits- und Wertdienste GmbH
Industriestr. 155 ·50999 Köln
Tel.: +49 2236 49036-30
Mail: bernd.schaefer@atlas-vsw.de
Web: www.atlas-vsw.de

Anzeigen

W.I.S. – Ihr Spezialist für Corporate Security & Safety



Innovative Sicherheit mit Tradition – seit 120 Jahren sorgen wir mit unseren 4.000 qualifizierten Mitarbeitern an über 30 Standorten bundesweit und in Österreich branchenübergreifend für erstklassige Sicherheit.

In unserem ganzheitlichen Angebot kombinieren wir Mensch und Technik zu einer optimalen Einheit. Innovative und hochwertige Sicherheitstechnik schafft bei uns die Grundlage Ihres individuellen Sicherheitskonzeptes. Hier vertrauen wir nur auf die beste Sicherheitstechnik im Markt. Die 24/7-Überwachung durch unsere zertifizierte Sicherheitszentrale analysiert und wertet Daten der Sicherheitssysteme aus. Unsere personelle Sicherheitsdienstleistung rundet das ganzheitliche Angebot ab. Durch die Präsenz unserer Sicherheitsmitarbeiter im öffentlichen Raum tragen wir zusätzlich zur objektiven und subjektiven Sicherheit bei und schaffen ein sicheres Umfeld für Ihr Unternehmen.

Bei unserem Security-as-a-Service-Angebot profitieren Sie von einem Höchstmaß an Sicherheit zu bequemen monatlichen Fixpreisen.

Vertrauen Sie auf W.I.S. und lassen Sie uns gemeinsam die Sicherheit Ihres Unternehmens stärken. Kontaktieren Sie uns noch heute, um mehr über unsere umfangreichen Sicherheitslösungen zu erfahren und ein maßgeschneidertes Angebot für Ihr Unternehmen zu erhalten. Ihre Sicherheit ist unsere Priorität!

Kontakt:
W.I.S. Sicherheit & Service GmbH & Co. KG
Industriestraße 171 · 50999 Köln
Tel.: +49 2301 186 15 20
Mail: info@wis-sicherheit.de
Web: www.wis-sicherheit.de

Seit 1983 Ihr Experte für Sicherheitsdienstleistungen

Daniel M. Ponds Passion für Taekwondo entstammen die Leitlinien Sicherheit, Struktur und Disziplin, die die Pond Security Service GmbH heute so erfolgreich machen. Seit 40 Jahren bewacht Pond mit über 3.000 Mitarbeiterinnen und Mitarbeitern über 100 Objekte in ganz Deutschland und dies auf höchstem Niveau, geprüft und zertifiziert nach DIN 77200.

Zur Kernkompetenz des Unternehmens gehört unter anderem die Sicherung von hochsensiblen Einrichtungen wie Konsulaten, Gerichten, militärischen Liegenschaften, Forschungszentren, Banken, Kernkraftwerken und Industrieanlagen.

Die Aus- und Weiterbildung der Mitarbeitenden steht dabei für Pond an oberster Stelle. Durch die Bildungszentrum Pond Academy GmbH ist das qualifizierte Personal stets individuell auf die Anforderungen der Kunden und die Gegebenheiten vor Ort geschult. Hinzu kommen zahlreiche technische Sicherheitslösungen wie Hand- und Torsonden, Videoüberwachung, Röntgenanlagen und Drohnen. Ausgebildete und zertifizierte Schutz- und Sprengstoffspürhunde-Teams bilden die zuverlässige vierbeinige Verstärkung für die Sicherheitskräfte der Pond Security. Mit dieser Grundlage können wir Ihnen eine maßgeschneiderte Lösung für die Sicherheit Ihres Objekts bieten.

Für mehr Infos oder bei Rückfragen sprechen Sie uns gerne an.

Kontakt:
Pond Security Service GmbH
Rückinger Str. 12 · 63526 Erlensee
Tel.: +49 6183 806-0
Mail: info@pond-security.com
Web: www.pond-security.com

Anzeigen

INDUSTRIE-BEWACHUNG
BRUNO WACHTMEISTER GMBH & CO KG

Experten für Ihre Sicherheit!

Die INDUSTRIE-BEWACHUNG WACHTMEISTER bietet seit vielen Jahrzehnten höchste Zuverlässigkeit und Kompetenz bei der Sicherung von Eigentum. Mit modernster Technik, bestens ausgebildetem Personal und perfektem Service sorgen wir rund um die Uhr für die Sicherheit unserer Kunden.

Zu unseren Dienstleistungen gehören unter anderem

- Werk- und Objektschutz
- Revier- und Streifendienst
- Alarmaufschaltung mit Intervention
- Empfangs- und Inhousedienste
- Arbeitssicherheit

Dem Vertrauen, das unsere Kunden seit vielen Jahrzehnten in uns setzen, werden wir durch kompromisslosen Einsatz für Qualität gerecht.

Die WACHTMEISTER-Vorteile

- Exzellente Erfahrung
- Intelligente Organisation
- Absolute Zuverlässigkeit
- Modernste Ausstattung
- Professioneller Service

Zertifizierte Serviceleitstelle

Unsere Alarmempfangsstelle (AES) genügt allen technischen Anforderungen an eine moderne Serviceleitstelle und ist nach DIN EN 50518, VdS 3138 mit Alarmprovider-Zulassung und VdS 2172 zertifiziert. Sie kann fast jedes System oder Protokoll für Alarm-, Störmelde- und Aufzugsanlagen empfangen. Aufschaltungen rund um die Uhr ohne Voranmeldung möglich.

Kontakt:
Kevin Holck
INDUSTRIE-BEWACHUNG
Bruno Wachtmeister GmbH & Co. KG
Bellingweg 14 · 70372 Stuttgart
Tel.: +49 711 955918-39
Mail: kh@ib-bw.de
Web: www.ib-bw.de

SECURITON

Der findigste Anwendungsspezialist für Sicherheit

Securiton Deutschland ist Ihr Partner für individuelle Belange rund um intelligente Alarm- und Sicherheitssysteme. Seit 45 Jahren bieten wir Ihnen intelligente Sicherheitstechnik für Brand-, Objekt- und Perimeterschutz.

Im Bereich Safety sind wir mit unseren Brandmeldesystemen und der Sonderbrandmeldetechnik der Sicherheitspionier für Brandfrühesterkennung. Aber auch elektroakustische Systeme sind hier eine wichtige Komponente.

Im Bereich Security sichern wir nicht nur den Boden, sondern auch den Luftraum. Wir nennen das „Dome Security", weil wir eine Art „Schutzschirm" über die Areale und Gebäude unserer Kunden legen – am Boden und in der Luft. Die wichtigsten Bestandteile dieses Schutzschirms sind die intelligente Videoüberwachung mit IPS-Faktor und die einzigartige Drohnendetektion und -abwehr. Aber auch ein hochintegrales Sicherheitsmanagement, die Zaundetektions- und Zutrittskontrollsysteme sowie Einbruch- und Gefahrenmeldeanlagen runden unser Portfolio erst zu einem ganzheitlichen Paket ab – für Ihren kompletten Rundumschutz.

Als Lösungsspezialist ist es unser Ziel, Sie persönlich zu beraten und Sie in allen anstehenden Sicherheitsfragen individuell zu betreuen. Dafür stehen wir an unseren 16 Standorten bundesweit für Sie bereit – auch in Ihrer Nähe.

Der Schutz von Leben und Sachwerten ist unsere Leidenschaft. Daher begeistern wir mit ganzheitlichen und hochwertigen Sicherheitslösungen.

Besonders. Sicher.

Kontakt:
Securiton Deutschland
Alarm- und Sicherheitssysteme
Von-Drais-Straße 33 · 77855 Achern
Tel.: +49 7841 6223-0
Mail: willkommen@securiton.de
Web: www.securiton.de

Anzeigen

ZIEMANN SICHERHEIT

ZIE.CAM.
Mobile Videoüberwachung.
Immer. Alles. Überblicken.

Sie ärgern sich wiederkehrend über unerlaubtes Betreten, Diebstahl, illegale Müllentsorgung, Graffitis und Vandalismus auf Ihrem Gelände? Die ZIE.CAM., unser mobiler ZIEMANN Videoturm, löst das Problem. Denn die ZIE.CAM. überwacht vor Ort rund um die Uhr Ihr Gelände oder Objekt. Jedes unerlaubte Betreten wird von uns erkannt.

Die ZIE.CAM. kann an unterschiedlichsten Objekten, Geländearten und Liegenschaften eingesetzt werden. Auf kleinster Grundfläche positionieren wir sie vor Ort, schalten sie auf unsere ZIEMANN Notruf- und Serviceleitstelle auf und erhalten 24/7 wetterunabhängig und DSGVO-konform Videobilder in optimaler Qualität.

ZIEMANN PLUSPUNKTE: Wir liefern Konzept, Technik, Aufschaltung und Überwachung aus einer Hand! Durch die Aufschaltung der ZIE.CAM. auf unsere zertifizierte ZIEMANN Notruf- und Serviceleitstelle haben wir die Lage immer im Blick und können bei Erfordernis umgehend entlang eines für Sie erstellten Sicherheitskonzeptes und angepasst auf die Anforderungen vor Ort reagieren.

Jede ZIE.CAM. entsteht bei uns in unternehmenseigener Konstruktion durch die Südalarm Czerulla GmbH, unsere auf Sicherheitstechnik spezialisierte Unit. Ein großer Vorteil für unsere Kunden, denn so lässt sich jede ZIE.CAM. von Beginn an auch baulich auf die Herausforderungen jeder Kundenlokation anpassen. Zugleich stellt die ZIEMANN-Inhouse-Produktion die Lieferfähigkeit der Systeme sicher.

Kontakt:
ZIEMANN SICHERHEIT GmbH
Gewerbestraße 19–23 · 79227 Schallstadt
Tel.: +49 621 84240-444
Mail: sicherheitsdienst@ziemann-gruppe.de
Web: **https://www.ziemann-gruppe.de/leistungen/mobile-videoüberwachung.html**

DSD

SICHERHEIT DIREKT ZU IHNEN NACH HAUSE GELIEFERT!

Lassen Sie sich den DSD liefern.

Der DSD ist für alle, die sich für die Sicherheitswirtschaft interessieren bzw. in dieser tätig sind.

AKTUELL. UMFASSEND. DIREKT.

Sie bekommen die aktuellen Themen aus allen Bereichen der Sicherheitswirtschaft wie Wirtschaft, Politik, Arbeit, Soziales, Technik, Unternehmen und Märkte druckfrisch auf den Tisch. Außerdem auch online — tagesaktuell!

Weitere Infos unter
www.dersicherheitsdienst.de

Herausgeber:
Deutsche Sicherheits-Akademie GmbH
Am Weidenring 56 - 61352 Bad Homburg

Eine Frage in die Runde

CER-Richtlinie zum Schutz der Kritischen Infrastrukturen: Wie bewerten Sie diese?

Die Erstveröffentlichung des Beitrags erfolgte am 25. Juli 2023 unter www.marktplatz-sicherheit.de.

Wir bedanken uns für die Abdruckgenehmigung.

Im Interview mit **Dr. Berthold Stoppelkamp**, Geschäftsführer des Bundesverbandes der Sicherheitswirtschaft (BDSW), **Ralf Philipp**, Leiter Marketing & Geschäftsentwicklung der CMD – Sicherheit und Dienstleistungen GmbH & Co. KG, **Sebastian Otten**, Sicherheitskoordinator bei der OBJEKTCONTROL Sicherheitsdienste Vogt GmbH, und **Tony Fleischer**, Geschäftsführer der proSicherheit GmbH.

Eine kurze Einleitung

Die sogenannten Kritischen Infrastrukturen (KRITIS) sind in Zeiten, in denen Russland einen Angriffskrieg gegen die Ukraine führt, gegen andere europäische Länder Drohungen ausspricht und sich mit unzähligen Hacker-Angriffen auf die verschiedensten Einrichtungen und Organisationen in Europa exponiert, potenziell besonders gefährdete Angriffsziele. Kein Wunder, dass der Europäische Rat und das Europäische Parlament diese Infrastrukturen besonders geschützt sehen will. Deshalb haben sie jüngst eine EU-Richtlinie (CER-Richtlinie) verabschiedet, die im vergangenen Dezember in Kraft getreten ist, die KRITIS-Widerstandsfähigkeit stärken und bis Oktober 2024 auf nationaler Ebene umgesetzt sein soll. Unter anderem empfiehlt sie die Qualitätskontrolle von privatem Sicherheitspersonal im KRITIS-Umfeld. Sie schreibt diese Qualitätskontrolle nicht etwa vor, sondern sie empfiehlt sie nur. Ob diese Empfehlung Behörden und Betreiber, die sich der Bedeutung ihrer Einrichtungen schon heute bewusst sein müssten, jetzt zu einem Umdenken dahin gehend bewegen mag, dass sie – anders als bis jetzt oft zu beobachten – ausreichend geschultes und ausgerüstetes Sicherheitspersonal einsetzen? Falls ja, könnten wir uns auch vorstellen, dass fortan die Empfehlung genügt, beispielsweise nicht in anderer Leute Haus einzubrechen oder keine Geldtransporter zu überfallen. Oder ist das zu polemisch? Wie bewerten Sie die CER-Richtlinie?

„Zwangszertifizierung lehnen wir ab“

Dr. Berthold Stoppelkamp
Geschäftsführer des Bundesverbandes der Sicherheitswirtschaft (BDSW)

Der BDSW begrüßt, dass sich künftig der nationale Gesetzgeber durch ein KRITIS-Dachgesetz im Rahmen der europäischen CER-Richtlinie in einem ganzheitlichen Schutzansatz zum Schutz von KRITIS nicht mehr allein auf die IT-Sicherheit fokussieren wird. Der BDSW strebt nicht die Anerkennung der gesamten Sicherheitswirtschaft als eigenständiger KRITIS-Sektor an.

Das Sicherheitsgewerbe mit seinen nunmehr über 270.000 Beschäftigten erbringt seit Jahren immer mehr Tätigkeiten, die der Absicherung beziehungsweise Aufrechterhaltung von sämtlichen KRITIS-Sektoren in Deutschland dienen. Dazu zählen Objektschutzaufgaben, Schutz von Lieferketten, Sicherstellung der Bargeldversorgung, Gewährleistung von Sicherheit und Ordnung im Personenverkehr und Durchführung von Luftsicherheitskontrollen. Das Sicherheitsgewerbe ist bereits heute faktisch integraler Bestandteil beim Schutz sämtlicher KRITIS-Sektoren und systemrelevant für die Resilienz von KRITIS.

Der nationale Gesetzgeber sollte die Systemrelevanz des Sicherheitsgewerbes übergreifend für Bund und Länder für den Schutz von KRITIS festschreiben. Im neuen Sicherheitsgewerbegesetz sollten verbindliche Basisqualitätsanforderungen für Sicherheitsunternehmen und ihre Beschäftigten festgeschrieben werden, die im Bereich KRITIS zum Einsatz kommen. Sofern sich KRITIS-Betreiber externer Sicherheitsdienstleister bedienen, dürfen nur Unternehmen und Beschäftigte des Sicherheitsgewerbes zum Einsatz

kommen. Für diesen Personenkreis – bei Einsatz in Objekten mit besonderem Gefährdungspotenzial – ist bereits heute auf gesetzlicher Grundlage eine Zuverlässigkeitsüberprüfung unter Nutzung des Bewacherregisters garantiert. Es bedarf insoweit nicht der Einführung einer zusätzlichen, neuen „Zuverlässigkeitsüberprüfung" für diesen Personenkreis.

KRITIS-Betreiber können künftig auf der Grundlage bestehender Industrienormen (beispielsweise EN 17483: Sicherheitsdienste für den Schutz Kritischer Infrastrukturen) zusätzliche, branchenspezifische weitere Qualitätsanforderungen an Sicherheitsdienste und ihre Beschäftigten stellen. Eine gesetzliche Pflicht zur „Zwangszertifizierung" lehnen wir ab."

„Was nutzen Empfehlungen, wenn nicht einmal Gesetze befolgt werden?"

KRITIS ist in Sachen öffentlicher Sicherheit nicht nur ein spannendes, sondern auch ein durchaus kontroverses Thema. Auf der einen Seite will man so viel Sicherheit wie möglich, auf der anderen Seite soll das möglichst wenig kosten. Um das „beste" Angebot zu erhalten, rufen die Betreiber einen Wettbewerb der Dienstleister aus, den in der Regel der billigste Anbieter gewinnt.

Viele Regelwerke sind angefüllt mit „Kann"-Formulierungen. Dienstleistungsverträge, ganz besonders die der öffentlichen Hand, enthalten in der Regel einen Passus hinsichtlich der internen Qualitätssicherung und daraus resultierenden Bonus/Malus-Regelungen. Natürlich orientieren sich diese nicht an der neuen CER-Richtlinie. Und wenn wir bestimmte KRITIS-Bereiche außen vor lassen – beispielsweise Sicherheitsdienstleistungen in militärischen oder kerntechnischen Anlagen, für die es sehr umfangreiche gesetzliche Regelungen gibt –, findet auch die DIN 77200 wenig Beachtung. Im Idealfall orientieren sich die Regelungen zur Durchführung von Kontrollen auch an der Thematik KRITIS. In der Praxis spielt es meines Erachtens eine untergeordnete Rolle.

In der neuen CER-Richtlinie gibt es einen Passus hinsichtlich der Qualifikation von Personal (Art. 13 Resilienzmaßnahmen kritischer Einrichtungen). In Deutschland sehe ich hier die Gewerbeaufsicht und Ordnungsbehörden gemeinsam mit dem Bundesinnenministerium in der Pflicht. Das Bewacherregister könnte hier eine wichtige Rolle spielen. Würden alle Regelungen durch die prüfenden Behörden bundesweit einheitlich umgesetzt und in regelmäßigen Abständen auch ohne externe Veranlassung (zum Beispiel Beschwerde) überprüft, wäre das schon ein großer Schritt in die richtige Richtung. Aber davon sind wir weit entfernt. Mir fallen auf Anhieb Dienstleister ein, die den vorhandenen Spielraum nicht nur maximal ausnutzen, sondern klar überschreiten und gegen die gesetzlichen Regelungen verstoßen. Teilweise mit Kenntnis der Auftraggeber.

Wenn also unsere aktuellen verpflichtenden Regelungen von einigen Unternehmen aktiv ignoriert werden, während diese Verstöße von den Auftraggebern der öffentlichen Hand ignoriert werden – was will ich dann mit einer Richtlinie voller Empfehlungen ausrichten?

Unternehmen, die alle gesetzlichen Anforderungen erfüllen, haben in der Regel einen erheblichen Nachteil bei der Kapazität des benötigten Personals oder schlicht keine Chance, preislich gegen Unternehmen zu halten, die gesetzliche Vorgaben eher als Empfehlung interpretieren und so die Preise deutlich nach unten drücken können. Sie geben schlicht das „beste" Angebot für den Auftraggeber ab.

Ralf Philipp

Leiter Marketing & Geschäftsentwicklung der CMD – Sicherheit und Dienstleistungen GmbH & Co. KG

„Bleibt deutlich hinter den Erwartungen zurück“

Sebastian Otten

Sicherheitskoordinator bei der OBJEKTCONTROL Sicherheitsdienste Vogt GmbH

Es ist offensichtlich fraglich, ob Empfehlungen allein ausreichen, um Behörden und Betreiber zum Umdenken zu bewegen. Dies wird in der polemischen Schlussfrage deutlich. Gut ausgebildetes und ausgerüstetes Sicherheitspersonal bildet das Rückgrat unserer Gesellschaft und unserer Liegenschaften. Allerdings hat Qualität ihren Preis, und Schulungen sowie angemessene Ausrüstung müssen in der Budgetierung berücksichtigt werden. Daher ist eine Empfehlung allein nicht ausreichend, um echte Veränderungen zu bewirken, die Branche wird zu oft über den Preis gebremst.

Ein erster Schritt zur Verbesserung der Sicherheit von KRITIS besteht im verpflichtenden Einsatz ausgebildeter Fachkräfte. Eine weitere wichtige Maßnahme ist die ausschließliche Beauftragung von Unternehmen, die gemäß DIN 77200 zertifiziert sind. Diese Zertifizierung stellt sicher, dass die Unternehmen bestimmte Qualitätsstandards erfüllen und ihren Angestellten eine kontinuierliche Weiterbildung von mindestens 30 Zeitstunden pro Jahr bieten.

In der Kombination wird sichergestellt, dass das eingesetzte Sicherheitspersonal über das notwendige Know-how und die Fähigkeiten verfügt, um den Schutz von KRITIS effektiv zu gewährleisten. Die sich ständig weiterentwickelnden Bedrohungen erfordern eine kontinuierliche Anpassung der Sicherheitsmaßnahmen und -technologien. Durch die jährliche Weiterbildung wird das Wissen auf dem neuesten Stand gehalten. Fachkräfte für Schutz und Sicherheit bringen das erforderliche Fachwissen und die Erfahrung mit, um Risiken zu erkennen, Bedrohungen zu analysieren und angemessene Sicherheitsmaßnahmen zu implementieren.

Es ist höchste Zeit, dass Europa verbindliche Mindeststandards für den Schutz von KRITIS definiert und umsetzt. Die CER-Richtlinie bleibt allerdings deutlich hinter den Erwartungen zurück und kann allein nicht ausreichen, um die Sicherheit zu gewährleisten.

„Ein zahnloser Tiger als erster Schritt“

Tony Fleischer

Geschäftsführer der proSicherheit GmbH

Diese Ausarbeitung von Richtlinien ist in allererster Linie ein guter Start auf dem Weg, unsere kritische Infrastruktur schützen zu wollen. Während kerntechnische Anlagen bereits über gute Verfahrensweisen zur Qualitätskontrolle verfügen, fehlt zum Beispiel den meisten Krankenhäusern diese Expertise. Die mir bekannte Richtlinie eines Trinkwasserversorgungsunternehmens sieht vor, dass nach Alarmauslösung über 80 Außenstellen binnen zwölf Stunden mit zwei Sachkundlern besetzt werden müssen. Natürlich 24 Stunden lang auf unbestimmte Zeit. Getestet wurde dies nie, aber auf dem Papier las sich das gut.

Hier bedarf es (je nach zu schützender Einrichtung) einer einheitlichen Vorgabe, was denn ein Sicherheitsdienst und die eingesetzten Sicherheitsmitarbeiterinnen und -mitarbeiter eigentlich leisten können sollten und wie dies zu überprüfen ist. Dass eine reine Empfehlung ein zahnloser Tiger ist, sollte jedem bewusst sein.

Es kann nur die Hoffnung bestehen, dass dies der erste Schritt ist auf dem Weg, mehr verbindliche Qualität zu schaffen und den durch Bürokratie ohnehin schon belasteten Kunden eine einheitliche Handlungsanweisung unterstützend an die Hand zu geben.

VdS-BrandSchutz Tage
FACHMESSE | FACHTAGUNGEN | THEMENFOREN

VdS-BrandSchutzTage 2023 am 6. und 7. Dezember in der Koelnmesse

Auf den renommierten VdS-BrandSchutzTagen werden am 6. und 7. Dezember 2023 wieder mehrere Tausend Fachbesucherinnen und -besucher erwartet, wie gewohnt in der Koelnmesse. Dank des wachsenden Erfolgs der Veranstaltung wird die große, internationale Fachmesse erstmals in der größeren Messehalle 10.1 ausgerichtet, in der noch mehr Aussteller und Livevorführungen Platz finden. Daneben profitieren die Messebesucherinnen und -besucher vom vielseitigen Programm auf der Messebühne sowie separat buchbaren Fachtagungen in den angrenzenden Sälen. Die VdS-BrandSchutzTage 2023 werden vom Kölner Bürgermeister Dr. Ralf Heinen eröffnet.

Internationale VdS-Fachtagung „Feuerlöschanlagen“

Die Fachtagung „Feuerlöschanlagen“ findet auf den VdS-BrandSchutzTagen 2023 mit internationalem Fokus und deutsch-englischer Simultanübersetzung statt und erstreckt sich über beide Veranstaltungstage – wie traditionell in jedem zweiten Jahr. Thematisiert werden aktuelle Fallbeispiele und Lösungen aus dem In- und Ausland.

Auch die anderen Fachtagungsklassiker der VdS-BrandSchutzTage dürfen nicht fehlen. Insgesamt stehen diese Tagungen auf dem Programm:

- Baulicher Brandschutz (6. Dezember 2023)
- Feuerlöschanlagen international/Fire Extinguishing Systems (mit Simultanübersetzung D/EN, 6./7. Dezember 2023)
- Hydrantenanlagen (Impulstagung, 6. Dezember 2023)
- 54. Fortbildungsseminar für Brandschutzbeauftragte (6./7. Dezember 20233)
- Brandmeldeanlagen (7. Dezember 2023)
- Rauch- und Wärmeabzugsanlagen (7. Dezember 2023)
- Bauen und Brandschutz in NRW (Kompaktseminar, 7. Dezember 2023)

VdS-BrandSchutzTalk und Foren

Die zwei Talkrunden des VdS-BrandSchutzTalks auf der Messebühne zogen auf den letzten VdS-BrandSchutzTagen viele Interessierte an. Auch in 2023 können alle Messebesucherinnen und -besucher kostenlos zuhören, wenn Expertinnen und Experten über wichtige Branchentrends diskutieren. Außerdem wieder auf der Messebühne: das Zukunfts- und das Ausstellerforum mit weiteren aktuellen Themen.

Freikarte

Für unsere Leser stehen kostenlose Eintrittskarten für den Messebesuch zur Verfügung. Die Freikarten können unter **vds.de/dsd** bezogen werden.

vds-brandschutztage.de

Ein wichtiger Bestandteil der VdS-BrandSchutzTage: die große Fachmesse mit Anbietern aus dem anlagentechnischen, baulichen und organisatorischen Brandschutz

Aktuelles Wissen zu spannenden Branchenentwicklungen bieten die separat buchbaren Fachtagungen auf den VdS-BrandSchutzTagen 2023

Live auf der Messebühne der VdS-BrandSchutzTage diskutieren Expertinnen und Experten über aktuelle Branchenthemen

Künstliche Intelligenz unterstützt den Sicherheitsdienstleister

Von Reinhard Rupprecht

Reinhard Rupprecht
Vizepräsident des BKA a.D., Ministerialdirektor beim BMI a.D. und heute als unabhängiger Berater in Sicherheitsfragen tätig

Künstliche Intelligenz (KI) ist als Fortentwicklung der Digitalisierung die Schlüsseltechnologie des 21. Jahrhunderts und erlebt als generative KI (Chatbot GPT – generative pretrained transformer) in den Medien und bei Fachveranstaltungen derzeit einen Hype. Noch vor einem Jahrzehnt spielte sie in der Sicherheitswirtschaft eine geringe Rolle, aber ihre Bedeutung auch für das Sicherheitsgewerbe wächst exponentiell.

KI – ein breites technologisches Spektrum

Der Begriff KI taucht erstmals 1955 in einer Schrift des US-Informatikers John McCarthy auf. Es gibt bisher keine allgemeingültige Definition von KI in der Fachliteratur, in Rechtsvorschriften oder technischen Normen. Am einfachsten lässt sich KI begreifen als selbstständiges Lernen von Maschinen oder deren Software, das sich innerhalb bestimmter Parameter selbst optimiert, oder als Eigenschaft eines IT-Systems, menschenähnliche intelligente Verhaltensweisen zu zeigen (Bitkom e. V. und Deutsches Forschungszentrum für künstliche Intelligenz; **www.dfKI.de**). Digitalisierung bildet die Voraussetzung für KI.

KI lässt sich in Teilbereiche und Entwicklungsstufen klassifizieren:

- Maschinelles Lernen im Erkennen von Mustern, Anomalien und Korrelationen
- Bildung neuronaler Netze, die die Sensorik befähigen, Muster und Anomalien zu erkennen,

die der Mensch nicht ohne Weiteres sehen oder hören kann
- Robotic Process Automation
- Deep Learning als selbstständiges Optimieren der Detektionsfähigkeit durch wachsende, qualitativ einwandfreie Datenmengen und Datenverarbeitung
- Automatisierung und Vernetzung von Prozessen in Wirtschaft und Verwaltung in Form von Texten, Lagebildern und Modellen
- Suche nach Kausalitäten durch Berechnung der Wahrscheinlichkeit und anteiligen Stärke einzelner Ursachen mittels Korrelationen (Data Mining)
- wissensbasierte Expertensysteme mit der Fähigkeit zu logischen Schlüssen auf der Grundlage formalisierten Fachwissens in verschiedenen Wissenschaftsbereichen
- generative KI durch Verarbeitung möglichst großer Datenmengen des Weltwissens mittels intelligenter Algorithmen mit der Fähigkeit einer allumfassenden Suchmaschine und der Generierung von Texten und Ausarbeitungen entsprechend den Nutzerwünschen (Chatbot GPT)
- Quantensprung in der Quanten- und Kryptotechnologie durch Anwendung von KI

Digitalisierung und KI in der Infrastruktur des Sicherheitsdienstleisters (SDL)

KI wird den SDL bei vielen informationsbasierten Büroarbeiten unterstützen, weil sie mithilfe von Algorithmen Datenmengen ordnen, analysieren und vernetzen kann. Neuronale Netze können gewaltige Text- und Bilddatenmengen verarbeiten. So ermöglicht zum Beispiel die KI Luminous von Aleph Alpha die Verarbeitung von beliebigen Text- und Bildkombinationen (Jons Andrulis in der FAZ am 16. Mai 2022). Wenn der SDL die Voraussetzungen für die Annahme von Best-Practice-Lösungen definiert, kann KI aus der Gesamtheit der operativen und geschäftlichen Daten in einem bestimmten Zeitraum Best Practices errechnen und begründen. Laut der Studie „AI-Ambitions 2022“ nutzten in diesem Jahr 21 Prozent der deutschen Unternehmen alle operativen Daten in KI- und Maschine-Learning-Projekten (Sicherheitsforum 5/2022, Seite 30). Für bundesweit tätige SDL mit hohen Beschäftigtenzahlen kann es erforderlich sein, für die Erfüllung eines neuen Auftrags Mitarbeiter zu gewinnen, die aufgrund ihrer Fähigkeiten und Mobilitätsbereitschaft am ehesten dafür in Betracht kommen. Mithilfe von KI ist es möglich, aus der Gesamtheit der Mitarbeiterdaten die nach den Vorgaben des SDL geeignetsten Mitarbeiter systematisch zu ermitteln. Allerdings ist für eine solche Verarbeitung personenbezogener Daten in einer „SKIII“-Datei die Zustimmung aller erfassten Mitarbeiter erforderlich. Mithilfe von Algorithmen lassen sich bei einer systematischen Analyse von Abrechnungsdokumenten auch finanzielle Unregelmäßigkeiten und Betrügereien erkennen. So haben Forscher des Fraunhofer-Instituts für Techno- und Wirtschaftsmathematik eine Software auf Basis von KI zur Erkennung von Abrechnungsbetrug bei Pflegeleistungen entwickelt (FAZ am 30. September 2022). Mit KI kann der Sicherheitsdienstleister auch die IT-Sicherheit seines Unternehmens erhöhen. Maschinelles Lernen wird zum Erkennen von Anomalien, von Phishingmails, Spammails und Schadsoftware verwendet.

KI im operativen Bereich

Mithilfe von KI lassen sich Sicherheitsdienstleistungen effizienter und kostengünstiger erbringen. Das gilt insbesondere für den Einsatz von Sicherheitstechnik in den unterschiedlichsten Bereichen. Beim Perimeterschutz können verschiedene Sensortechnologien – Videoüberwachung, Radar, Lidar, Verkabelung im Zaun oder im Boden verlegt – zum Einsatz kommen, die in ihren Funktionen der Detektion, der Fehlalarmresistenz und der Verfolgung eines eingedrungenen Täters durch KI mittels präziser Mustererkennung, Objektbestimmung, Richtungserkennung und Nachverfolgung durch vernetzte Kamerasysteme optimiert werden. Die Kombination multispektraler PTZ-Kameras mit Radar erhöht die Erkennungswahrscheinlichkeit und reduziert Fehlalarme (DSD 1/2021, Seite 18–20). In der Zutrittskontrolle spielt KI eine bedeutende Rolle. Die Zutrittsberechtigung wird digital auf einen RFID-Ausweis übertragen und am Eingangsterminal durch einen Update-Leser überprüft und aktualisiert. Zugangsberechtigung, etwaige Beschränkungen des Zugangs zu bestimmten sensiblen Innenbereichen und das Besuchermanagement werden miteinander verknüpft. Der Zutritt zu hochsensiblen Bereichen ist mit einer Zwei-Faktor-Authentifizierung ausgestattet. Die Identitätsprüfung kann durch den Vergleich biometrischer Merkmale erfolgen. Die Begrüßung eines Besuchers und seine Unterstützung im Anmeldeprozess übernimmt ein Roboter. Für die Zufahrtskontrolle ist die Kennzeichenerfassung durch Videoüberwachung ein probates Mittel. Mit dem Weitbereichsleser für Schranken, Rolltore oder Garagenzufahrten werden auf Basis von Ultrahochfrequenz Transponder auch aus dem Fahrzeug heraus gelesen. Die Einfahrtsberechtigung lässt sich mit der Steuerung des Fahrzeugs im Kontrollbereich und mit der Zuweisung eines Parkplatzes verknüpfen. KI lässt sich zur Optimierung des Zufahrts- und Zutrittskontrollmanagements bei Großveranstaltungen durch Erkennung und wirksame Lenkung von Besucherströmen, vorausschauende

Berechnungen des Verkehrsflusses und dem Aufspüren einer etwaigen Panikentwicklung einsetzen. Die Branddetektion wird durch KI optimiert. So arbeitet zum Beispiel das Edwards-ModuLaser-System mit Algorithmen zur Staubunterdrückung. Durch automatische Anpassung an die jeweiligen Umgebungsbedingungen werden höchste Empfindlichkeit, optimale Alarmschwellen und niedrige Fehlalarmraten sichergestellt. Mit der Überwachung der internen Meldermesskammer und dem davorliegenden Staubfilter kann die KI die Betriebsparameter automatisch kontinuierlich anpassen, um einer Verunreinigung entgegenzuwirken (Frank Einlehner in GIT Sicherheit, 7-8/2021, S. 66 f.). Auch das Branderkennungssystem Aviotec von Bosch arbeitet auf der Basis von KI-Algorithmen, die Feuer und Rauch bei wechselnden Wetter- und Lichtverhältnissen erkennen können (GIT Sicherheit, 10/2021, S. 96 f.). Und das von IQ wireless GmbH entwickelte Sensorsystem IQ FireWatch ist ebenfalls unter allen Wetterbedingungen einsetzbar und detektiert Rauch bis zu 60 km Entfernung. Es ist daher insbesondere zur). Das System deckt durch eine Kombination verschiedener Sensoren einen Spektralbereich von 400 bis 1.100 Nanometer ab, sodass seine „Sehkraft" die des menschlichen Auges übertrifft. Ähnlich dem von Polizeibehörden angewandten „predictive policing" kann ein Sicherheitsdienstleister durch ein entsprechendes „predictive risk management" (PRM) die Prognose der Eintrittswahrscheinlichkeit von kriminellen Angriffen oder sonstigen Schadensereignissen bei einem Unternehmen, in einem Wohnbezirk (gated area) oder einem sonstigen räumlichen Bereich (z. B. Geschäftsquartier, Gewerbegebiet, Windräder- oder Solarpark oder einer anderen, eventuell abgelegenen, Kritischen Infrastruktur), dessen Schutz er übernommen hat, faktenbasiert verlässlicher machen. Alle relevanten soziografischen, infrastrukturellen, sicherheitstechnischen und verkehrsspezifischen Daten einschließlich bisheriger Sicherheitsvorfälle in tages-, wochen- und jahreszeitlicher Einordnung müssen mithilfe intelligenter Algorithmen ausgewertet werden. Die Verlässlichkeit des Berechnungsergebnisses hängt vor allem von der Qualität und Quantität der verarbeiteten Datenmenge ab. Besonders wertvoll sind Daten über abgebrochene Angriffe aufgrund erkannter oder nicht überwundener Sicherheitstechnik. Auf diese Weise können Sicherheitslücken erkannt und geschlossen, Kontrollstreifen gezielter und effektiver eingesetzt werden. Bei Kontrollgängen innerhalb eines Unternehmens/Gebäudes zeigt das KI-unterstützte Wächterkontrollsystem der Streife an, welche Punkte, Räume, Türen oder Anlagen aufgrund der ausgewerteten Sensorik besondere Aufmerksamkeit erfordern.

KI unterstützt die Maschinensicherheit in vielfältiger Weise. So kann ein räumlicher Gefahrenbereich durch optische Sensoren überwacht werden, indem durch eine Software aufgenommene Bilddaten von drei räumlich getrennt angeordneten Sensoren zu einem dreidimensionalen Abbild zusammengesetzt werden. Oder es werden zum Beispiel die sicherheitsrelevanten Parameter einer Aluminiumdruckgasanlage mit Sensoren erfasst, und die Anlage wird abgeschaltet, wenn Druck oder Temperatur außerhalb des zugelassenen Sicherheitsbereichs liegen. Ein übergeordneter Anomaliedetektor erkennt auf Basis eines „Entscheidungsbaum-Algorithmus" Sensor-, Netzwerk- und Hardwarefehler und löst in Echtzeit einen Stopp der Anlage aus. Bei allen sicherheitstechnischen Anlagen wird die Wartungs- und Instandhaltungsorganisation durch KI revolutioniert. Aufgrund aller verfügbaren Daten aus dem Konstruktionsprozess und dem gesamten Lebenszyklus, aus dem laufenden Betrieb, den Einsatz- und Umgebungsbedingungen wird im KI-basierten „predictive maintenance"-Verfahren der jeweils optimale Wartungs- und Instandhaltungszeitpunkt errechnet. Damit können ein Anlagenausfall und eine kostenaufwendige Betriebsunterbrechung vermieden werden. Auch die Leitstellentechnik wird durch KI optimiert. Insbesondere können Alarmmeldungen mit Lagebildaufrufen und auch Leitstellen mit unterschiedlichen Softwaresystemen mithilfe von Algorithmen vernetzt werden.

Robotik und Drohnen

Robotik unterstützt den SDL in vielen Funktionen. Roboter eignen sich für die Perimeterbestreifung, Kontrollgänge in Objekten,

messtechnische Aufgaben und Überprüfung von Alarmen. So wird zum Beispiel der geländegängige, radgetriebene Argus von SMD Robotics für Patrouillendienste und mobile Videoüberwachung, der vierbeinige Spot von Boston Dynamics für Kontrollgänge, Mess- und Prüfaufgaben und der radgetriebene Promobot von RDI Robots für digitale Empfangsdienste und Indoorpatrouillen eingesetzt. Wie das Fraunhofer-Institut für Fabrikbetrieb und -automatisierung berichtet (GIT Sicherheit, 3/2022, S. 56 f.), hat es mit dem Cobot-Planer eine webbasierte Applikation entwickelt, die ermittelt, bei welchen Geschwindigkeiten des Roboters eine sichere Zusammenarbeit gewährleistet ist. Die Planungshilfe unterstütze Programmierer bei der sicheren Auslegung von kollaborativen Robotern. Forscher vom Califonia Institute of Technology haben eine „rollende Drohne" vorgestellt, einen Multifunktionsroboter, der seine vier Räder vielfältig einsetzen kann, um Treppen oder Mauern zu überwinden, und sie als Rotoren nutzt, um als Drohne zu agieren. Drohnen sind für den SDL sowohl für den Objektschutz, vor allem von Anlagen oder Knotenpunkten von Versorgungsleitungen fernab

vom Kernbereich eines Unternehmens, wie für die Früherkennung und Schadensüberprüfung in der Branddetektion und für die Alarmverifikation von Bedeutung. Die dafür erforderliche optische und messtechnische Sensorik ist KI-gesteuert.

Rahmenbedingungen und Grenzen

Um eine möglichst umfassende Unterstützung durch KI zu planen und diese Planung effizient und kostengünstig umzusetzen, bedarf der SDL informationstechnischer Kompetenz. Dazu muss er in aller Regel ein auf KI spezialisiertes IT-Sicherheitsunternehmen hinzuziehen. KI ist anfällig gegenüber kriminellen Angriffen mit dem Ziel der Manipulation von Daten oder des Diebstahls geistigen Eigentums. Das BSI hat in dem Leitfaden „sicherer, robuster und nachvollziehbarer Einsatz von KI" 2021 Entwicklern und Nutzern eine Reihe von spezifischen Abwehrmaßnahmen empfohlen: eine Analyse des gesamten „Lebenszyklus" des KI-Systems hinsichtlich relevanter Risiken und die Robustheit des Systems durch „Trainingsangriffe" zu stärken; die verwendeten Metriken gegen zufällige oder gezielte Änderungen zu sichern; für Trainings- wie Testdaten ein professionelles Datenmanagement einzuführen und sie vor Manipulationen zu schützen; Anfragen an und Zugriffe auf das KI-System zu protokollieren und die Protokolle auf Anomalien zu prüfen; die korrekte Funktionsweise des KI-Systems regelmäßig zu überprüfen. Und das Fraunhofer-Institut für kognitive Systeme empfiehlt eine erweiterte Softwarearchitektur, die die KI überwacht und die getroffenen Entscheidungen auf Plausibilität überprüft sowie der KI durch den Ansatz eines „dynamischen Safety-Managements" mehr Freiraum zu geben als durch klassische Safety-Ansätze, die immer vom Worst-Case-Szenario ausgehen. Am 19. Juli 2023 hat das DIN einen neuen Standard zur Förderung der Erklärbarkeit von KI veröffentlicht. Der neue Standard DIN SPED 92001-3 soll helfen, das Vertrauen in die Nutzung und die Sicherheit durch Erklärbarkeit von KI zu stärken. Prof. Norbert Pohlmann, Institut für Internet-Sicherheit, erläutert in GIT Sicherheit, 5/2023, S. 62 f., das Forschungsprojekt vertrauenswürdige Plattform für KI-Lösungen und Datenräume. Entwicklern von KI soll die Möglichkeit eröffnet werden, sowohl die Vertrauenswürdigkeit ihres Unternehmens als auch die ihrer KI-Lösungen und Datenräume im Rahmen einer Agenda zu dokumentieren. Am 2. Februar 2023 hat das BSI das Projekt 464 „Security of AI-Systems-Fundamentals" vorgestellt, das den Stand der Forschung im Bereich der Sicherheit von KI-Systemen erfasst.

Die Ergebnisse eines Workshops zum aktuellen Stand der Prüfbarkeit von KI-Systemen in sicherheitskritischen Bereichen hat das BSI in einem Whitepaper zusammengefasst. Und es hat einen „AI Cloud Service Compliance Criteria Catalogue" erstellt. Grenzen für den Einsatz von KI ergeben sich vor allem aus Datenschutz und dem Diskriminierungsverbot. Dabei wird oft übersehen, dass personenbezogene Daten nach ihrer Anonymisierung keinem Datenschutz unterliegen. Im April 2021 hat die EU-Kommission den Entwurf einer Verordnung veröffentlicht, deren Ziel es ist, einen umfassenden einheitlichen Rechtsrahmen für die Entwicklung und Anwendung von KI in den Mitgliedstaaten zu schaffen. Sie verfolgt dabei einen risikobasierten Ansatz und legt einen einheitlichen horizontalen Rechtsrahmen mit acht Anwendungsbereichen fest. Die Ausschüsse des EU-Parlaments für Binnenmarkt und für bürgerliche Freiheiten haben am 11. Mai 2023 Änderungsanträge zum Entwurf der Kommission beschlossen. Dem Beschluss ist das Plenum am 14. Juni 2023 gefolgt. Nach diesem Beschluss sollen KI-Systeme, die ein unakzeptables Risiko für die Sicherheit von Menschen darstellen (manipulative Techniken, Ausnutzung der Schwachstellen von Menschen, Social Scoring) streng verboten werden. Die Hochrisikoanwendungen sollen um die Bereiche Gesundheit, Sicherheit, Grundrechte und Umwelt erweitert werden. Anbieter von Foundation-Modellen müssen Risiken bewerten und abmildern, Auslegungs-, Informations- und Umweltanforderungen einhalten und sich in der EU-Datenbank registrieren lassen. Generative Foundation-Modelle müssen die Generierung durch KI offenlegen. Es wird spannend, zu welchem Ergebnis der nun anstehende Trilog zwischen EU-Kommission, Parlament und Rat führen wird. Bis zum Jahresende soll eine Einigung gefunden werden. Für den Einsatz von KI-Tools bei Kundenaufträgen sollte zur Vermeidung rechtlicher Konflikte eine Regelung der Nutzung von KI in Verträgen und den AGB erfolgen (Thomas Schwenke, LL.M in AssCompact am 19. Juli 2023). Das Leistungsniveau der KI wird weiter zunehmen, in immer kürzeren Innovationszyklen. Die rasante Entwicklung von generativen Text- und Bildverarbeitungssystemen, mit denen die amerikanischen Big-Tech-Konzerne aktuell gegenseitig konkurrieren, zeigt dies in eindrucksvoller Weise. Gleichwohl wird KI die menschliche Intelligenz, die gänzlich anders strukturiert ist als KI, die systemfremde Umstände und das Weltwissen, Intuition und Kreativität in Entscheidungsprozesse einbringt, entgegen allen Warnhinweisen einiger Wissenschaftler nie ersetzen können. Der BDSW wird sicher überlegen, inwieweit er künftig – in Kooperation mit relevanten Fachverbänden wie Bitkom und dem Bundesverband künstliche Intelligenz – die IT-Sicherheit und KI-Anwendungen in der Sicherheitswirtschaft verstärkt in den Blick nehmen und fördern kann.

Lünendonk-Liste: Die 25 führenden Sicherheitsdienstleister wachsen 2022 um 10,5 Prozent

Die 25 führenden Sicherheitsdienstleister in Deutschland wachsen im Jahr 2022 um 10,5 Prozent. Das ist eine Steigerung um 4,2 Prozentpunkte gegenüber dem Vorjahr (2021: +6,3 %). Die Anzahl der Beschäftigten steigt 2022 im Mittel um 3,5 Prozent verglichen mit 2021. Die Branche für Sicherheitsdienstleistungen setzt damit ihren Wachstumskurs nach der Coronapandemie weiter fort – auch ohne Berücksichtigung des Preiseffekts. Für die kommenden Jahre prognostizieren die 25 führenden Anbieter ein Plus vom 5,7 bis 7,6 Prozent pro Jahr.

LÜNENDONK

www.luenendonk.de

Die Unternehmen blicken angesichts der hohen Nachfrage nach privaten Sicherheitsdienstleistungen optimistisch in die Zukunft. Insbesondere das anhaltende Interesse an Sicherheitstechnik und die damit verbundenen Services lassen die für die Lünendonk-Studie analysierten Unternehmen positiv auf die kommenden Jahre blicken.

Das Ranking im Detail

Der Marktführer Securitas erreicht erstmals einen Jahresumsatz von mehr als 1 Mrd. Euro. Mit einer Leistung von 1.035 Mio. Euro wurde ein Plus von 86 Mio. Euro bilanziert. Allein der Zuwachs ist das 2,4-Fache des Jahresumsatzes der auf Rang 25 platzierten IWS aus Aschaffenburg (36 Mio. Euro).

Auf Rang zwei folgt mit 479 Mio. Euro Sicherheitsumsatz KÖTTER aus Essen, die 21 Mio. Euro mehr erlöst als die auf Rang drei folgende Kieler Wach- und Sicherheitsgesellschaft (458 Mio. Euro). Zu der Firmengruppe gehören Schwestergesellschaften, wie unter anderem die Sicherheit Nord. Die drei führenden Dienstleister beschäftigen als einzige Unternehmen jeweils mehr als 10.000 Menschen.

Die Niedersächsische Wach- und Schliessgesellschaft auf Rang vier erwirtschaftet inklusive der VSU einen Jahresumsatz von 340 Mio. Euro, gefolgt von Pond Security Service aus Erlensee bei Hanau in Hessen (309 Mio. Euro). Somit befinden sich 2022 erstmals alle Top-5-Unternehmen über der 300-Millionen-Euro-Umsatzschwelle.

Auf den Rängen sechs und sieben folgen ebenfalls unverändert die beiden Sicherheits-Sparten der Facility-Service-Multidienstleister WISAG und Klüh mit 242,6 Mio. Euro respektive 169 Mio. Euro. Die nachfolgenden W.I.S. und Stölting verzeichnen jeweils leichte Umsatzsteigerungen bei leicht reduzierter Belegschaft. Stölting hat zuletzt die RF Sicherheit übernommen.

Komplettiert werden die Top 10 von Piepenbrock, die den Umsatz unter anderem dank eines Großauftrags zur Luftsicherheitskontrolle am Flughafen Düsseldorf von 91 auf 127 Mio. Euro steigern konnten. Piepenbrock verbessert sich damit um einen Rang gegenüber dem Vorjahr.

Gegenbauer agiert künftig als Apleona am Markt

Die Gegenbauer Sicherheitsdienste, die seit dem vollzogenen Zusammenschluss mit dem Facility-Service-Multidienstleister Apleona unter dem Namen Apleona am Markt agieren, wachsen um 21 Prozent und verbessern sich

Bild: # 1271666444 / istockphoto.com

damit von Listenrang 14 auf elf. Nahezu gleichauf liegt die Berliner Dussmann Group mit einem Sicherheitsumsatz von 99,3 Mio. Euro auf Rang zwölf.

Ebenfalls nahe beieinander liegen die Nürnberger Wach- und Schließgesellschaft mit 88,7 Mio. Euro Umsatz und die big-Gruppe aus Karlsruhe mit 88,1 Mio. Euro. Mit drei Millionen Euro weniger (85,1 Mio. Euro) folgt die Berliner Ardor Group auf Rang 15. Ardor verzeichnet mit einem Umsatzplus von 20,5 Prozent das viertgrößte Wachstum aller 25 Listenunternehmen.

Auf den weiteren Rängen sticht die ESD Sicherheitsdienste mit Hauptsitz in Mühldorf am Inn östlich von München, unter anderem aufgrund der Übernahme der ExSiRo, mit einem Zuwachs von 24 Prozent auf 64,1 Mio. Euro hervor. Die ehemalige GSE Protect firmiert nun als ICTS Protect Germany und erreicht einen Umsatz von 60,3 Mio. Euro und Listenrang 23. Komplettiert wird das Ranking durch die Vollmergruppe auf Rang 24 mit 43,3 Mio. Euro und die IWS aus Aschaffenburg auf Platz 25 mit 36 Mio. Euro.

Lünendonk-Partner und Studienautor Thomas Ball ordnet die Ergebnisse ein: „Unsere neue Liste zeigt ganz klar, dass die Sicherheitsdienstleister durch die große Nachfrage auch ein starkes Umsatzwachstum realisieren. Gleichzeitig steigt die Zahl der Beschäftigten durchschnittlich um 3,5 Prozent, obwohl Lohneffekte deutlich größer als in den vergangenen Jahren ausfielen. Die Liste unterstreicht damit erneut die Bedeutung der Branche für die deutsche Wirtschaft."

Bezug

Die Lünendonk-Liste 2023 „Führende Sicherheitsdienstleister in Deutschland" steht ab sofort unter **https:www.luenendonk.de/produkte/listen/luenendonk-liste-2023-fuehrende-sicherheitsdienstleister-in-deutschland/** zum kostenfreien Download bereit. Die vollständige Marktstudie erscheint voraussichtlich im September, basiert auf einer Analyse von 47 führenden Sicherheitsdienstleistern und wird kostenfrei verfügbar sein. Die Marktstudie enthält regionale Auswertungen, zahlreiche Marktstrukturdaten sowie Einschätzungen zu aktuellen Themen und Trends. Die Studie wird ermöglicht durch die Studienpartner Apleona, Bayern Corporate Services, SecMarket, Stölting und WISAG Sicherheit & Service.

Zutrittsmanagement für KRITIS-Betreiber

Von Rainer Sander

Integrieren Betreiber Kritischer Infrastrukturen (KRITIS) moderne Zutrittskontrollen, erhöhen sie ihre physische Resilienz essenziell. Ein wichtiges Kriterium im kommenden KRITIS-Dachgesetz.

Die neue europäische NIS2-Richtlinie (Richtlinie zur Netz- und Informationssicherheit 2), die sich speziell an Unternehmen richtet, die in Deutschland und in Europa Kritische Infrastruktur betreiben, nimmt durch den seit Frühling 2023 vorliegenden Referentenentwurf des Bundesministeriums des Inneren, für Bau und Heimat für das sogenannte „NIS2UmsuCG" (NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) immer schneller Fahrt auf. Verantwortliche wie Geschäftsführer sollten nun aufgrund des näher rückenden Zeitpunktes, zu dem die NIS2-Richtlinie in nationales Recht überführt werden muss (Stichtag: 17. Oktober 2024), sowie der daraus resultierenden teilweisen persönlichen Haftung für die Umsetzung der Sicherheitsmaßnahmen in ihrer Einrichtung mit der Planung selbiger beginnen. Dies dient auch dazu, den teilweise drastischen Sanktionen zuvorzukommen, die je nach Einrichtung bis zu 20 Mio. Euro betragen können und die bei „nach § 28 (4) wichtigen" oder „nach § 28 (3) besonders wichtigen" Einrichtungen teilweise an den weltweiten Jahresumsatz des vergangenen Geschäftsjahres gekoppelt sind. Zutrittsmanagement ist eine essenzielle Maßnahme, um die physische Resilienz eines Betreibers im Sinne der NIS2-Richtlinie, des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) und des kommenden KRITIS-Dachgesetzes signifikant zu steigern und zu sichern.

Merkmale „integralen Zutrittsmanagements"

Ebenfalls betroffen sind die Betreiber „wichtiger" und „sehr wichtiger" Kritischer Infrastruktur durch das sich noch in Planung befindliche KRITIS-Dachgesetz. Dieses Gesetz bezieht sich auf die EU-CER-Richtlinie (EU 2022/2557), zu der

Rainer Sander

Leiter Integrale Zutrittsmanagementlösungen bei der Comelit Group S.p.A. Deutschland (https://comelitgroup.com/de-de/)

Die Erstveröffentlichung des Beitrags erfolgte in der Spezialausgabe Zutrittskontrolle 2023 der Zeitschrift PROTECTOR.
www.protector.de

Wir bedanken uns für die Abdruckgenehmigung.

Bild: # 701055376 / istockphoto.com

das Innenministerium Ende 2022 ein Eckpunktepapier vorgelegt hat. Das Eckpunktepapier geht sogar über die Richtlinie hinaus und diskutiert unter anderem verpflichtende Schutzstandards für die physische Sicherheit, wie zum Beispiel Personenvereinzelungsanlagen, Zäune und Zutrittsmanagementlösungen.

Wer sollte nun eine integrale Zutrittsmanagementlösung planen und realisieren? Von der bevorstehenden Notwendigkeit, sichere und angemessene Zutrittsmanagementlösungen anzuschaffen, sind alle KRITIS-Betreiber in Deutschland und Europa betroffen. Hierzu gehören Organisationen oder Einrichtungen, die eine bedeutende Rolle für das staatliche Gemeinwesen spielen und deren Ausfall oder Beeinträchtigung zu nachhaltigen Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen gravierenden Folgen führen würde. Dazu zählen beispielsweise Bedarfsträger wie Polizei und Feuerwehr, aber auch Verkehr, Energienetzbetreiber, Wasserversorgung, Gesundheitswesen, digitale Infrastruktur und weitere, die in Deutschland in acht verschiedene Sektoren unterteilt sind. Die Anforderung gilt auch für „nach § 28 (4) wichtige“ oder „nach § 28 (3) besonders wichtige“ Einrichtungen wie mittelgroße Unternehmen und Großunternehmen in den Bereichen digitale Infrastruktur, Bankwesen, Finanzmärkte, Gesundheitswesen, Energie, Transport und Verkehr, Abwasser und andere.

Was kennzeichnet nun ein „integrales Zutrittsmanagement“ für KRITIS-Betreiber? Der erste Begriff ist „Zutrittsmanagement“, der am besten durch die „4 W-Fragen“ charakterisiert werden kann. Das bedeutet, dass man festlegt, welche Person (WER) durch welche Tür (WO) zu welcher Zeit (WANN) unter welchen Bedingungen (WIE) einen bestimmten Bereich betreten darf.

„Von der bevorstehenden Notwendigkeit, sichere und angemessene Zutrittsmanagementlösungen anzuschaffen, sind alle KRITIS-Betreiber in Deutschland und Europa betroffen.“

Der zweite Begriff, „integral“, bedeutet in diesem Kontext, dass ein ganzheitlicher und umfassender Ansatz für das Zutrittsmanagement gewählt wird. Es reicht nicht aus, lediglich einen Zutrittsleser neben der Tür zu installieren und zu glauben, dass man als Verantwortlicher eines

KRITIS-Betriebs seiner sicherheitstechnischen Sorgfaltspflicht nachkommt. Es ist vielmehr erforderlich, die Tür beispielsweise durch einen Riegel-Fallenkontakt auf Öffnung, offenes Stehen oder Aufbruch zu überwachen. Es ist auch wichtig, den Verriegelungsstatus der Tür sensorisch zu überwachen. Ein integraler Ansatz bedeutet beispielsweise, dass im Falle eines gewaltsamen Türaufbruchs eine Alarmmeldung an einen taktischen Leitstand weitergeleitet wird, um beispielsweise Werksschutz oder Wachpersonal mit automatisch bereitgestellten Videobildern beziehungsweise Streams ein klares Lagebild zu vermitteln.

Schutzbedarfsanalyse und Auswahl der richtigen Partner

Die Implementierung eines integralen Zutrittsmanagements, das die sicherheitstechnische Resilienz eines KRITIS-Betreibers normativ erhöht, stellt derzeit viele Betreiber vor diverse Herausforderungen.

Diese Herausforderungen beginnen bereits beim KRITIS-Betreiber selbst, dessen Führungsebene nun in der Verantwortung steht, falls dies noch nicht geschehen ist, interne Ansprechpartner und Teams zu benennen. Gemeinsam mit ausgewählten Herstellern, Lieferanten, Planern, Errichtern und Experten sollten sie nach einer umfassenden Schutzbedarfsanalyse die vorhandenen physischen Sicherheitslösungen im eigenen Bestand evaluieren. Dabei ist es wichtig, den Sicherheitsgrad und die Einsatzfähigkeit dieser Lösungen im Sinne der NIS2-

Vier grundlegende Elemente bilden das Herzstück eines integralen Zutrittsmanagementsystems, das speziell auf die Anforderungen von KRITIS-Betreibern abgestimmt ist. Bild: Comelit

Richtlinie und des kommenden KRITIS-Dachgesetzes zu bewerten.

Dieser Prozess erfolgt in enger Zusammenarbeit und wiederholter Abstimmung mit dem jeweiligen Bedrohungsbild und dem eigenen Schutzbedarf. Der KRITIS-Betreiber steht dabei oft vor der Herausforderung, den schwierigen Zielkonflikt zwischen Gesetzgebung und Sicherheitslage einerseits und den begrenzten finanziellen Ressourcen andererseits optimal zu bewältigen. Hierbei ist es für den Betreiber entscheidend, die richtigen Hersteller und erfahrenen Partner an seiner Seite zu haben, um gemeinsam die richtigen Prioritäten zu setzen und beispielsweise teure Teilgewerke zu vermeiden, die hohe Kosten verursachen, aber möglicherweise offene Angriffsvektoren ungesichert lassen.

Taktisches und technisches Besuchermanagement als Vorfilter

Das integrale Zutrittsmanagement beginnt bereits vor dem Betreten der KRITIS-Örtlichkeit. Hierbei spielt das taktische Besuchermanagement eine wichtige Rolle, indem es Personen im Voraus informiert und unerwünschten Besuchern den Zugang zur sensiblen Örtlichkeit des KRITIS-Betreibers verwehrt oder zusätzliche Sicherheitsvorkehrungen trifft. Hierfür stehen verschiedene Möglichkeiten zur Verfügung, wie zum Beispiel eine Vorabzuverlässigkeits- oder -sicherheitsüberprüfung.Besuchermanagementlösungen, die Teil des Zutrittsmanagements sind, dienen jedoch nicht nur der Vorabkontrolle von Besuchern. Sie unterstützen insbesondere auch während des Besuchs, zum Beispiel durch Evakuierungs- und Notfallmanagement, sowie nach dem Besuch, bei der Rückgabe oder Deaktivierung des Ausweisträgers und dem Sicherheits-Check-out.

Welche Elemente sind notwendig bei einem Zutrittsmanagementsystem für KRITIS-Betreiber und welche Normen sind hierbei sehr hilfreich? Ein integrales Zutrittsmanagementsystem für KRITIS-Betreiber besteht immer aus vier klassischen Zutrittselementen sowie mindestens vier oder mehr weiteren Randgewerken, die man sowohl einzeln als auch zusammen hinsichtlich Sicherheitsbedarf, Risikoklasse und Funktion bewerten sollte. Dazu zählen:

- die Identität einer Person (z. B. Karte, elektronischer Schlüsselanhänger, Biometrie),
- der Sensor (z. B. Zutrittsleser),
- die Logik (z. B. Zutrittskontroller und Software) und
- der Aktor (Vergleichsergebnis aus Nutzer und zugewiesenen Rechten wird umgesetzt z. B. durch Türöffnung).

Diese vier grundlegenden Elemente bilden das Herzstück eines integralen Zutrittsmanagementsystems, das speziell auf die Anforderungen von KRITIS-Betreibern abgestimmt ist. Weiterhin sind häufig die folgenden vier integrierten Randgewerke Teil eines umfassenden Zutrittsmanagementsystems für KRITIS-Betreiber: Interkom- und Videosicherheitslösung, Einbruchmeldetechnik, Besuchermanagement. Bei sehr großen Kunden sollte zudem eine entsprechende taktische

Managementoberfläche vorhanden sein, in die alle vorhandenen und neuen Subsysteme integriert werden können, einschließlich mehrerer verschiedener Zutrittslösungen.

Sehr hilfreich für KRITIS-Betreiber ist hierbei die DIN EN 60839-11, mittels derer eine Risikoermittlung vor der Beschaffung und Umsetzung eines Zutrittsmanagements durchgeführt werden kann. Mithilfe dieser Norm werden die Eintrittswahrscheinlichkeit eines Risikos und das potenzielle Schadensausmaß gegenübergestellt. Unternehmen und Organisationen werden dann in vier Risikograde eingeteilt, die den spezifischen Bedürfnissen und Anforderungen entsprechen.

KRITIS-Unternehmen fallen in der Regel mindestens in den Risikograd 3 oder sogar 4 (mittel bis hoch und hoch) gemäß DIN EN 60839-11-1. Bei einem hohen Risikograd wird ein sehr hohes Wissen beim potenziellen Angreifer vorausgesetzt, ebenso wie eine hohe Fertigkeit im Umgang mit der zu attackierenden Zutrittslösung sowie umfassendes Wissen über Erkennungsmethoden und IT-Technologien.

Identität als besonders zu schützender Angriffsvektor bei Zutrittslösungen

Ein besonders zu schützender Angriffsvektor bei KRITIS-Betreibern betrifft die Identität einer Person oder eines Besuchers, wie unter Punkt 1 aufgeführt. Dies kann in Form einer Karte, eines elektronischen Schlüsselanhängers oder eines biometrischen Merkmals erfolgen. Es ist von entscheidender Bedeutung, eine moderne ID-Technologie mit einer hohen Standardverschlüsselung einzusetzen, beispielsweise Mifare Desfire EV2 oder höher mit einer mindestens AES 128-Bit-Standard-IT-Verschlüsselung. Dadurch wird vermieden, dass die ID-Zutrittskarte innerhalb weniger Sekunden geklont werden kann. Für biometrische Merkmale gilt dasselbe, wobei auch eine hochsichere und erweiterte Sensorik zum Einsatz kommen sollte, wie beispielsweise Lebenderkennung, Fake-Detektionssensorik und KI-Technologie.

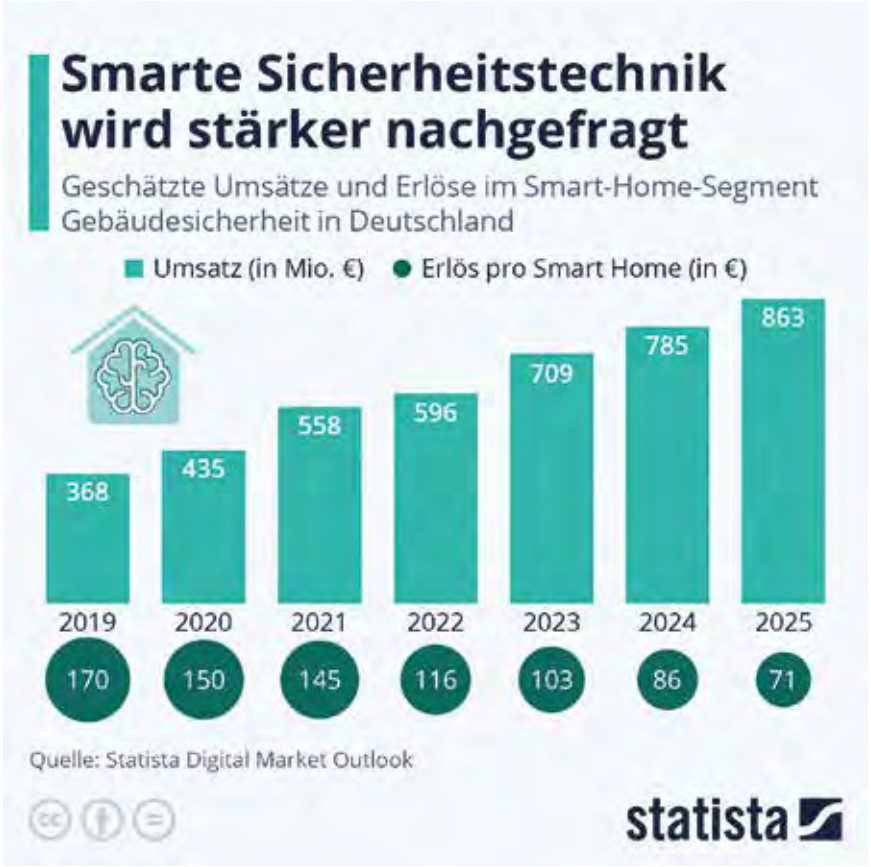
In der Praxis verwenden jedoch einige KRITIS-Betreiber noch immer leicht klonbare Karten- und Biometrietechnologien, wie zum Beispiel Legic Prime, Mifare Classic oder einfach klonbare Fingerabdrucktechniken. Dies stellt ein fahrlässiges Risiko dar und sollte schnellstmöglich durch sichere Technologien ersetzt werden. Häufig möchten Kunden die ID-Zutrittskarte auch als Lichtbildausweis oder zur Zeiterfassung verwenden, wie es bereits bei einigen Bedarfsträgern in Deutschland der Fall ist. Dabei entsteht jedoch eine Kollision zwischen dem Komfort, nur ein Medium zu haben, und der erforderlichen Trennung betrieblicher und sicherheitstechnischer Aspekte, wie es auch in der DIN ISO 27001 definiert ist. Gerade KRITIS-Betreiber sollten besonderes Augenmerk auf diese Trennung legen. Es ist keinesfalls empfehlenswert, die Zutrittskarte gleichzeitig als Lichtbildausweis zu nutzen, um Angreifern keinerlei Anhaltspunkte zu geben, wo der gefundene Ausweis verwendet werden könnte. Auch bei der hybriden Verwendung als Zutrittskarte und Zeiterfassungskarte

ist aus unserer Sicht eine Trennung von sicherheitstechnischen und betrieblichen Aspekten notwendig, selbst wenn dies mit gewissen Komforteinschränkungen einhergeht. Solche Überlegungen spielen auch eine wichtige Rolle bei der Integration des Datenschutzes in das aktuelle IT-Grundschutz-Kompendium des BSI (Bundesamt für Sicherheit in der Informationstechnik) und dienen als wichtige Entscheidungsgrundlage.

Herausforderungen für KRITIS- und Non-KRITIS-Betreiber

Sicherheit war schon immer mehr als nur eine einzelne technische Lösung. Sie erfordert stets einen ganzheitlichen, integralen Ansatz, um die definierten Schutzziele zu erreichen. Dabei ist es besonders wichtig, im Vorfeld die richtigen Partner auszuwählen, die über das erforderliche Wissen und die Erfahrung, insbesondere im Bereich der relevanten Normen, verfügen. Bei Comelit begleiten wir KRITIS-Betreiber seit Jahren in Zusammenarbeit mit Ingenieurbüros, Planern, Sicherheitserrichtern, Partnerunternehmen und anderen Herstellern ganzheitlich. Als Hersteller von NDAA- und GDPR-konformen Videosicherheitssystemen, integralen Zutrittsmanagementlösungen und hochsicherer Interkomtechnik verfolgt Comelit einen ganzheitlichen Ansatz. Unser Ziel ist es, bei Kunden eine Vielzahl von verschiedenen isolierten Technologien in wenige, hochsichere integrale Lösungen zusammenzuführen, die den Schutzzielen des Kunden gerecht werden. Seit Ende letzten Jahres sind wir auch aktiv als Mitglied im BHE (Bundesverband Sicherheitstechnik) und im VfS (Verband für Sicherheitstechnik).

> „Häufig möchten Kunden die ID-Zutrittskarte auch als Lichtbildausweis oder zur Zeiterfassung verwenden. Dabei entsteht jedoch eine Kollision zwischen dem Komfort und der erforderlichen Trennung betrieblicher und sicherheitstechnischer Aspekte."



Wer organisiert die Passagier- und Handgepäckkontrolle?

Luftfahrt aktuell 2/2023 – Fakten und Hintergründe zum deutschen Luftverkehr

Herausgegeben vom Bundesverband der Deutschen Luftverkehrswirtschaft e. V. (BDL)
www.bdl.aero

Vor jedem Abflug gilt für Fluggäste und ihr Handgepäck: Luftsicherheitskontrolle passieren. Dabei werden die Passagiere und das Gepäck auf Sprengstoff und andere gefährliche Gegenstände hin überprüft. Das ist wichtig für die Sicherheit aller am Flughafen und im Flugzeug. Wie ist die Passagier- und Handgepäckkontrolle in Deutschland eigentlich geregelt? Wer ist an welchem Flughafen zuständig?

Sicherheit hat im Luftverkehr höchste Priorität. Die Passagier- und Handgepäckkontrolle dient dem Schutz vor Angriffen auf die Sicherheit des zivilen Luftverkehrs und obliegt daher dem Staat. Unter Berücksichtigung des europäischen Rechtsrahmens und internationaler Standards und Empfehlungen, sind in Deutschland die Befugnisse und Maßnahmen, die zur Durchführung der Passagier- und Handgepäckkontrolle sowie der Kontrolle aufgegebener Gepäckstücke notwendig sind, im Wesentlichen in § 5 des Luftsicherheitsgesetzes (LuftSiG) geregelt. Deshalb wird auch häufig von „§ 5-Kontrollen" gesprochen.

Bei der Passagier- und Handgepäckkontrolle handelt es sich um eine Sicherheitsmaßnahme, die bundeseinheitlich durchgeführt werden muss. Grundsätzlich ist das Bundesinnenministerium (BMI) zuständig. Das BMI hat für viele Flughafenstandorte die Verantwortung für die Durchführung der Luftsicherheitskontrollen der Bundespolizei übertragen, die diese mithilfe von privaten Sicherheitsdienstleistern durchführt. Am Standort Frankfurt hat das BMI die Durchführungsverantwortung zum 1. Januar 2023 dem Flughafenbetreiber Fraport übertragen. Und in Bayern hat die Bayerische Staatsregierung die Verantwortung für die Luftsicherheitskontrollen selbst mit ihrer Landesluftsicherheitsbehörde übernommen. An den übrigen, kleineren Standorten sind die Luftsicherheitsbehörden der Länder verantwortlich für die Luftsicherheitskontrollen.

Anforderungen an alle Sicherheitskontrollen an deutschen Flughäfen

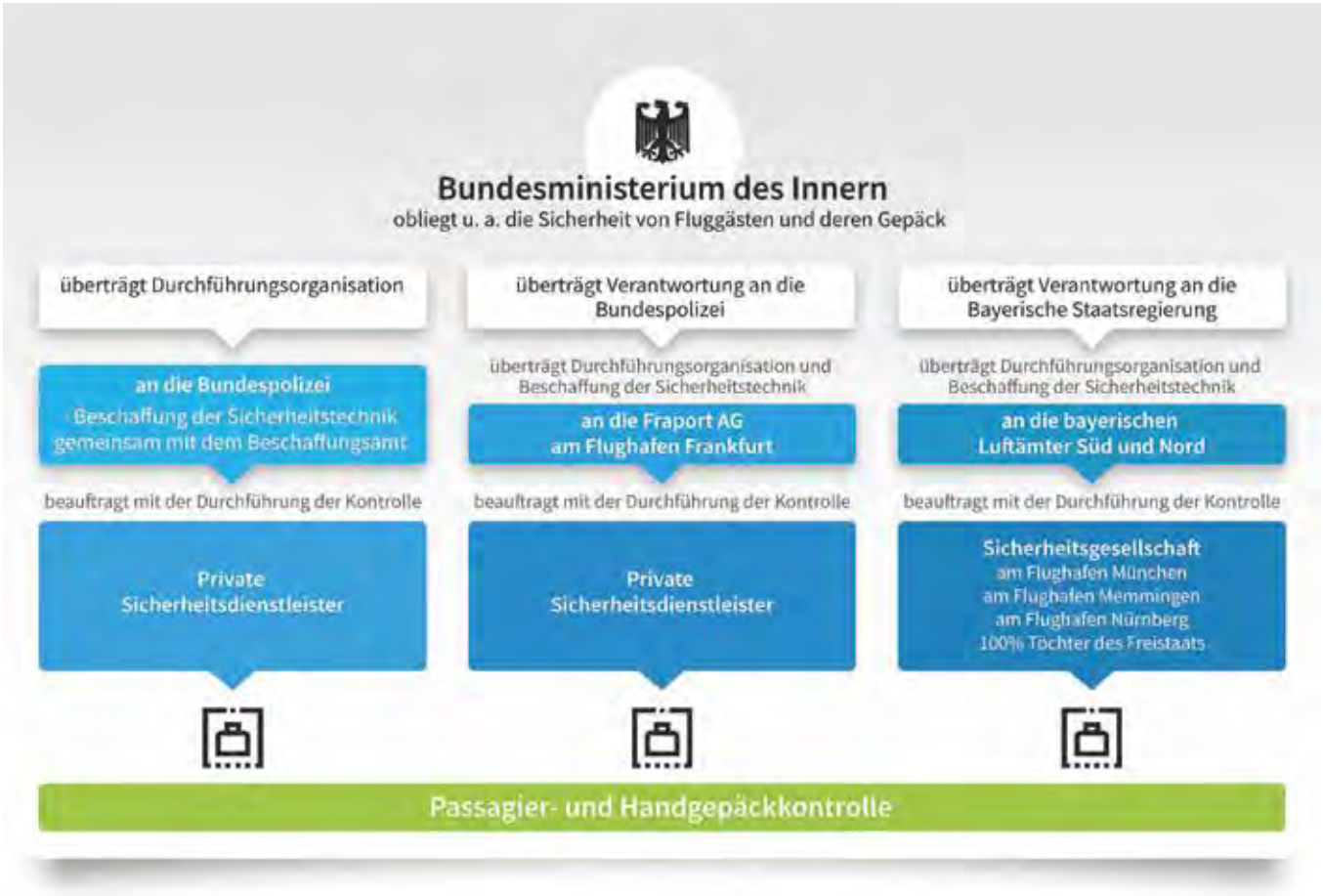
Unabhängig davon, wer letztlich die Durchführungsorganisation der Luftsicherheitskontrolle (Siko) übernimmt, gelten überall die gleichen Vorschriften und Anforderungen. Gesetzlich einheitlich geregelt sind der Ablauf der Passagier- und Handgepäckkontrolle, die Qualifikation der Arbeitskräfte, die die Kontrolle durchführen, und die Anforderungen an die notwendige Kontrolltechnik. Auch der Schutz der Passagiere an der Siko ist eine bundeseinheitliche Anforderung; für diesen ist die Polizei an allen Standorten zuständig. Daher sind an allen Kontrollen immer auch bewaffnete oder bewaffnete Polizeibeamte anzutreffen.

- **Bundesweit einheitliche Anforderungen an das Personal –** Die Arbeitskräfte, die die Siko durchführen, müssen die bundeseinheitlich geregelten Abläufe an der Passagier- und Handgepäckkontrolle kennen und daher bestimmte Qualifikationen erfüllen. Diese sind durch BMI-Erlasse geregelt und gelten bundesweit. Darüber hinaus müssen alle Bewerber eine behördliche Zuverlässigkeitsüberprüfung (ZÜP) durchlaufen.
- **Bundesweit einheitliche Anforderungen an die Sicherheitstechnik –** Die technischen Geräte, die bei der Siko zum Einsatz kommen, müssen bestimmte Kriterien erfüllen und zugelassen sein. Welche das sind, bestimmt die EU-Kommission und für Deutschland zusätzlich eine Zertifizierungsstelle, die bei der Bundespolizei angesiedelt ist. Sie prüft die Technik, die zum Einsatz kommt, und entscheidet über ihre Zulassung. Nur Kontrolltechnik, die von der Zertifizierungsstelle zugelassen wurde, darf an den Flughäfen in Deutschland eingesetzt werden.

Die Flughäfen selbst stellen an allen Standorten die Fläche zur Verfügung, die für die Siko benötigt wird.

Organisation und Durchführung durch die Bundespolizei

An Flughäfen, an denen die Bundespolizei die Verantwortung für die Sicherheitskontrollen hat, lässt sie diese durch beauftragte private Sicher-



heitsdienstleister durchführen. Die Bundespolizei entscheidet auch, wie die Kontrollspuren technisch ausgestattet werden. Beschaffungsamt und Bundespolizei legen ebenfalls über ein Ausschreibungsverfahren fest, welche externen Sicherheitsdienstleister mit der Durchführung der Kontrolle betraut werden. Die Verantwortung für die sichere und effiziente Durchführung der Kontrollen trägt an diesen Standorten die Bundespolizei.

Organisation und Durchführung in Bayern

Neben einigen wenigen anderen Bundesländern hat sich das Land Bayern entschieden, die Siko selbst zu organisieren. Bayern hat unter der Fachaufsicht des Bayerischen Verkehrsministeriums (StMB) die Zuständigkeit für die Siko an die nachgeordneten Landesluftsicherheitsbehörden übertragen: das Luftamt Südbayern für die Flughäfen München und Memmingen sowie das Luftamt Nordbayern für den Flughafen Nürnberg. Die konkrete Kontrolle wird in Bayern von Beschäftigten von Sicherheitsgesellschaften durchgeführt, die 100-prozentige Tochterunternehmen des Freistaates sind – an jedem Flughafen mit einer eigenen Sicherheitsgesellschaft. Am Münchner Flughafen bspw. nennt sie sich „Sicherheitsgesellschaft am Flughafen München mbH" (SGM). Über die Prozesse an den Sikos und die eingesetzte Kontrolltechnik entscheidet das StMB gemeinsam mit dem Luftamt; zur operativen Steuerung gibt es regelmäßige und enge Abstimmungen zwischen StMB, Luftamt, Sicherheitsgesellschaften und Flughafenbetreiber. Die Verantwortung für die sichere und effiziente Durchführung der Kontrollen trägt an diesen Standorten jeweils die bayerische Behörde.

Organisation und Durchführung am Flughafen in Frankfurt

Seit 1. Januar 2023 verantwortet Fraport am Flughafen Frankfurt die Organisation, Steuerung und Durchführung der rund 170 Luftsicherheitskontrollen. In der Verantwortung der Bundespolizei bleiben die gesetzliche Rechts- und Fachaufsicht und die Gewährleistungsverantwortung für die Luftsicherheit, der bewaffnete Schutz der Kontrollstellen, die Zertifizierung und Zulassung von neuer Kontrollinfrastruktur sowie die Zertifizierung und Rezertifizierung der Luftsicherheitsassistenten. Zeitgleich begannen private Sicherheitsunternehmen im Auftrag der Fraport AG mit der Durchführung der Passagierkontrollen am Flughafen Frankfurt. Im Zuge der Steuerungsübernahme setzt Fraport zudem CT-Geräte in der Passagiersicherheitskontrolle ein. Bis zum Frühjahr 2024 werden 40 CT-Geräte am Frankfurter Flughafen im Einsatz sein.

„Die Sicherung des Bargeldkreislaufes ist eine Gemeinschaftsaufgabe“

Im Gespräch mit Michael Mewes

Michael Mewes

Dipl.-Wirtsch.-Ing., ist seit 2004 im Vorstand der Cash Logistik Security. Er besitzt eine ausgewiesene Expertise in der Geld- und Wertbranche und ist im Vorstand des Branchenverbandes BDGW seit 2008. Sein Arbeitsfokus: Administration, Efficiency Management und Prozessoptimierung.

Die Erstveröffentlichung des Beitrags erfolgte am 15. Mai 2023 unter www.geldinstitute.de.

Wir bedanken uns für die Abdruckgenehmigung.

Michael Mewes ist ein Experte aus der Geld- und Wertbranche und im Vorstand bei Cash Logistik Security. Im Interview spricht er über die Notwendigkeit einer funktionierenden Bargeldversorgung, die aktuellen Probleme dabei und wie eine Zusammenarbeit mit Banken besser funktionieren könnte.

Geld- und Wertdienstleister haben eine zentrale Funktion im Bargeldkreislauf. Sie stellen den Schutz der physischen Transporte zwischen Bundesbank, Kreditinstituten und Handel sicher. Es liegt also im ureigensten Interesse der Geld- und Wertdienstleister, sich auf Not- und Krisenfälle ausreichend und angemessen vorzubereiten. Was ist hier der Status quo in Deutschland?

Michael Mewes: Ohne den Einsatz der Wertdienstleister käme der Bargeldkreislauf in Deutschland zum Erliegen und die Versorgung der Bevölkerung mit Bargeld wäre nicht möglich. Diese wichtige Rolle der Wertdienstleister hat dazu geführt, dass die Unternehmen grundsätzlich als Kritische Infrastruktur eingestuft worden sind und bei Erreichung definierter Grenzwerte der KRITIS-Verordnung unterliegen. Die Unternehmen sind damit auf Basis dieser Verordnung gesetzlich zu umfangreichen Maßnahmen verpflichtet, um ihre Arbeitsfähigkeit zu sichern.

Darüber hinaus gilt die Beauftragung von Wertdienstleistern durch die Kreditinstitute gemäß den Vorgaben der von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) herausgegebenen Mindestanforderungen an das Risikomanagement (MaRisk) als wesentliche Auslagerung. Damit gelten umfangreiche Vorgaben für die Dienstleistersteuerung und -überwachung und insbesondere müssen auch Regelungen für Not- und Krisenfälle mit den Wertdienstleistungsunternehmen vereinbart werden. Für größere Kreditinstitute gelten zudem noch die sehr umfangreichen Guidelines der European Banking Authority (EBA).

Und um dieses Vorgabenpaket noch abzurunden, sind die Mitgliedsunternehmen unserer Bundesvereinigung Deutscher Geld- und Wertdienste (BDGW) auf die Einhaltung der Regelungen des gemeinsam beschlossenen BDGW-Sicherheitsstandards verpflichtet, der den Unternehmen ebenfalls umfassende Vorsorgemaßnahmen für Not- und Krisenfälle vorgibt.

Alles in allem existieren also umfangreiche Regelungen, an denen sich die Wertdienstleister orientieren und die die Grundlage für die Notfallplanungen der Wertdienstleister bilden. Auf dieser Basis haben die Unternehmen unternehmensbezogene BCM-Konzepte entwickelt, die zudem durch kundenindividuelle Maßnahmenpapiere ergänzt werden.

Welche Stelle ist Ihrer Erfahrung nach die gefährdetste Stelle im Bargeldkreislauf?

Michael Mewes: Im Hinblick auf den Angriff krimineller Akteure ist der Bargeldkreislauf grundsätzlich an allen Stellen gefährdet, an denen Angriffe aussichtsreich erscheinen. Momentan liegt da ein deutlicher und öffentlichkeitswirksamer Schwerpunkt bei den Angriffen auf Geldausgabeautomaten, hier sind die Zahlen in den letzten Jahren bedauerlicherweise stark gestiegen. Es gibt umfangreiche Aktivitäten der Kreditinstitute, der zuständigen Innenministerien, der Polizei sowie weiterer Beteiligter, dieses Geschehen in den Griff zu bekommen.

Aber diese Taten sollten natürlich nicht den Blick verstellen auf das Gesamtgeschehen. Ausweislich der jährlichen Kriminalitätsstatistik (PKS) gab es im Jahr 2021 ca. 4.000 Raubtaten, die sich gegen Örtlichkeiten gerichtet haben, mit denen die Täter eine Beuteerwartung verbinden. Die allermeisten Taten (ca. 3.600) haben sich dabei gegen Kassenräume, Geschäfte, Tankstellen etc. gerichtet, auf Kreditinstitute, Poststellen usw. gab es ca. 160 Angriffe, 91 Angriffe richteten sich gegen unprofessionelle Geldtransporte und nur zwei gegen professionelle Wertdienstleister. Generell ist festzustellen, dass unsere Präventionsarbeit der letzten Jahre sehr erfolgreich war. Dies gilt übrigens auch für die Kreditinstitute, hier sind die Fallzahlen auch seit Jahren deutlich rückläufig.

Und für alle Leser, die als Fans unbarer Zahlungsmittel meinen, ohne Bargeld gäbe es keine Kriminalität, hält die PKS auch wichtige Informationen bereit. Es gab ca. 76.000 Diebstahlsfälle unbarer Zahlungsmittel und fast 65.000 Fälle von Betrug bzw. Computerbetrug mittels rechtswidrig erlangter unbarer Zahlungsmittel.

Im Hinblick auf Not- und Krisenfälle ist die Versorgung der Bevölkerung der kritischste Prozess im Bargeldkreislauf. Hierauf müssen alle Akteure ihr Hauptaugenmerk legen, um nach Möglichkeit jedem Bürger Zugang zu Bargeld zu ermöglichen. Denn in so einer Lage ist Bargeld das einzige resiliente Zahlungsmittel, mit dem tatsächlich auch gezahlt werden kann.

Was hat Ihrer Ansicht nach mehr zu einem Umdenken in Sachen Bargeldversorgung geführt? Corona oder die politische Situation in der Ukraine?

Michael Mewes: Schon in der Finanzkrise 2007 ff. hat sich gezeigt, dass Bargeld in Krisenzeiten für Bürger und Institutionen eine große Bedeutung hat. Die Nachfrage nach Bargeld ist seinerzeit weltweit sprunghaft angestiegen und die professionellen Bargeldakteure waren schwer beschäftigt, den Bargeldnachschub an allen Versorgungsstellen sicherzustellen. Ungeachtet der unberechtigten Angriffe auf das Bargeld während der Coronazeit ist die Nachfrage nach Bargeld zu Beginn dieser Krise ausweislich der Zahlen der Bundesbank sprunghaft um das Vierfache angestiegen. Der Angriffskrieg gegen die Ukraine hat dann erneut die Krisennachfrage nach Bargeld befeuert, und zwar zum einen durch die Nachfrage der Bürger und zum anderen durch die große Zahl an Flüchtlingen.

Tatsächlich wird viel von dem nachgefragten Bargeld nicht für den täglichen Konsum, sondern eher aus Vorsorgegründen beschafft. Aber wie richtig die Menschen mit diesem Bedürfnis nach Sicherheit liegen, haben wir im letzten Jahr beim Ausfall Tausender Zahlungsterminals in Deutschland gesehen. Die Bargeldzahlungen haben sich im Handel spontan verdoppelt, weil der Ausfall der Terminals durch Bargeldzahlungen kompensiert wurde. Ein großer Teil dieser Gelder kam offensichtlich aus den Bargeldreserven der Menschen, da die Nachfrage an den Geldautomaten nicht im gleichen Umfang gestiegen ist.

Die Bedeutung von Bargeld ganz besonders auch in Not- und Krisenzeiten ist vielfach belegt. Die Akteure im Bargeldkreislauf – allen voran die Deutsche Bundesbank – sind sich dieser Tatsache sehr bewusst. Sie arbeiten kooperativ und intensiv daran, den Bargeldkreislauf krisenfest zu erhalten und auch in Zeiten zurückgehender Bargeldnutzung die Verfügbarkeit und Nutzbarkeit von Bargeld zu sichern.

Ein neues Sicherheitsrahmenkonzept soll den Bargeldakteuren, insbesondere den Geld- und Wertdienstleistern, ermöglichen, auf Sicherheitsszenarien mit den entsprechenden Konsequenzen zu reagieren und bereits vorhandene Krisenkonzepte anpassen zu können. Worauf legt das Sicherheitsrahmenkonzept besonderen Wert? Was sollten Banken hier wissen?

Michael Mewes: Ein wichtiges Ergebnis der Studie ist, dass nicht jeder Akteur für sich allein denken muss und darf, sondern dass wir die Aufgabe der Sicherung des Bargeldkreislaufes als Gemeinschaftsaufgabe und ganzheitlich begreifen müssen. Dazu bietet die Studie viele Arbeitshilfen, um die individuelle Situation der eigenen Institution zu bewerten und die Schnittstellen zu anderen Akteuren in den Blick zu nehmen. Krisenvorsorge ist eine mühsame und zunächst nicht besonders fruchtbare Aktivität, erst im Fall der Fälle zeigt sich die Qualität der Vorbereitung.

Aber es geht auch nicht nur darum, im Krisenfall die Arbeitsfähigkeit zu sichern, indem man beispielsweise die Themen Kommunikation und Formularwesen vorgedacht hat. Es geht vielmehr auch darum, bei der generellen Geschäftsplanung die Bargeldinfrastruktur zu sichern und die eigene wie die übergreifende Ver- und Entsorgungslage im Tätigkeitsgebiet für das Alltagsgeschäft und für die Krisenlage handlungsfähig zu halten.

Bargeld ist das einzige resiliente Zahlungsmittel, aber ohne eine ausreichende und resiliente Bargeldinfrastruktur hilft uns diese Tatsache nicht weiter. Dies müssen alle Akteure verstehen und darauf hat ja auch die Bundesbank aktuell mahnend hingewiesen.

„Leider entsteht gelegentlich der Eindruck, dass Bargeld von Kreditinstituten nicht geschätzt und alles ‚auf die Karte' gesetzt wird. Aber diese Entwicklungen sind falsch und gefährlich, wie sich in der Praxis vielfach gezeigt hat." (Michael Mewes)

Was erwarten Sie künftig von den Banken? Wo hätten Sie mehr Unterstützung?

Michael Mewes: Leider entsteht gelegentlich der Eindruck, dass Bargeld von Kreditinstituten nicht geschätzt und alles ‚auf die Karte' gesetzt wird. Aber diese Entwicklungen sind falsch und gefährlich, wie sich in der Praxis vielfach gezeigt hat. Dabei plädieren wir nicht für einseitige Festlegungen bzw. Präferenzen. Wir benötigen als Menschen vielmehr auch zukünftig einen Mix aus Zahlungsmitteln und dabei haben sowohl bare als auch unbare Zahlungsmittel ihren Platz. Wir werben bei den Kreditinstituten für eine entsprechende Grundhaltung.

Als Wertdienstleister erwarten wir eine konstruktive Zusammenarbeit bei den genannten Themen. Wichtig ist dabei auch ein gleichlautender Auftritt bei den Gesetzgebern mit der Forderung, in dem neuen KRITIS-Dachgesetz nicht nur Verpflichtungen zu normieren, sondern auch die Rechte der KRITIS-Betreiber zu stärken. So ist es beispielsweise von besonderer Bedeutung, für unsere Fahrzeuge Fahrerlaubnisse und Tankbevorrechtigungen zu erhalten, ansonsten steht die Bargeldversorgung schnell still.

Da die zurückgehende Nutzung barer Zahlungsmittel naturgemäß die Stückkosten für alle Aktivitäten rund ums Bargeld treibt, müssen wir zudem gemeinsam an effizienteren Techniken und Verfahren im Bargeldkreislauf arbeiten, um Bargeld auch wettbewerbsfähig zu halten.

Mehr falsche 200- und 500-Euro-Banknoten im Umlauf

www.bundesbank.de

DEUTSCHE BUNDESBANK EUROSYSTEM

Die Deutsche Bundesbank hat im ersten Halbjahr 2023 in Deutschland rund 26.700 falsche Euro-Banknoten im Nennwert von knapp 2,9 Mio. Euro aus dem Verkehr gezogen. Die Anzahl der Fälschungen stieg gegenüber dem zweiten Halbjahr 2022 um 10 Prozent. Trotzdem bleibt das Falschgeldaufkommen weiterhin niedrig: Rein rechnerisch entfielen sechs falsche Banknoten auf 10.000 Einwohner, sagte Burkhard Balz, im Vorstand der Deutschen Bundesbank unter anderem zuständig für Bargeld.

Besonders stieg die Anzahl der falschen 200- und 500-Euro-Banknoten. Dadurch fiel im ersten Halbjahr 2023 die Schadenssumme um 66 Prozent höher aus als im vorherigen Halbjahr. Mit den gefälschten 200- und 500-Euro-Banknoten wurden vor allem betrügerische Geschäfte mit Luxuswaren wie Schmuck, Goldbarren, Uhren und Autos abgewickelt, so Balz.

Die folgende Tabelle zeigt die Verteilung der Fälschungen auf die einzelnen Stückelungen im ersten Halbjahr 2023 und die Veränderung im Vergleich zum zweiten Halbjahr 2022:

Noten	1. Halbjahr 2023	Anteil (gerundet)	Veränderung zum Vorhalbjahr
5 €	314	1 %	27 %
10 €	1.698	6 %	15 %
20 €	5.305	20 %	6 %
50 €	9.862	37 %	+1 %
100 €	3.222	12 %	16 %
200 €	4.111	15 %	+87 %
500 €	2.178	8 %	+293 %
Gesamt	**26.690**		**+10 %**

Anzahl falscher Münzen gestiegen

Während im zweiten Halbjahr 2022 rund 40.800 falsche Münzen im deutschen Zahlungsverkehr festgestellt wurden, waren es im ersten Halbjahr 2023 rund 49.000 Stücke. Pro 10.000 Einwohner und Jahr fielen in Deutschland im ersten Halbjahr 2023 rechnerisch rund zwölf falsche Münzen an. Der deutliche Anstieg (+21 Prozent) liegt daran, dass die Kreditinstitute und Werttransportunternehmen noch Rückstände von nicht mehr umlauffähigen Münzen aus der Coronapandemie abarbeiten. In diesen waren auch falsche Münzen enthalten.

Die Fälschungen traten ausschließlich bei den drei höchsten Stückelungen auf und verteilten sich im ersten Halbjahr 2023 wie folgt:

Münzen	Anzahl	Anteil (gerundet)
50 Cent	**294**	1 %
1 €	2.520	5 %
2 €	46.172	94 %

Neue Lünendonk-Studie zu Cybersecurity 2023: Die Bedrohungslage steigt weiter an

Die Gefahr, Opfer eines Cyberangriffs zu werden, ist im vergangenen Jahr nochmals gestiegen. Infolge der voranschreitenden Digitalisierung ergeben sich neue Einfallstore und Angriffsvektoren für Hacker. Ebenso sind die Verschlüsselung und der Verkauf digitaler Assets und sensibler Daten ein lukratives Geschäft für Cyberangreifer. 84 Prozent der Unternehmen stufen folglich für das Jahr 2023 die Gefahrenlage im Vergleich zu 2022 als höher ein. Vor allem die Gefahr von DDoS-Angriffen (Distributed Denial of Service) wird größer eingeschätzt, was unter anderem mit der gestiegenen Professionalität von Hackerorganisationen zusammenhängt. Die Mehrheit der Unternehmen sieht sich zum aktuellen Zeitpunkt jedoch gut auf Cyberangriffe vorbereitet, allerdings haben viele Unternehmen auf dem Weg zu einer hohen Cyberresilienz noch einige Herausforderungen zu lösen: So beschränken 40 Prozent ihre Cybersecurity-Maßnahmen ausschließlich auf ihre eigenen Unternehmensnetzwerke, anstatt den Blick stärker auf die unternehmensübergreifenden Prozesse zu richten.

Dies sind Ergebnisse der neuen Lünendonk-Studie 2023 „Von Cyber Security zu Cyber Resilience – Wie Unternehmen auf die steigende Bedrohungslage reagieren“. Die Studie entstand in fachlicher Zusammenarbeit mit KPMG und steht unter **www.luenendonk.de** zum kostenfreien Download bereit.

Cybersecurity wird essenziell und komplexer

Mit zunehmender Digitalisierung ist es nicht mehr ausreichend, den Fokus nur auf den Schutz der eigenen Unternehmensnetzwerke zu richten. Cybersecurity muss frühzeitig bei der Entwicklung von Digitalstrategien und digitalen Produkten berücksichtigt werden. Tatsächlich sehen 86 Prozent der Unternehmen IT-Security bereits als Wertschöpfungsfaktor und festen Bestandteil ihrer digitalen Transformation an.

„Die Ergebnisse zeigen, dass die Bedeutung von Cybersecurity in Unternehmen im Bewusstsein des Topmanagements angekommen ist. Treiber hierfür sind unter anderem die regulatorischen Anforderungen an den Schutz von Kundendaten und geistigem Eigentum sowie die Absicherung Kritischer Infrastrukturen. Allerdings haben viele Unternehmen noch nicht die organisatorische und kulturelle Reife für eine Cyberresilienz aufgebaut“, kommentiert Mario Zillmann, Partner bei Lünendonk & Hossenfelder und Studienautor.

Tatsächlich verfügen nur 36 Prozent der befragten Unternehmen über ein zentrales Security Monitoring und nur jedes vierte Unternehmen (25 Prozent) über teil- oder vollautomatisierte Prozesse zur Erkennung und Abwehr von Cyberangriffen. Eine zentrale Einheit zur kontinuierlichen Überwachung des Security Monitorings und zur Reaktion auf Vorfälle, haben sogar nur 16 Prozent der befragten Unternehmen aufgebaut.

Aber auch die voranschreitende Cloud-Transformation verändert den Blick auf Cybersecurity.

Bilder: Lünendonk & Hossenfelder GmbH

Die Lünendonk & Hossenfelder GmbH mit Sitz in Mindelheim (Bayern) analysiert seit dem Jahr 1983 die europäischen Business-to-Business-Dienstleistungsmärkte (B2B). Im Fokus der Marktforscher stehen die Branchen Digital & IT, Managementberatung, Wirtschaftsprüfung sowie Steuer- und Rechtsberatung, Real Estate Services und Personaldienstleistung (Zeitarbeit, IT-Workforce). Zum Portfolio zählen Studien, Publikationen, Benchmarks und Beratung über Trends, Pricing, Positionierung oder Vergabeverfahren. Der große Datenbestand ermöglicht es Lünendonk, Erkenntnisse für Handlungsempfehlungen abzuleiten. Seit Jahrzehnten gibt das Marktforschungs- und Beratungsunternehmen die als Marktbarometer geltenden „Lünendonk®-Listen und -Studien“ heraus.
www.luenendonk.de

LÜNENDONK

„Die Komplexität zur Erkennung und Abwehr von Cyberangriffen nimmt durch die Cloud zu“, ergänzt Tobias Ganowski, Consultant bei Lünendonk & Hossenfelder. „Gerade Multi- und Hybrid-Cloud-Landschaften erfordern eine Orchestrierung und Verzahnung der einzelnen Security-Prozesse zu einem integrierten Security-Ansatz. Unternehmen werden daher in den nächsten Jahren die Vernetzung der vielen bereits vorhandenen dezentralen IT-Security-Tools zu integrierten Cloud Security Tool Suits im Sinne eines End-to-End-Managements vorantreiben, ebenso wie die Integration der hybriden Multi-Cloud- und Multi-Provider-Umgebungen in die bestehenden Security-Systeme.“

Cybersecurity-Budgets steigen

„Die meisten Unternehmen haben erkannt, dass nicht die Frage ist, ob, sondern wann sie erfolgreich gehackt werden. Eine hohe Cyberresilienz wird somit dadurch erreicht, dass Unternehmen zu jeder Zeit – sei es vor, während oder nach einem Angriff – Transparenz über ihre IT-Systeme haben und wissen, welche Maßnahmen zu welchem Zeitpunkt zu ergreifen sind“, erläutert Mario Zillmann. Daher planen 92 Prozent der befragten Unternehmen für 2023 und 2024 deutlich höhere Investitionen in das Security-Monitoring sowie 80 Prozent im Bereich Security Incident and Event Management (SIEM).

Ebenso stehen Cloud Security und Data Center Security nun bei deutlich mehr Unternehmen im Fokus. 69 Prozent werden bis 2024 in Cloud Security investieren (2022: 64 Prozent und sogar 78 Prozent in Data Center Security [2022: 74 Prozent]). Eine weitere Topmaßnahme ist für 86 Prozent das Vulnerability Management, also Lösungen zur Erkennung von Schwachstellen in den Security-Prozessen.

Über die Lünendonk-Studie

Für die Lünendonk-Studie 2023 „Von Cyber Security zu Cyber Resilience – Wie Unternehmen auf die steigende Bedrohungslage reagieren“ wurden 100 IT- und IT-Security-Verantwortliche mittelständischer Unternehmen und Konzerne befragt. Die Befragten stammen je zur Hälfte einerseits aus dem Finanzsektor sowie andererseits aus Unternehmen in der Industrie, dem Automotive-Bereich, dem Handel, der Energie- und Telko-Branche. Die Studie wurde in fachlicher Zusammenarbeit mit KPMG realisiert und steht ab sofort unter **www.luenendonk.de** zum kostenfreien Download bereit.

Frage: Wie hat sich die Bedrohungslage in Hinblick auf Cyber-Angriffe seit Anfang 2022 insgesamt verändert?; n = 100
Frage: Für wie wahrscheinlich halten Sie es, dass Ihr Unternehmen in den kommenden zwei Jahren einem schwerwiegenden Angriff zum Opfer fällt, durch ...; n=100; Skala von 1 = „sehr wahrscheinlich“ bis 4 = „gar nicht wahrscheinlich“; Werte beziehen sich auf „sehr wahrscheinlich“ und „eher wahrscheinlich“

Cyberattacken und Desinformationskampagnen in Deutschland – aktuelle Bedrohungen

Von Prof. Dr. Stefan Goertz

Das deutsche Bundesamt für Sicherheit in der Informationstechnik erklärt aktuell, dass die Bedrohung im Cyberraum in Deutschland so „hoch wie nie zuvor" sei, verursacht auch durch Cybercrime und Cyberattacken im Kontext des Ukrainekrieges.[1)]

Ein wesentliches Element einer hybriden Kriegsführung ist die Verschleierung. Akteure hybrider Kriegsführung operieren anonym oder bestreiten Beteiligungen an Operationen, Vorfällen und Kriegsverbrechen. Hybride Kriegsführung ist erfinderisch und koordiniert. Ein entscheidender Kriegsschauplatz von Hybridkriegsführung ist der Cyber- und Informationsraum. Die Kriegsführung Russlands gegen die Ukraine ist hybrid und dies spätestens seit der Annexion der Krim 2014. Die Kriegsführung Russlands im neuen Ost-West-Konflikt bedroht auch zahlreiche Staaten der westlichen Welt, Europas, auf verschiedenen Ebenen, mit verschiedenen Akteuren. Das „System Putin" kombiniert klassische Militäreinsätze, wirtschaftlichen Druck, (potenzielle) Angriffe auf Kritische Infrastrukturen (KRITIS), Cyberattacken sowie Desinformationskampagnen in den Medien und sozialen Netzwerken. Nach der Logik des russischen Generalstabschefs Waleri Gerassimow ist diese Kriegsführung Russlands „entgrenzt".[2)]

Aktuelle Cyberattacken

Im April 2023 wurde bekannt, dass der deutsche Rüstungskonzern Rheinmetall erneut Ziel einer Cyberattacke wurde. Das Ausmaß ist noch nicht absehbar, die Kölner Staatsanwaltschaft ermittelt. Rheinmetall ist Deutschlands größter Rüstungskonzern. Bei Militärfahrzeugen und im Munitionsgeschäft zählt das Unternehmen zu den drei größten Herstellern der westlichen Welt.[3)]

Eine weltweite Welle von Cyberattacken mit Erpressungssoftware legte zu Beginn des Jahres 2023 zahlreiche Unternehmen und öffentliche Einrichtungen in Europa und Nordamerika lahm. Nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) könnten aktuell Hunderte deutsche Firmen betroffen sein. Nach Angaben des BSI lag der geografische Schwerpunkt der Cyberattacken auf Frankreich, den USA, Deutschland und Kanada.[4)]

Die Firma Vulkan kooperiert nach Angaben deutscher und internationaler Berichte mit den wichtigsten russischen Geheimdiensten FSB, GRU und SWR. In den im Frühjahr 2023 ausgewerteten „Vulkan Files" wurden Angriffsziele benannt, zum Beispiel das „Lahmlegen von Kontrollsystemen von Eisenbahn-, Luft- und Schiffstransport" und die „Störung von Funktionen von Energieunternehmen und kritischer Infrastruktur".[5)] Mehrere westliche Geheim- und Nachrichtendienste halten die „Vulkan Files" für authentisch. Der Vorsitzende des Parlamentarischen Kontrollgremiums des Deutschen Bundestages, Konstantin von Notz, geht von „Hunderten solcher Cyberwaffen" aus, die gerade entwickelt würden. Die „Vulkan Files" legen zudem nahe, dass die als „Sandworm" weltweit bekannte gewordene Spezialeinheit 74455 des russischen Militärgeheimdienstes GRU mit der IT-Firma Vulkan kooperiert hat. „Sandworm" soll unter anderem verantwortlich sein für Angriffe auf ukrainische Firmen im Juni 2017. Die Schadsoftware geriet außer Kontrolle und befiel weltweit Tausende Computer, auch in den USA, und verursachte Schäden in dreistelliger Millionenhöhe. Mehrere „Sandworm"-Hacker sind deswegen in den USA angeklagt worden.[6)]

Im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine zählte das Cyber-Peace-Institut in Genf für das Jahr 2022 mehr als 850 Cyberattacken. Diese wurden demnach von prorussischen und proukrainischen Hackern gegen Ziele in der Ukraine, Russland und rund drei Dutzend anderen Ländern ausgeführt, darunter auch 23 in Deutschland. Prorussische Hackernetzwerke würden durch immer stärkere Vernetzung immer unberechenbarer, erklärte die Chefanalystin des Instituts, Emma Raffray, Anfang 2023. Bei den betroffenen Flughäfen seien Websites vorübergehend gestört worden. Allein im September 2022 wurden an zwei Tagen fünf Cyberattacken mit 18 Zielen in Deutschland registriert.[7)]

Prof. Dr. Stefan Goertz

Hochschule des Bundes, Fachbereich Bundespolizei, Lübeck

Dieser Beitrag stellt die persönliche Auffassung des Autors dar.


Bild: Markus Spiske / unsplash.com

Seit Beginn der deutschen Unterstützung für die Ukraine mit Waffenlieferungen und Sanktionen gegen Russland gelten Cyberattacken gegen Energieversorger oder militärische Einrichtungen als große Bedrohung für Deutschland. Die russischen Geheimdienste verfügen über Fähigkeiten, neben KRITIS auch den politischen Betrieb anzugreifen. Bereits kurz nach Beginn des Ukrainekrieges kam es in Deutschland zu einer Angriffswelle durch die mutmaßlich von russischen Geheimdiensten gesteuerte Hackerkampagne „Ghostwriter". In der Vergangenheit hatte „Ghostwriter" nach Angaben des Bundesamtes für Verfassungsschutz bereits „erfolgreich Daten von Mandatsträgerinnen und Mandatsträgern und sonstigen politischen Zielen" erbeutet. Diese könnten womöglich über sogenannte Hack-and-Leak-Operationen öffentlich gemacht und für Desinformationskampagnen missbraucht werden.[8)]

Aktuelle Desinformationskampagnen

Russische Desinformationskampagnen gegen Deutschland und andere europäische Staaten sind kein neues Phänomen, haben allerdings seit dem Beginn des russischen Angriffskrieges gegen die Ukraine eine neue Qualität und Quantität angenommen.

Als für die Bekämpfung russischer Desinformationskampagnen zuständige Organe beschreibt die Bundesregierung das Auswärtige Amt (AA), das Bundespresseamt (BPA) sowie das Bundesministerium des Innern und für Heimat (BMI) und seine nachgeordneten Behörden (vor allem das Bundesamt für Verfassungsschutz), die das Internet hinsichtlich dort kursierender falscher oder irreführender Informationen beobachten.[9)] Die Bundesregierung betreibe nach eigenen Angaben eine „proaktive faktenbasierte und zielgruppengerechte Kommunikation zur aktuellen Lage und zu den ergriffenen Maßnahmen". Neben „angemessenen reaktiven Maßnahmen, wie der Richtigstellung von Falschinformationen", stünden „Prävention und der Aufbau von gesamtstaatlicher und gesellschaftlicher Resilienz" im Fokus.[10)] Hierzu führte die Bundesministerin des Innern und für Heimat, Nancy Faeser, im Mai 2022, in der ersten Hochphase russischer Desinformationskampagnen gegen Deutschland seit Beginn des russischen Angriffskrieges gegen die Ukraine, aus: „Der Kampf gegen Desinformation ist eine zentrale Herausforderung zum Schutz unserer Verfassung – deshalb dürfen wir diesen Schutz nicht nur als behördliche Aufgabe des BfV verstehen. Verfassungsschutz ist eine umfassende Aufgabe von Staat und Gesellschaft."[11)] Bundesinnenministerin Faeser bewertete es als

Erfolg, dass die EU wenige Tage nach Beginn des Krieges Sanktionen gegen die russischen Medien Russia Today und Sputnik verhängte und damit die Reichweite russischer staatsnaher Medien eingeschränkt habe. Hierbei räumt Faeser jedoch ein, dass seit den EU-Sanktionen gegen diese staatsnahen russischen Medien prorussische Desinformation und Propaganda verstärkt über Accounts in den sozialen Medien verbreitet werde. Außerdem werde versucht, „die Nutzerinnen und Nutzer auf alternative Plattformen wie zum Beispiel Telegram umzuleiten".[12] Von Telegram aus kann die russische Propaganda leicht von anderen Akteuren, Gruppen und Einzelpersonen verbreitet werden.[13]

Eine Datenauswertung des WDR, des NDR und der Süddeutschen Zeitung zeigte jedoch bereits im April 2022, dass Facebook nicht gegen die russischen Desinformationskampagnen in Deutschland ankommt. Eine Vielzahl von Fake News, beispielsweise über die Massaker und Gräueltaten russischer Soldaten an Ukrainerinnen und Ukrainern von Butscha, verbreiteten sich im April 2022 auf Facebook rasant. Videos mit Fake News russischer Desinformationskampagnen wurden in Deutschland Tausende Male angeschaut.[14]

Zur Facebook-Seite der russischen Botschaft in Deutschland, die seit dem Beginn des Krieges unbehelligt Desinformation, Propaganda und Fake News in Deutschland verbreiten kann, kamen zahlreiche kleine Accounts aus dem verschwörungsideologischen Milieu, beispielsweise die Facebook-Seite „Anonline". Diese wurde unmittelbar nach dem Beginn des russischen Angriffskrieges gegründet, nach vier Wochen und 250 Pro-System-Putin-Posts folgten ihr in Deutschland im April 2022 über 10.000 Menschen. Insgesamt wurden von „Anonline" gepostete Videos mehr als zwei Millionen Mal gesehen. Facebook-Seiten wie diese gibt es viele und ihre Followerzahlen verzehnfachten sich teilweise innerhalb einer Woche nach dem Beginn des Angriffskrieges.[15] Hier scheinen die zuständigen deutschen Ministerien und Behörden noch keine wirksamen Gegenmittel gefunden zu haben.

Das Bundesinnenministerium zeigte sich Ende August 2022 beunruhigt über gefälschte und täuschend echt aussehende Medien-Websites mit prorussischen Desinformationen rund um den Ukrainekrieg. So teilte ein Sprecher des Bundesministeriums des Innern und für Heimat mit: „Wir haben mit Sorge zur Kenntnis genommen, dass über Fake Accounts in bestimmten sozialen Medien täuschend echt aussehende, allerdings gefälschte Webauftritte von etablierten Nachrichtenseiten verlinkt werden. Dort werden demnach erfundene Nachrichten und gefälschte Videos – Teil der russischen Desinformationskampagnen – verbreitet. Diese verfolgen das Ziel, Vertrauen in Politik, Gesellschaft und staatliche Institutionen zu untergraben", erklärte der Sprecher des Bundesinnenministeriums.[16]

Das ZDF sprach Ende August 2022 von der größten Desinformationskampagne in Deutschland bisher: Nachgemachte Medienseiten als Teil einer großflächig angelegten russischen Desinformationskampagne verbreiten, mutmaßlich vom „System Putin" orchestriert, Propaganda, Hunderte Fake Accounts teilen sie massenhaft in sozialen Medien. Die Versuche, die öffentliche

Bild: # 179689060 / stock.adobe.com

Meinung in Deutschland mit prorussischer Propaganda zu beeinflussen, erreichten eine zuvor nicht gekannte Dimension. Bei dieser neuen, großflächig angelegten Desinformationskampagne Russlands wurden massenweise Webseiten großer Medienmarken wie Bild, Welt, t-online und Spiegel täuschend echt nachgebaut, um genau solche Fake News und Fakevideos in die Welt zu setzen. Ein Heer von extra angelegten Fake Accounts verbreitete in einem zweiten Schritt diese Falschnachrichten in den sozialen Medien.[17]

Konstantin von Notz, stellvertretender Fraktionsvorsitzender der Grünen und Vorsitzender des Parlamentarischen Kontrollgremiums, wodurch er einen sehr umfassenden und profunden Informationsstand hat, was Informationen der deutschen Nachrichtendienste zu den russischen Desinformationskampagnen angeht, sagte bereits Ende August 2022, die Dimension von Desinformationskampagnen zur intransparenten Manipulation demokratischer Diskurse habe ein „besorgniserregendes Ausmaß" angenommen. Neben Sicherheitsbehörden und Plattformbetreibern sei auch die Politik gefragt,

so von Notz: „Wir brauchen neue und bessere Strukturen zur Erkennung und Abwehr dieser hybriden Bedrohungen."[18]

Neue Gegenmaßnahmen, Akteure und Mittel – Vorschläge

Aufgrund der oben dargestellten Bedrohungen sollten umgehend folgende Maßnahmen von der Bundesregierung, den zuständigen Ministerien und deren Behörden gegen Desinformationskampagnen getroffen werden:

- Ein staatliches Zentrum bzw. ein Beauftragter für die Analyse von Desinformationskampagnen und Fake News sowie das Veröffentlichen von Counter-Narratives sollte umgehend beauftragt werden, als Bindeglied zwischen den Medien, den sozialen Medien und den Behörden.
- Die Forschung zum Themenbereich Desinformationskampagnen, Fake News, Narrative, Strategien und Akteure sowie Counter-Narratives muss dringend und schnellstmöglich intensiviert werden und dafür benötigt es eine bundesweite Strategie und Konzeption.
- Medienkompetenz muss ein großer zukünftiger Schwerpunkt an den Schulen darstellen und danach im Rahmen von politischer Bildung durch Angebote zu lebenslangem Lernen für alle Altersgruppen ergänzt werden. Es geht hier um lebenslange Resilienz gegen Desinformationskampagnen, Fake News und Propaganda, um das Stärken bzw. Aufbauen einer demokratischen Resilienz. Dies muss in einem whole-of-society approach angegangen werden.
- Eine europaweite Vernetzung des oben vorgeschlagenen staatlichen Zentrums bzw. eines Beauftragten für die Analyse von Desinformationskampagnen und Fake News sowie das Veröffentlichen von Counter-Narratives sowohl mit der EU selbst als auch mit den einzelnen EU-Staaten müsste sofort initiiert werden, da es gerade im Bereich nordeuropäischer Länder wie Finnland und osteuropäischer Länder wie Tschechien und Polen Best-Practice- und Lessons-Learned-Erkenntnisse gibt, weil diese Staaten schon seit vielen Jahren russischen Desinformationskampagnen ausgesetzt sind.[19]

Fazit

Im Kampf gegen den Westen, im neuen Ost-West-Konflikt des 21. Jahrhunderts, nutzt das „System Putin" Cyberattacken sowie Desinformationskampagnen gegen Deutschland und andere westliche Staaten.

Die vom deutschen Bundeskanzler Scholz postulierte „Zeitenwende" konzentriert sich auf neue Kampfpanzer und Kampfflugzeuge, übersieht aber, dass die russische Hybridkriegsführung einen neuen Ost-West-Konflikt begonnen hat, der außerhalb der Ukraine, in der EU, sehr stark in den sozialen Medien geführt wird, durch Fake News und Desinformationskampagnen. Deutschland und die anderen EU-Mitgliedstaaten benötigen umgehend staatliche Zentren bzw. Beauftragte für die Analyse von Desinformationskampagnen und effektive Counter-Narratives, die sehr eng mit Akteuren der Wissenschaft und der Sicherheitswirtschaft kooperieren.

Unsere Demokratie benötigt starke Abwehrkräfte gegen Desinformationskampagnen, Fake News und Propaganda. Diese Abwehrkräfte müssen in uns gestärkt werden – sofort.

Literatur

1) Vgl. **https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html** (30.07.2023)

2) Vgl. Goertz, S. (2023): Russische Cyberattacken, Angriffe gegen KRITIS sowie Desinformationskampagnen – die Gegenmaßnahmen der deutschen Politik und Behörden. In: Polizei Praxis 1/2023, S. 52.

3) Vgl. **https://www.tagesschau.de/inland/cyberangriff-rheinmetall-101.html** (30.07.2023)

4) Vgl. **https://www.tagesschau.de/inland/gesellschaft/cyberattacke-deutschland-101.html** (30.07.2023)

5) Vgl. **https://www.zdf.de/politik/frontal/doku-vulkan-files-cyberangriff-russland-ukraine-krieg-leak-daten-100.html** (30.07.2023)

6) Vgl. ebd.

7) Vgl. **https://www.zdf.de/nachrichten/politik/cyber-angriffe-hacker-deutschland-ukraine-krieg-russland-102.html** (30.07.2023)

8) Vgl. **https://www.spiegel.de/politik/innenministerin-nancy-faeser-ueber-russische-cyberangriffe-wir-stehen-im-wettlauf-mit-immer-neuen-angriffsweisen-und-technologien-a-779c815a-9514-4229-ac07-f2afa4f87876** (30.07.2023)

9) Vgl. **https://www.bmi.bund.de/SharedDocs/topthemen/DE/topthema-desinformation/massnahmen-der-bundesregierung.html** (30.07.2023)

10) Vgl. ebd.

11) **https://www.bmi.bund.de/SharedDocs/reden/DE/2022/faeser-20220519-bfv-symposium.html** (30.07.2023)

12) Vgl. ebd.

13) Goertz, S. (2022): Russische Desinformationskampagnen in Deutschland. Gegenmaßnahmen der Bundesregierung und Behörden – Kritik und Vorschläge. In: Veko online 26.10.2022 **https://www.veko-online.de/?view=article&id=2177:titel-russische-desinformationskampagnen-in-deutschland&catid=189&highlight=WyJydXNzaXNjaGUiLCJkZXNpbmZvcm1hdGlvbnNrYW1wYWduZW4iLCJydXNzaXNjaGUgZGVzaW5mb3JtYXRpb25za2FtcGFnbmVuII0=** (30.07.2023)

14) Vgl. **https://www.tagesschau.de/investigativ/ndr-wdr/russland-desinformation-105.html** (30.07.2023)

15) Vgl. ebd.

16) Zitiert nach: **https://www.zdf.de/nachrichten/politik/innenministerium-fake-webseiten-ukraine-krieg-russland-100.html** (30.07.2023)

17) Vgl. **https://www.zdf.de/nachrichten/politik/desinformation-kampagne-facebook-ukraine-krieg-russland-100.html** (30.07.2023)

18) Zitiert nach: **https://www.rnd.de/politik/russland-faelscht-deutsche-nachrichtenseiten-und-verbreitet-propaganda-AYHVPHB5TRGU5IHQFTIBP5Y4WE.html** (30.07.2023)

19) Vgl. Goertz, Russische Desinformationskampagnen in Deutschland. Gegenmaßnahmen der Bundesregierung und Behörden – Kritik und Vorschläge. In: Veko online 26.10.2022

Welche Spuren interne Täter im Netzverkehr legen

Vier Arten von internen Angreifern verlangen einen Schutz auf Netzwerk- und Endpunktebene.

Von Paul Smit

Viele Diskussionen malen gerne den eigenen Mitarbeiter als IT-Sicherheitsrisiko an die Wand. Die tatsächliche Gefahr, die von ihm ausgeht, ist aber oft unklar. Verschiedene Täterprofile interner Angreifer können größeren Schaden anrichten. Eine Erkennung und Abwehr dieser Aktionen sind nur durch einen permanenten Blick auf den Netzwerkdatenverkehr und die Endpunkte möglich – basierend auf Künstlicher Intelligenz.

Hinter den internen Gefahren für IT, Informationen und Geschäftsprozesse stehen absichtliche oder unabsichtliche Aktionen von Mitarbeitern sowie von Zulieferern oder freien Mitarbeitern mit Zugriff aufs Netz.

Absicht, Versehen oder mit gekaperter Identität – Täterprofile interner Angreifer

Die größte Gefahr geht vom absichtlich agierenden Binnentäter aus, der seine Zugänge auf Dateien, Applikationen und Systeme nutzt. Persönliche und finanzielle Gründe sind die Hauptmotivation, weit vor einer Sabotage. Hier gibt es zwei Typen:

- Der **Kollaborateur** ist für seine Auftraggeber aktiv: Konkurrenten, cyberkriminelle Malware-Akteure oder gar Staaten.
- Der „**einsame Wolf**“ agiert unabhängig und unbeeinflusst. Handelt es sich um einen Anwender mit den entsprechenden Privilegien, verfügt ein solcher Täter über ein ernstzunehmendes Gefahrenpotenzial.

Der nicht absichtlich oder achtlos handelnde Täter lässt sich ebenfalls in zwei Kategorien einteilen.

- Der **Bauer im Schach der Cyberkriminellen („pawn“)**: Er ist ein autorisierter Anwender, den Hacker ohne dessen Willen manipulieren. Cyberkriminelle greifen ihn mit gezieltem Spear Phishing an, um seine Identität zu kapern. Viele Angriffe zielen auf den Endpunkt eines einzelnen Anwenders.
- **Unabsichtlich handelnder „goof“**: Er verstößt aus Arroganz, Ignoranz, Inkompetenz oder schlichtweg mangelndem Bewusstsein gegen Richtlinien der IT-Sicherheit. Er ist oft eine leichte Beute für Phishingangriffe mit anschließender Privilegieneskalation.

Informationen beiseiteschaffen und löschen kann jeder Mitarbeiter am PC. Für größere und komplexere Angriffe verengt sich der Täterkreis. Der überwiegende Teil der Belegschaft verfügt nicht über die Mittel, die Rechte und das Wissen, um schwerwiegende Angriffe auf einen Back-up- oder Active-Directory-Server zu starten. Zudem können sie keine Privilegien eskalieren oder in größerem Umfang Daten aus einem vom Provider gut abgeschirmten Cloud-Endpunkt exfiltrieren. Dazu sind nur technisch kompetente Mitarbeiter aus der IT-Administration in der Lage. Kapern aber Angreifer die Identitäten eines gewöhnlichen Mitarbeiters, können auch diese zu einer gefährlichen Waffe werden.

Der Blick nach innen

Jeder Angreifertyp hinterlässt Spuren im Netzverkehr und auf den Endgeräten. Auf Netzwerkebene nutzen sie etwa mit Server Message Blog (SMB) das Windows-Netzwerkprotokoll für ihre eigenen Zwecke. Eine Exfiltration von Informationen verrät sich durch den Kontakt zu einer unbekannten IP-Adresse. Wenn sich interne Nutzer plötzlich anders verhalten, erkennt eine Künstliche Intelligenz diese punktuellen Abweichungen von Normalabläufen sowohl im Netzwerk als auch auf dem Endpunkt. KI-Lösungen machen Vorgänge sichtbar und setzen sie in einen Kontext. Selbst kleine und mittelständische Unternehmen können diese KI-Lösungen nutzen. Gerade für den Schutz vor Angreifern aus dem Inneren sind sie ein notwendiges Instrument für eine handhabbare IT-Sicherheit.

Anomales Verhalten von Tätern im Netzwerk ist vor allem durch folgende Aktivitäten sichtbar:

- **Unerlaubter oder anomaler Zugriff auf Systeme oder Daten mit legitimen Zugangsdaten:** Ein Mitarbeiter loggt sich etwa plötz-

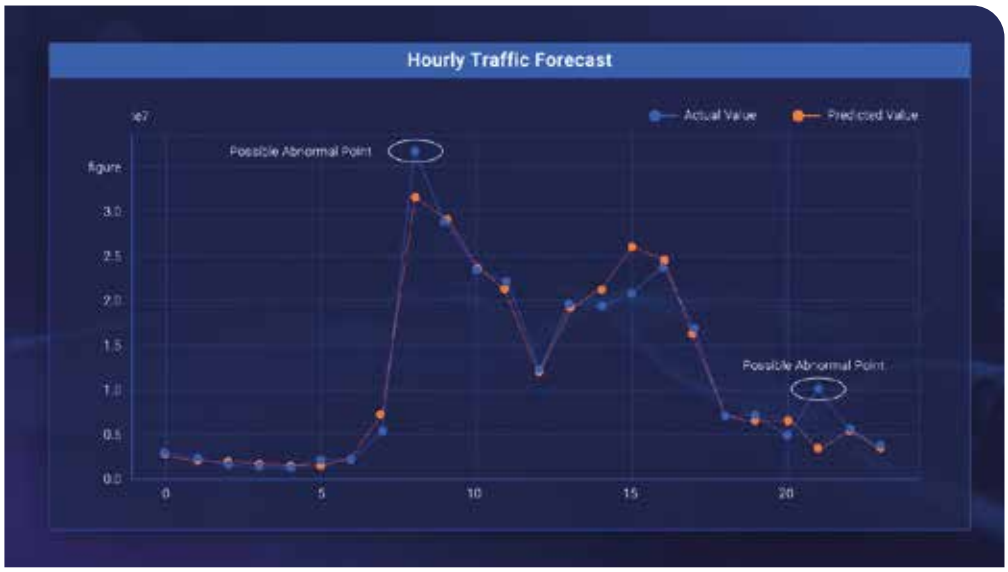
Paul Smit

Chief Technical Officer bei ForeNova Technologies

ForeNova Technologies B.V. ist ein schnell wachsender Cybersicherheitsspezialist, der mittelständischen Unternehmen preiswerte und umfassende Network Detection and Response (NDR) anbietet, um Schäden durch Cyberbedrohungen effizient zu mindern und Geschäftsrisiken zu minimieren. NovaCommand wurde vom renommierten Sans-Institute getestet. Mit ForeNova NovaGuard steht auch ein EDR-Agent zur Verfügung. Der Dienst ForeNova MDR kombiniert aktuelle, auf Künstlicher Intelligenz basierende Sicherheitstechnologien mit dem Know-how, der Expertise und dem Urteilsvermögen von menschlichen Sicherheitsanalysten. ForeNova B.V. betreibt seine Lösung für Kunden aus einem Rechenzentrum in Frankfurt am Main und konzipiert alle Lösungen DSGVO-konform. Die Zentrale des Unternehmens befindet sich in Amsterdam.
Weitere Informationen unter **https://www.forenova.com/de/**

lich zu ungewöhnlichen Zeiten oder an ungewöhnlichen Orten im Netz ein. Ein IT-Administrator oder Mitarbeiter durchsucht Bereiche des Netzes, für die er keine Rechte hat. Diese Szenarien sind ebenso verdächtig wie ein Zugriff auf einen Back-up-Server, der für gewöhnlich nur zum Verwalten, Überprüfen der Sicherungen oder zum Wiederherstellen von Daten erfolgt.

- **Suche im Netzwerk:** Ein interner Nutzer bewegt sich im Normalfall sicher auf den ihm vorgegebenen Bahnen und steuert gezielt Systeme, Daten und Applikationen an. Verlässt er diese, verhält er sich wie ein externer Angreifer: Er steuert nach und nach Systeme an, um sie auszukundschaften oder zu verändern.
- **Datenexfiltration:** Sensible Daten werden auf einen externen Datenträger kopiert oder per Mail und Cloud-Dienste versandt. Der Anschluss eines Gerätes ist ebenso sichtbar wie der Ausschlag des Datenverkehrs.



Abwehr im Netz und am Endpunkt

Angriffe eines Binnentäters können durch das kontinuierliche Monitoring des gesamten internen und externen Datenverkehrs erkannt werden. Etwa durch eine konsistente User-Entity-Behaviour-Analyse (UEBA), den Blick auf Nutzeraktivitäten, die Analyse der Log-ins, Dateizugriffe und des Ressourcengebrauchs.

Daraus leiten sich vorbeugende Maßnahmen in der Netzwerktopologie und in der Blockade von Angriffen durch eine Endpoint Detection and Response unmittelbar vor der Exekution eines Angriffes ab. Zu diesen Maßnahmen gehören im Netz und am Endpunkt vor allem:

- **Mikrosegmentierung im Netzwerk**: um Systeme, die mit dem angegriffenen Endpunkt regelmäßig kommunizieren, im Ernstfall schnell vollständig blockieren zu können. Dies beschränkt gleichzeitig den Radius der Seitwärtsbewegungen eines internen Angreifers.
- **Kontrolle der Endpunkte**: Hacker ändern Systeme nicht nur durch neue Malware, sondern auch durch neue Konfigurationen. Die Analyse von Änderungen des Systems ist deshalb die erste Bedingung für den Block eines Systems. Ist eine Anomalie auf einem Endpunkt hinreichend auffällig, veranlasst eine automatisierte Abwehr sofort den Back-up des Systems, um die Informationen vor einer Verschlüsselung zu retten. Der angegriffene PC kommt dann in Quarantäne – genauso wie die Rechner der anderen Mitarbeiter einer Abteilung.
- **Nutzen von IT-Sicherheitstechnologien** wie vor allem Antivirus, Firewall, Data Loss Prevention oder Identity Access Management.

Das menschliche Auge des Sicherheitsanalysten

Viele, oft individuell handelnde, Binnentäter sind durch eindimensionale Sicherheitsansätze oder durch automatisiertes Monitoring allein nicht zu erkennen. Die Angreifer nutzen in der Regel legitime Tools und installieren selten eine Malware. Sie benötigen kein Einbruchswerkzeug. Entitäten wie Nutzer oder Systeme sind aber dennoch durch bestimmtes anomales Verhalten erkennbar. Für das Gesamtbild und vor allem für die effiziente Abwehr bedarf es zusätzlich des menschlichen Auges eines Sicherheitsanalysten. Er analysiert das aufgezeichnete Verhalten interner Entitäten. Er erkennt durch außergewöhnliche Log-ins, dass wahrscheinlich nicht mehr der eigentliche Nutzer den Account kontrolliert. Er reagiert auf Alarme zu einer Malware-Infektion oder hat ihn bei Phishingkampagnen als möglicher Ausgangspunkt einer internen Attacke im Blick. Er steuert die Abwehr und blockt verdächtige Protokolle oder Datenübertragung über die von ihm verwaltete Firewall. Im Dialog mit den zu schützenden Unternehmen erkennt der Sicherheitsanalyst, ob hinter einem verdächtigen Verhalten sich nicht doch ein legitimer Nutzer verbirgt – ein neuer Mitarbeiter, eine neue Filiale oder eine neu vergebene Kompetenz.

Dienst-Smartphone wird im Urlaub zur Gefahr für Unternehmen

G DATA-Umfrage: Über 80 Prozent der Deutschen nutzen auf Reisen freies WLAN mit ihrem Diensthandy.

Unterwegs spart öffentliches WLAN mobile Daten und Kosten. Das ist auch mit dem Diensthandy bequem, aber gefährlich, denn Kriminelle nutzen es als Einfallstor. Die repräsentative G DATA-CyberDefense-Umfrage zum Gebrauch von Firmengeräten im Urlaub offenbart Nachholbedarf bei der IT-Sicherheit: Vier von fünf Personen verwenden mit ihrem dienstlichen Smartphone freies WLAN und riskieren, dass vertrauliche Daten von ihrem Unternehmen in die Hände von Cyberkriminellen geraten. G DATA gibt fünf Tipps, was vor Urlaubsbeginn in Sachen IT-Sicherheit wichtig ist.

Bild: Frederik Lipfert / unsplash.com

IT-Sicherheit kennt keine Ferien. Eine repräsentative G DATA-Umfrage zum Reiseverhalten zeigt, dass bei jedem zweiten Deutschen auch ein Smartphone oder Tablet von der Firma mit im Gepäck ist. Das Problem: Vier von fünf der befragten Personen nutzen mit ihrem dienstlichen Gerät öffentliches WLAN im Hotel, am Bahnhof oder am Flughafen. Nur jeder Zweite setzt dabei auf eine sichere Verbindung mit einem Virtual Private Network, kurz VPN. In kostenfreien WLAN-Hotspots lauert eine große Bedrohung. Cyberkriminelle können sich zwischen Nutzern und Zugriffspunkt schalten und auf diese Weise E-Mails, Kreditkartendaten oder Log-in-Daten für das Firmennetzwerk mitlesen. Um die Unternehmensdaten zu schützen und Missbrauch zu verhindern, sollte die IT-Sicherheit in den Ferien mit Dienst-Smartphone nicht vernachlässigt werden.

Freies WLAN ohne VPN stellt im Urlaub ein großes Sicherheitsrisiko dar

Ob als Navigationsgerät bei der selbst geplanten Entdeckungstour im Urlaubsort oder als Kameraalternative für Erinnerungen, das Smartphone ist auch auf Reisen unverzichtbar. Frei verfügbares WLAN im Café oder an anderen öffentlichen Orten ist bei Verbindungsproblemen oder aus Kostengründen verlockend, denn es verspricht eine stabile und schnelle Verbindung. Laut der repräsentativen G DATA-Urlaubsumfrage nutzen 82,4 Prozent der Reisenden mit Dienstgerät öffentliches WLAN und riskieren damit, dass Cyberkriminelle Zugang zu Firmendaten bekommen. Frei verfügbare WLAN-Netze sind in der Regel nicht verschlüsselt oder passwortgeschützt. Cyberkriminelle können hierdurch den Datenstrom mitlesen oder Schadsoft-

G DATA CyberDefense
Mit ganzheitlichen CyberDefense-Dienstleistungen macht G DATA CyberDefense verteidigungsfähig gegen Cybercrime. Das renommierte IT-Security-Unternehmen schützt mit KI-Technologien, Endpoint Protection, Security Monitoring und bietet Penetrationstests, Incident Response sowie Awareness-Trainings an, um Unternehmen bestmöglich abzusichern.

Die G DATA CyberDefense AG unterstützt ihre Kunden in jeder Sicherheitslage. Vom Headquarter in Bochum sorgen mehr als 550 Mitarbeitende für die digitale Sicherheit von Unternehmen, Kritischen Infrastrukturen wie Krankenhäusern oder Flughäfen sowie Millionen Privatanwendern. Mit fast 40 Jahren Expertise in Malware-Analyse hat sich G DATA zu einem Top-Player der Cybersecurity-Welt entwickelt und betreibt Forschung und Softwareentwicklung ausschließlich in Deutschland. Die G-DATA-Sicherheitslösungen sind in mehr als 90 Ländern erhältlich und wurden von unabhängigen Testinstituten vielfach ausgezeichnet.

www.gdata.de

ware auf das Gerät schleusen. Nur die Hälfte der Reisenden mit Smartphone oder Tablet nutzen VPN, um sich sicher im Internet zu bewegen.

„Unternehmen sollten auf eine VPN-Software nicht verzichten, wenn sie die Möglichkeit bieten, Smartphones und Tablets auch privat zu nutzen", sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense. „Öffentliche WLAN-Netze zum Surfen oder USB-Anschlüsse zum Laden können

Bild: yousef alfuhigi / unsplash.com

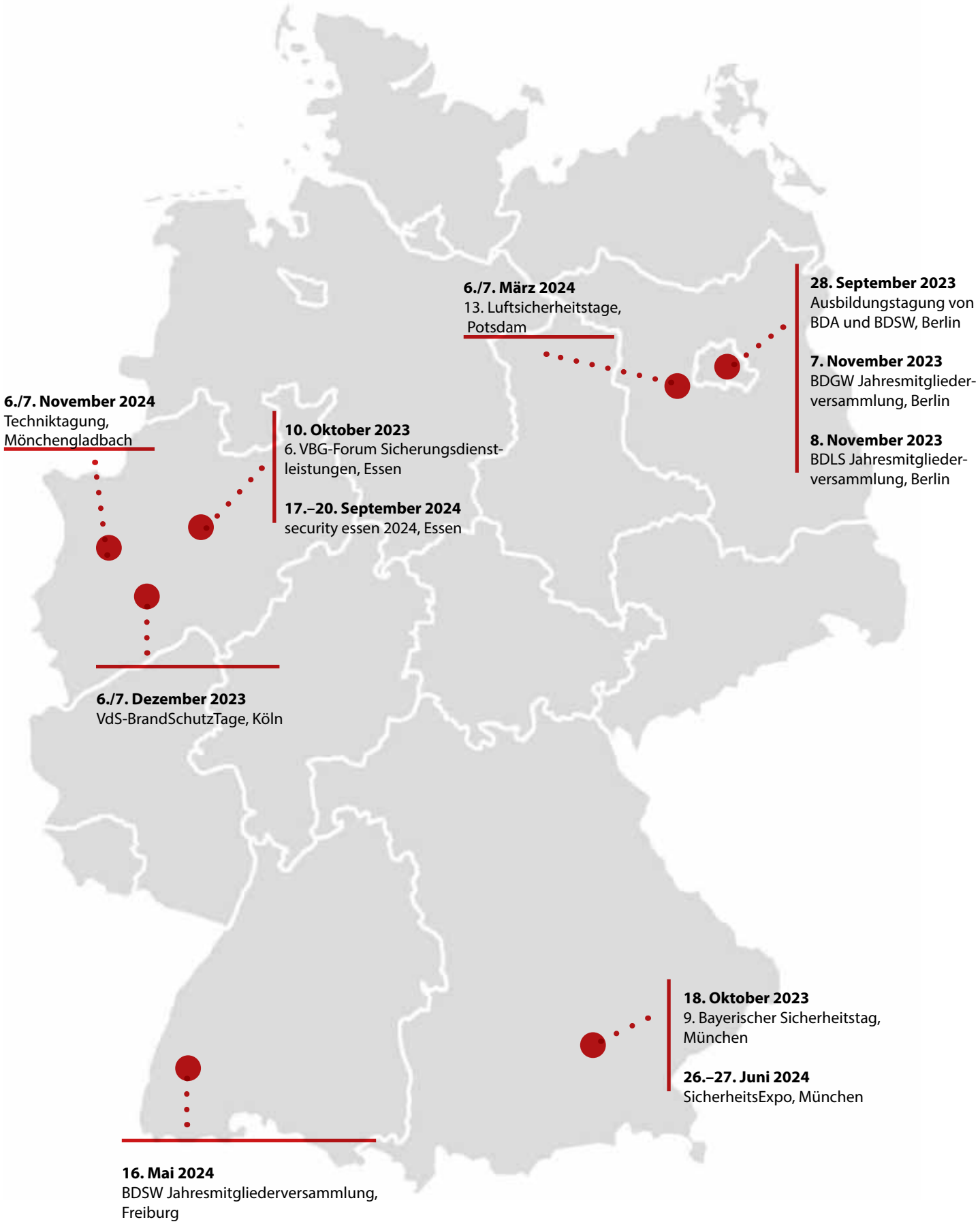
riskant sein. Um die Mitarbeitenden für die Gefahren im Urlaub zu sensibilisieren und eine höhere Sicherheit zu gewährleisten, bieten sich zum Beispiel auch Security-Awareness-Trainings an."

Generell gilt für den Urlaub mit internetfähigen Geräten, egal ob Privat- oder Firmengerät: Sie sollten so wenig Daten wie möglich enthalten. Wichtig ist es außerdem, alle Anwendungen mit Updates auf den neuesten Stand zu bringen – vom Betriebssystem über die Apps bis hin zur Sicherheitssoftware.

Fünf Sicherheitstipps von G DATA für den digitalen Reisekoffer

- **Back-ups machen:** Vor Reiseantritt sind Datensicherungen von wichtigen Informationen, Fotos und Kontakten sinnvoll. Durch Sicherung auf einem Speichermedium oder in der Cloud lassen sich diese im Falle eines Geräteverlusts schnell wiederherstellen. Generell gilt: so wenig vertrauliche Daten wie möglich in den Urlaub mitnehmen.
- **Security-Software installieren:** Eine leistungsfähige Sicherheitslösung gehört zur Grundausstattung jedes PCs und Mobilgeräts. Neben einem effektiven Virenschutz sollte diese auch einen Spamfilter, eine Firewall und einen Echtzeitschutz gegen Online-Bedrohungen umfassen. Wenn das Handy abhandenkommt, lassen sich Daten häufig auch aus der Ferne löschen.
- **Updates durchführen:** Ein aktuelles Betriebssystem sowie Updates von Anwendungen und Apps schließen kritische Sicherheitslücken. Angriffe laufen somit ins Leere und der Computer oder das mobile Gerät bleibt sicher.
- **VPN-Software installieren:** VPN sorgt für eine sichere Verbindung durch eine verschlüsselte Übertragung von Daten. Diese sind von außen nicht einsehbar und können von Cyberkriminellen nicht entschlüsselt werden.
- **Powerbank oder USB-Kondom einpacken:** USB-Ladestationen bieten Cyberkriminellen viel Raum, um Schaden anzurichten. Eine Alternative zu öffentlichen Ladeorten ist die eigene Powerbank. USB-Ladestationen sollten nur mit einem USB-Kondom genutzt werden, das in keinem Gepäck fehlen sollte. Es schützt beim Aufladen vor Datenableitung und wird zwischen Ladekabel und Buchse gesteckt, sodass nur der Strom zum Aufladen fließt.

Mehr Tipps für eine sichere Reise mit digitalen Geräten finden Sie im G DATA-Ratgeber „Sicher im Urlaub" unter: **www.gdata.de/tipps-tricks/sicher-im-urlaub**.



6./7. November 2024
Techniktagung, Mönchengladbach

10. Oktober 2023
6. VBG-Forum Sicherungsdienstleistungen, Essen

17.–20. September 2024
security essen 2024, Essen

6./7. Dezember 2023
VdS-BrandSchutzTage, Köln

6./7. März 2024
13. Luftsicherheitstage, Potsdam

28. September 2023
Ausbildungstagung von BDA und BDSW, Berlin

7. November 2023
BDGW Jahresmitgliederversammlung, Berlin

8. November 2023
BDLS Jahresmitgliederversammlung, Berlin

18. Oktober 2023
9. Bayerischer Sicherheitstag, München

26.–27. Juni 2024
SicherheitsExpo, München

16. Mai 2024
BDSW Jahresmitgliederversammlung, Freiburg

Tiefgreifende Veränderung

Von Holger Köster

Holger Köster

Geschäftsführer der HERSA-Unternehmensgruppe und Vorsitzender des BDSW-Arbeitskreises Wirtschaftsschutz

Die Erfindung der Dampfmaschine oder der Elektrizität wird nicht ohne Grund als revolutionär bezeichnet. Sie haben das Leben der Menschen grundlegend verändert. Ähnlich wird es sich mit der Künstlichen Intelligenz (KI) verhalten. Ihr Einsatz im Bereich Sicherheit und Verteidigung bringt selbstverständlich tiefgreifende Veränderungen mit sich.

Während Chancen für innovative Sicherheitsanwendungen entstehen, wächst natürlich auch die Gefahr KI-gesteuerter Angriffe. KI ist dabei aber kein bloßer Teilaspekt technischer Entwicklung, sondern wird alle anderen Bereiche grundlegend transformieren. Nicht auf die leichte Schulter zu nehmen sind auch ethische Vorbehalte.

Andererseits birgt KI enormes Potenzial – sowohl zivil als auch militärisch. KI hat ja auch bereits unsere Sicherheitsbranche erreicht, denn, um nur ein Beispiel zu nennen, die ersten Roboter agieren bereits als Helfer im Wachschutz und in der Gebäudeinspektion. Sie sind nicht abgelenkt, können sehr viele Informationen gleichzeitig verarbeiten und werden im Einsatz niemals müde. Außer – der Akku ist leer.

Obwohl der Roboter seine Aufgaben zu 100 Prozent sicher und zuverlässig erfüllt, behält der Mensch derzeit noch die Kontrolle über ihn. Während der Roboter wacht, prüft und meldet, trifft der Mensch die ultimative Entscheidung und wird aktiv, wenn es sinnvoll und notwendig ist. Auf diese Weise wird moderne, KI-unterstützte Sicherheitsarbeit zu einer integrierten Teamlösung bestehend aus Mensch (Sicherheitsmitarbeiter) und Maschine.

So wäre KI sozialverträglich, ethisch vertretbar und somit auch in der Zukunft denkbar.

In diesem Sinne: Bleiben Sie auf der sicheren Seite!

Ihr
Holger Köster

Bild: Dieter Poschmann / pixelio.de

Automation und KI haben sich schon längst in der Industrie einen festen Platz erobert. Unser Bild zeigt einen Absetzroboter.

Künstliche Intelligenz: keine Zukunftsmusik, sondern schon längst Teil unseres Alltags

Von Klaus Henning Glitza

Niemand muss Terminator oder „Aufstand der Maschinen" gesehen haben, um Künstliche Intelligenz (KI) nicht zumindest ein bisschen unheimlich zu finden. Die Vorstellung, dass Maschinen intellektuelle Fähigkeiten des Menschen nachahmen oder gar übertreffen, ist vielen Zeitgenossen in nachvollziehbarer Weise ein Graus. Dabei ist KI keine Science-Fiction, sondern in bestimmten Varianten schon längst Teil unseres Alltags geworden. Auch im Wach- und Sicherheitsdienst haben KI-Anwendungen bereits ihren Platz gefunden.

Klaus Henning Glitza

Ehemaliger Redakteur der Hannoverschen Allgemeinen Zeitung, Träger des Deutschen Förderpreises Kriminalprävention (Stiftung Kriminalprävention, Münster) und seit 2003 als Fachjournalist für Sicherheitsfragen tätig

„Künstliche Intelligenz" ist nach einer Definition des Europäischen Parlaments „die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren". Das ist von der klassischen Automation, bei der praktisch im Sinne einer Dressur alle Schritte vorprogrammiert und angelernt sein müssen, zu unterscheiden. Eine KI-Anwendung kann, so ist es das Ziel, ähnlich einem Menschen sehen, hören und „fühlen", sprich: spüren und messen. Auf dieser Grundlage ist eine Maschine imstande, Muster und Schemata zu erkennen und zu verallgemeinern. Das befähigt sie, eine neue Situation einzuschätzen, aus Erfahrungen zu lernen und auf dieser Grundlage autonom zu entscheiden und zu handeln. Ohne dass sie dafür speziell programmiert werden muss. Entscheidend ist dafür Maschinelles Lernen (ML). Dabei werden laut SAP „Algorithmen darauf trainiert, Muster und Korrelationen in großen Datensätzen zu finden und auf Basis dieser Analyse die besten Entscheidungen und Vorhersagen zu treffen". Kurzum: Die lernende Maschine entwickelt sich selbstständig weiter. Dank neuronaler Netze, die dem menschlichen Gehirn nachempfunden sind. Das ist zumindest die noch ferne Vision von Forschenden, die aber nach Eigenaussagen diesem Endziel jeden Tag ein Stückchen näherkommen.

Wir merken: KI ist aber nicht unbedingt KI. Wir haben es heute weitestgehend mit einer teilautonomen Künstlichen Intelligenz zu tun. In dieser hat der Mensch seinen festen Platz. Die etwas irritierende Bezeichnung dafür ist „schwache KI". Damit werden Anwendungen bezeichnet, die den Menschen in Einzelbereichen unterstützen, ihm praktisch dienen. Menschen werden dadurch genau so wenig überflüssig wie Mathematiker, nur weil es Rechenmaschinen und Supercomputer gibt.

„Starke KI" steht für Systeme, die selbstständig auch komplexe Aufgaben meistern können, ohne dass zwingend ein Mensch dabei sein muss. Sie sind somit in der Lage, den Menschen zu ersetzen und/oder die Manpower insgesamt erheblich, bis in die Nähe der Nulllinie, zu reduzieren.

Eine nicht zu verkennende Problematik liegt darin, dass eine KI-Anwendung zwar ähnlich wie ein Mensch nach den Gesetzen der Logik handelt, aber dies quasi auf mathematischen Wegen. Das

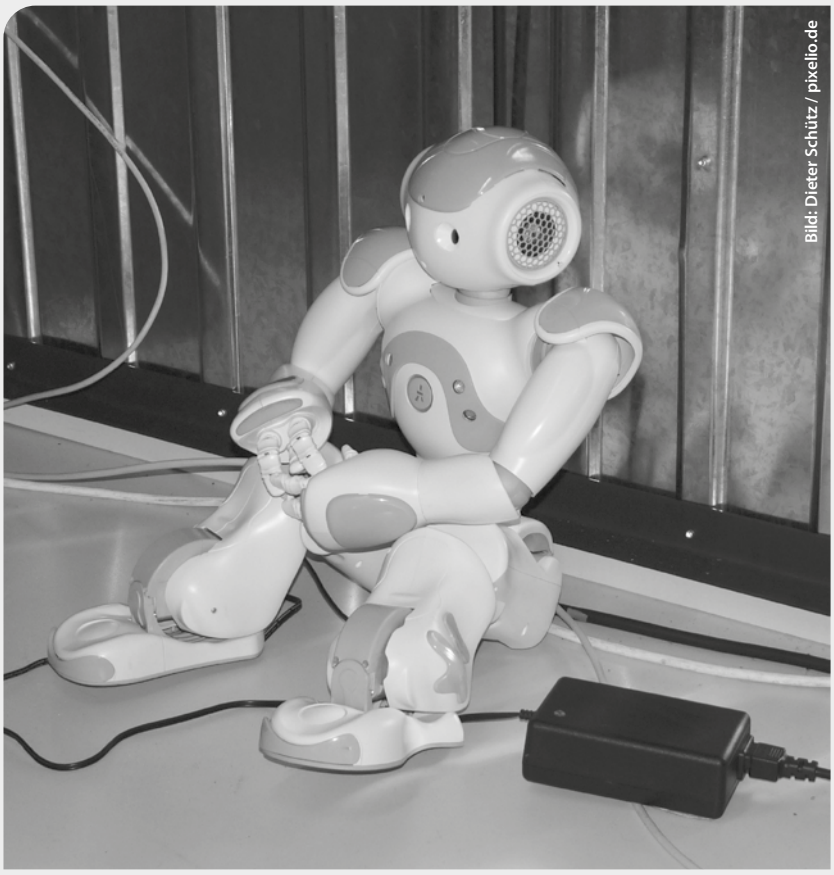


Bild: Dieter Schütz / pixelio.de

Ein müder Roboter? Das gibt es in der Hightech-Welt nicht. Es sei denn, der Akku ist leer.

„Hier ist ein Mensch und keine Maschine." Diese Botschaft hat ihren Hintergrund in ChatGPT, einem KI-gesteuerten Programm, das menschliche Sprache versteht und individuell darauf antworten kann. ChatGPT ist schon bei vielen Unternehmen im Einsatz.

Bild: Stefan Bayer / pixelio.de

heißt zum einen, dass dem Output eines Roboters nach gegenwärtigem Stand der Technik nichts von dem zugrunde liegt, was wir als Menschlichkeit betrachten. Wenn eine Maschine entscheidet, kann dies durchaus zu einer Diskriminierung führen. Und natürlich fehlerhaft sein, denn auch ein Roboter kann Daten fehlinterpretieren. Und die „kalten" Entscheidungen einer Maschine sind für Menschen nicht unbedingt nachvollziehbar. Was ihnen fehlt und wahrscheinlich auch nicht nachgerüstet werden kann, sind Gefühle, die immer in menschliche Entscheidungen einfließen – und das keineswegs nur zum Schlechten. Fatal für den menschlichen Teil eines Maschine-Mitarbeiter-Teams: Wie sich die Maschine entscheidet, ist nicht voraussehbar, da ihre Denkmuster sich von denen menschlicher Wesen diametral unterscheiden.

Menschen könnten in verzwickte Situationen kommen, wenn sie den Entscheidungen einer Maschine folgen. Die Frage stellt sich: Ist es letzten Endes beweisbar, wie sich der Roboter entschieden hat, zum Beispiel bei Zerstörung? Im Ergebnis haftet immer der Mensch, denn einen Gegenstand, auch wenn er smart ist und menschenähnlich denkt, kann niemand zur Rechenschaft ziehen. Folgt ein Mensch also der Maschine und haftet dafür eventuell höchstpersönlich oder trifft er eine eigene Entscheidung? KI kann Probleme lösen, aber auch Probleme generieren.

Ein weiterer negativer Aspekt ist das Faktum, dass Maschinen den Menschen verdrängen könnten. Und der Mensch letzten Endes als fühlendes, aber fehlbares Wesen in die zweite, wenn nicht dritte Reihe rückt. Das ist wohl das Hauptproblem, das diverse Skeptiker auf den Plan ruft.

Bild: www.helenesouza.com / pixelio.de

Ein Mensch am Lenkrad. Ein Bild mit Nostalgiecharakter, denn künftig sollen Kraftfahrzeuge dank KI autonom fahren. Der Mensch: nur noch ein Zuschauer. Dieser Ansatz wird am häufigsten mit der KI in Zusammenhang gebracht.

Doch nun zu der Frage, die noch spannender ist als die allgemeine Darstellung des KI-Prinzips. Nämlich: Welche Anwendungen gibt es in der Sicherheitsbranche bereits?

Hier sind in erster Linie smarte Roboter zu nennen, die sich als „unerschrockene Helfer im Wachschutz und in der Gebäudeinspektion" erweisen. Solche Systeme, in den USA konstruiert, aber in Deutschland auf Kundenbedürfnisse hin programmiert, bieten unter anderem hiesige Technologieunternehmen an. „Die neuen Mitarbeiter im Sicherheitsdienst sind dabei zuverlässig, belastbar, stets fokussiert und rundum vernetzt", wird nach Eigenangaben auf die Vorteile einer robotergestützten Lösung verwiesen. Nimmermüde und nie abgelenkt – die Wachkraft der Zukunft?

Stößt der „Robot-Dog" auf eine unbekannte Person auf dem Gelände oder eine andere Auffälligkeit (beispielsweise Tür/Fenster offen), sendet er Livebilder an die Leitstelle. Dabei folgt er keinem starren Programm, sondern nutzt dynamische Algorithmen, um aus jeder neuen Situation eigenständig zu lernen. Gibt die Leitstelle bei einem bestimmten Objekt Entwarnung, weil es sich beispielsweise um eine neue oder zusätzliche Maschine in der Produktionsstraße handelt, so erkennt der Roboter fortan dieses Objekt und schlägt nicht mehr Alarm, macht eines der Technologieunternehmen deutlich.

KI ist die „Seele" dieser vierbeinigen und laut Hersteller geländegängigen Laufroboter, die Hunden ähneln. Ganz wie die echten Vierbeiner können sie vor-, rück- und seitwärts gehen und Treppen steigen. Ausgestattet sind sie mit einer hochauflösenden 360-Grad-Rundumkamera, ultrahellem LED-Licht und einem Lichterkennungssystem (LiDAR), „das auf die Reflexion von elektromagnetischen Wellen setzt, um den Raum vor ihnen zu vermessen und abzubilden". So könne der Roboter „Menschen und Objekte erkennen und zuordnen, Veränderungen in der Umgebung wahrnehmen und auch Instrumente präzise ablesen", beschreibt einer der Anbieter die Leistungsmerkmale.

Ähnlich, nur ohne vierbeinige Robot-Wächter, funktionieren smarte Videoüberwachungssysteme. Sie können KI-basiert verdächtige Verhaltensmuster erkennen. Dadurch, dass beispielsweise Kleintiere von Eindringlingen und berechtigt abgestellte Gegenstände von fragwürdigen unterscheiden können, reduzieren sie Fehlalarme.

In der akuten Phase der COVID-19-Pandemie wurde verschiedentlich eine Screening-Plattform auf Basis einer industrietauglichen Infrarotkamera eingesetzt. Dieses System schaffte es, vollautomatisch und berührungslos die Körpertemperatur von Personen als Indikator einer COVID-Infektion

zu messen und zusammen mit weiteren Analysen mittels KI auszuwerten. Bei Mitarbeitenden, deren Daten bereits hinterlegt waren, dauerte das 20 Sekunden, bei Erstbesuchern eine Minute. Die Screening-Plattform hatte sich in Industriebetrieben, Krankenhäusern, Altenheimen und bei Veranstaltungen/Meetings bewährt. Nicht zuletzt wegen der kurzen Reaktionszeiten.

KI ist bereits heute integraler Bestandteil von Zutrittskontrollsystemen, die auf Fingerprints oder Personenerkennung basieren. Der bekannte Vorteil solcher Systeme: Fingerabdrücke und Gesichtszüge können weder verloren noch gefälscht werden. Auf diesem Gebiet kommt eine sich fortentwickelnde KI der wünschenswerten Perfektionierung eines Zutrittskontrollmanagements entgegen, das auf biometrischen Merkmalen basiert.

Die immer mehr zur Digitalisierung neigende Gebäudesicherheit kann relativ leicht um Wachschutzkomponenten erweitert werden. Das sind KI-basierte Systeme, die beispielsweise abweichende Temperaturen in Räumlichkeiten detektieren können. Die Messgenauigkeit ist so hoch, dass bereits ein Mensch, der sich außerhalb der Arbeitszeit in einem Büro bewegt, aufgrund seiner Wärmeabstrahlung erkannt wird.

Auch bei der Abwehr von IT-Bedrohungen kann KI überaus hilfreich sein. Konventionelle Virenscanner und Firewalls reagieren mehr oder minder zeitversetzt auf bereits aktive Schadprogramme. KI kann dagegen aufgrund bestimmter Muster, die den meisten Viren/Trojanern zu eigen sind, die Schädlinge identifizieren und abblocken. Diese vordergründig tolle Option hat jedoch einen gefährlichen Haken. KI kann auch, und vielleicht noch optimaler, für IT-Angriffe genutzt werden. So können zum Beispiel automatisiert Schwachstellen erkannt werden. Solche Programme sind nach zuverlässigen Angaben in kriminellen Kreisen bereits im Einsatz. Geld spielt dabei keine Rolle. Wir alle wissen, die Finanzkraft von Cybercrime-Strukturen lässt sich durchaus mit der von Konzernen vergleichen. Auf dem Gebiet der IT-Sicherheit ist KI somit Segen und Fluch zugleich.

Segen und Fluch – das zieht sich durch sämtliche denkbaren KI-Anwendungen im Sicherheitswesen. Ein Segen kann KI im Zeichen des Fachkräftemangels und der Personalnot sein. Ein Fluch ist sie dort, wo sie dazu dient, Menschen „wegzurationalisieren", respektive allzu viele Fragen offenlässt oder nicht nur der Sicherheit dient, weil sie auch Angreifern Mittel an die Hand gibt.

KI muss wohldosiert ein- und umgesetzt werden. Die Verlockungen der Technik hin und her. Der Mensch muss das Maß aller Dinge bleiben. An ihm muss sich alles orientieren. Das ist eine unabdingbare Voraussetzung für eine allseits kompatible und akzeptierbare KI.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

Verfassungsschutzbericht 2022

Im letzten Jahr gab es mehr politisch motivierte Straftaten. Die Anzahl linker Straftaten sank, rechts stieg sie an. Ebenso war ein Anstieg von Ermittlungsverfahren bei Spionagefällen zu verzeichnen. Diese richten sich gegen mutmaßliche Zuträger russischer, türkischer und marokkanischer Dienste. Die größte Bedrohung in Bezug auf Wirtschafts- und Wissenschaftsspionage bleibt aber China.

www.verfassungsschutz.de

eco-Umfrage zu fünf Jahren Datenschutz-Grundverordnung

78,4 Prozent der 2.500 Befragten nennen mindestens eine aktive Maßnahme zum Datenschutz. 49,7 Prozent schränken auf dem Smartphone die Berechtigungen von Apps ein. 40,2 Prozent konfigurieren ihren Internetbrowser, um ihre Daten zu schützen, und 35,2 Prozent nutzen soziale Medien bewusst mit Blick auf ihre persönlichen Daten.

www.eco.de

DsiN-Sicherheitsindex 2023

Der diesjährige DsiN-Sicherheitsindex zur Sicherheitslage von Verbrauchern im Netz fällt mit 57,2 Punkten auf den tiefsten Wert seit seiner ersten Erhebung vor zehn Jahren. Maßgeblich dafür ist der starke Anstieg von IT-Sicherheitsvorfällen um 11,2 Indexpunkte (+20 Prozent). Rund 56 Prozent der Menschen im Netz benötigen zusätzliche Hilfestellungen.

www.sicher-im-netz.de

TÜV Cybersecurity Studie 2023

Befragt wurden allein Verantwortliche für IT-Sicherheit bei 501 Unternehmen ab zehn Mitarbeitern in Deutschland. Elf Prozent der Unternehmen waren im vergangenen Jahr von einem IT- Sicherheitsvorfall betroffen. 57 Prozent fühlen sich von organisierten Hacker-Banden bedroht. Jeweils 27 Prozent sehen staatlich organisierte Wirtschaftsspionage oder politisch motivierte Akteure als große Gefahr.

www.tuev-verband.de

RA Dr. Berthold Stoppelkamp

zuständiges Geschäftsführungsmitglied für den BDSW-Arbeitskreis Wirtschaftsschutz

Eine Nationale Sicherheitsstrategie ohne Sicherheitsgewerbe?

Von Rechtsanwalt Dr. Berthold Stoppelkamp

RA Dr. Berthold Stoppelkamp

Geschäftsführer des Bundesverbandes der Sicherheitswirtschaft (BDSW) in Berlin

Im Berichtszeitraum Mai 2023 bis Juli 2023 bestimmten die Themen der Angriffskrieg auf die Ukraine, der Start der sog. Gegenoffensive der Ukraine, der sog. Aufstand in Russland, die Vorstellung der Nationalen Sicherheitsstrategie durch die Bundesregierung sowie der umfassende Schutz Kritischer Infrastrukturen (KRITIS) durch ein KRITIS-Dachgesetz die sicherheitspolitische nationale Diskussion und mediale Berichterstattung. Am 13. Juli 2023 hat das Kabinett erstmals eine China-Strategie für die Bundesregierung beschlossen. Diese verfolgt das Ziel, Deutschland nicht von China wirtschaftlich abzukoppeln, aber in Handelsbeziehungen zukünftig kritische Abhängigkeiten zu vermeiden. Diese sog. De-Risking-Strategie ist als zielführender Ansatz zum zukünftigen Umgang mit China zu charakterisieren. Zum KRITIS-Dachgesetz hat das BMI bereits Mitte Juli 2023 mit einem ersten Referentenentwurf die Ressortabstimmung eingeleitet. Dies erfolgte nach langem Warten nun endlich auch für das für die Sicherheitswirtschaft wichtige Sicherheitsgewerbegesetz (SiGG). Ende Juli wurde für beide Referentenentwürfe die Verbändebeteiligung eingeleitet. Ausgelöst durch Gewalttaten in Berliner Freibädern kam es im Juli zu einer bundesweiten heftigen Diskussion über die angemessenen Sicherheitsvorkehrungen in Freibädern. Dabei bestand am Ende der Diskussion bei Politik, Polizei, Bäderbetreibern und Schwimmmeistern Konsens, dass primär durch einen verstärkten Einsatz privater Sicherheitsdienste sich das Sicherheitsniveau in den Freibädern signifikant verbessern lässt.

Nationale Sicherheitsstrategie erblickt das Licht der Welt

Das Bundeskabinett hat erstmals in der Geschichte Deutschlands am 14. Juni 2023 eine Nationale Sicherheitsstrategie (NAS) beschlossen und durch den Bundeskanzler und vier weitere Minister und Ministerinnen (AA, BMVg, BMI und BMF) der Öffentlichkeit vorgestellt. Dabei ist nicht nur den sog. Sicherheitspolitikern klar, dass es kaum ein Politikfeld gibt, das so weit und umfassend gesehen werden kann wie die Sicherheitspolitik. Die Regierungsparteien hatten die Ausarbeitung der NAS bereits in ihrem Koalitionsvertrag für diese Legislaturperiode festgelegt. Die NAS orientiert sich dabei am Leitbild eines integrierten Sicherheitsbegriffes. Sie umfasst daher Bereiche der inneren und äußeren Sicherheit unter Berücksichtigung des Zusammenwirkens aller relevanten Akteure, Mittel und Instrumente, durch deren Ineinandergreifen die Sicherheit Deutschlands umfassend erhalten und gegen Bedrohungen von außen gestärkt wird. „Wehrhaft", „Resilient", „Nachhaltig" lauten die drei Themenblöcke der NAS. Die komplette NAS ist abrufbar unter:
www.bundesregierung.de/breg-de/aktuelles/nationale-sicherheitsstrategie-2195890

Mehr Licht als Schatten

Auch wenn es einige kritische Anmerkungen zur NAS aus dem politischen Raum bzw. seitens von Branchenverbänden gibt, so überwiegen doch – im politischen Raum – bezüglich der in der NAS aufgelisteten Sicherheitsrisiken und sicherheitspolitischen Handlungsfeldern weitgehend Zustimmung. Dabei versteht es sich von selbst, dass ein solches Papier bei drei die Bundesregierung stützenden Parteien und mehreren beteiligten Ministerien immer nur ein Kompromisspapier auf dem kleinsten gemeinsamen Nenner sein kann. Insofern fehlt es insgesamt an einer eindeutigen Priorisierung von Handlungsfeldern, konkreten Maßnahmen und Zielen. Kritisiert wird beispielsweise, dass man sich nicht auf einen sog. nationalen Sicherheitsrat, der ressortübergreifend für eine gemeinsame strategische außen-, sicherheits- und

verteidigungspolitische Linie Sorge trägt, einigen konnte. Hierfür hatte sich die FDP, aber auch die Opposition von CDU/CSU starkgemacht. Aber auch aus Sicht der Digitalwirtschaft wird kritisiert, dass der Fokus zu sehr auf die klassische Innen- und Außenpolitik gerichtet sei und insofern der Cyberraum zu sehr vernachlässigt werde. Damit verfehlt laut dem Branchenverband Bitkom die Strategie ihr Ziel, Deutschland wirklich sicher und resilient gegenüber künftigen Krisen und Kriegen zu machen – gerade auch mit Blick auf Formen hybrider Kriegsführung.

Sicherheitsgewerbe nur Mittel zum Zweck

Das Sicherheitsgewerbe bzw. der BDSW waren selbst nicht Teil des vom AA federführend im Vorfeld initiierten und organisierten Dialogprozesses für die Erstellung der NAS. Dies galt im Übrigen auch für alle Bundesländer, die trotz nachdrücklicher Aufforderung durch die Innenministerkonferenz (IMK) und originärer Zuständigkeit für Fragen der inneren Sicherheit, nicht von der Bundesregierung in den Entstehungsprozess der NAS eingebunden wurden. Insofern mussten BDSW-Anliegen direkt gegenüber dem AA bzw. gegenüber dem BMI eingebracht werden. Allerdings zeigt die NAS durch Nichterwähnung, dass die Bundesregierung dem Sicherheitsgewerbe – im Gegensatz zu den Feststellungen der IMK bzw. der ausdrücklichen, erstmaligen Feststellung im Koalitionsvertrag der 19. Legislaturperiode, dass private Sicherheitsdienste einen wichtigen Beitrag zur Sicherheit in Deutschland leisten – leider nach wie vor keine strategische Bedeutung für die Sicherheit Deutschlands einräumt.

Das Sicherheitsgewerbe wird vielmehr von der Bundesregierung nach wie vor allein als operativer Unterstützer für staatlich definierte Schutzziele (z. B. Sicherung der Bargeldversorgung) und staatliche Sicherheitsmaßnahmen (z. B. Luftsicherheit) oder als Unterstützer für den Schutz der Wirtschaft betrachtet. Insofern ist es aus Sicht des BDSW zumindest zu begrüßen, dass in der NAS der verstärkte Schutz von Wirtschaft und Wissenschaft, insbesondere von Kritischen Infrastrukturen einschließlich systemrelevanter Unternehmen vor Spionage und Sabotage, ob im physischen oder im digitalen Bereich, ausdrücklich Erwähnung findet. Hierzu soll laut NAS die nationale Wirtschaftsschutzstrategie weiterentwickelt werden. Wer, wenn nicht das Sicherheitsgewerbe allein, kann diesen Schutz mit seinen integrierten Sicherheitslösungen in Deutschland am besten gewährleisten.

Hingegen bekennt sich die Bundesregierung zu Recht in der NAS ausdrücklich zur Wettbewerbs- und Kooperationsfähigkeit der deutschen Sicherheits- und Verteidigungsindustrie innerhalb der EU und Europas sowie zum Ausbau derselben. Hierfür wird die Bundesregierung ihr Strategiepapier der Sicherheits- und Verteidigungsindustrie aktualisieren. Für die Verteidigungsindustrie dürfte es allerdings im Sinne von Planungssicherheit bedauerlich sein, dass die NAS nicht ansatzweise mit Haushaltsmitteln unterlegt wird.

Ausblick

In einer Gesamtschau ist die NAS zu begrüßen. Allerdings wäre es eine Illusion zu glauben, dass bei zukünftigen Krisen die Bundesregierung nur in die NAS schauen muss, um konkrete Schutzmaßnahmen für die Sicherheit Deutschlands zu ergreifen. Der BDSW wird sich, soweit das Sicherheitsgewerbe tangiert ist, in den weiteren Umsetzungsprozess der NAS einbringen. Ziel muss es sein, dass das Sicherheitsgewerbe zukünftig auch strategisch von der Bundesregierung für die Sicherheit Deutschlands einbezogen wird. Allein für das Sicherheitsgewerbe ein eigenes Gesetz zu schaffen, ist angesichts der gewachsenen Bedeutung des Sicherheitsgewerbes für den Schutz der Wirtschaft und für die öffentliche Sicherheit in Deutschland nicht ausreichend.

KURZ BELICHTET

Im Rahmen der Interessenvertretung für BDSW bzw. BDGW gab es im Berichtszeitraum (Mai 2023 bis Juli 2023) eine Vielzahl von Direkt- und Netzwerkkontakten in den parlamentarischen Bereich, die Leitungsebene von Ministerien, Sicherheitsbehörden, Wissenschaft bzw. zu Verbandspartnern.

Dialog mit der Politik zum Leistungsspektrum und zu Anliegen der Sicherheitswirtschaft
Josef Oster MdB, Obmann der CDU/CSU-Bundestagsfraktion im Innenausschuss (links), und BDSW-Geschäftsführer Dr. Berthold Stoppelkamp

Dialog zur Sicherung der Bargeldversorgung auch in Krisenfällen

Am 15. Juni 2023 veranstaltete die Deutsche Bundesbank in Berlin ein Symposium mit über 100 Teilnehmern aus Politik, öffentlicher Verwaltung, Finanzwirtschaft, Wertdienstleistern und Wissenschaft zum Themenkomplex „Sichere Bargeldversorgung – auch in der Krise". Nach einem Eingangsstatement nahm der Leiter der Berliner BDGW-Geschäftsstelle, Dr. Berthold Stoppelkamp, gemeinsam mit Vertretern von Deutscher Bundesbank, Wissenschaft und Forschung an der Podiumsdiskussion „Von der wissenschaftlichen Politikberatung zur konkreten Umsetzung" über die Implementierung von Handlungsempfehlungen des BASIC-Forschungsprojektes „Resilienz der Bargeldversorgung – Sicherheitskonzepte für Not- und Krisenfälle" teil, an dem auch die BDGW entscheidend mitgewirkt hatte. Dabei hob er die Leistungsfähigkeit und Bedeutung der Wertdienstleister für die Resilienz der Bargeldversorgung in Deutschland hervor. Zudem forderte er zur Stärkung der Rolle der Wertdienstleister im Bargeldkreislauf vom Gesetzgeber die Schaffung von Sonderrechten bei den täglichen Geld- und Wertdienstleistungen im Straßenverkehrsrecht, aber speziell auch für Not- und Krisenfälle wie beispielsweise die bevorrechtigte Zuteilung von Kraftstoffen.

Dr. Berthold Stoppelkamp, Leiter der Berliner BDGW-Geschäftsstelle

Podiumsdiskussion „Von der wissenschaftlichen Politikberatung zur konkreten Umsetzung": (vl.) Dr. Tim Stuchtey (BIGS Potsdam), Moderatorin Sissi Hajtmanek, Prof. Dr. Marcus Wiens (TU Bergakademie Freiberg), Dr. Berthold Stoppelkamp (BDGW) und Dr. Jelena Stapf (Deutsche Bundesbank)

BDSW und BDGW – Sicherheitspartner der Polizei

Im Rahmen der Sicherheitspartnerschaft Mecklenburg-Vorpommern fand am 4. Mai 2023 eine Lenkungsausschusssitzung in der IHK zu Rostock statt. Neben einer Bewertung der Sicherheitslage und Auswertung der Polizeilichen Kriminalstatistik 2022 standen Themen zur Sicherung der Bargeldinfrastruktur im Fokus der Sitzung.

(Vl.) Sandro Münse (Abteilungsleiter im LKA MV), Ass. jur. Doreen Wiesner-Damaschke (Referentin IHK zu Rostock) und Dr. Berthold Stoppelkamp (BDSW/BDGW)

Grundwissen für Brandschutzbeauftragte

Kompendium zur Aus- und Weiterbildung

Von Dr.-Ing. Wolfgang J. Friedl, Richard Boorberg Verlag (**www.boorberg.de**), 2023, 5. überarbeitete Auflage, 224 Seiten, 29,80 Euro, ISBN 978-3-415-07428-6

Die überarbeitete 5. Auflage des Brandschutzklassikers vermittelt in kompakter Form alles, was Brandschutzbeauftragte wissen müssen. Inhaltlich orientiert sich das Buch an der aktuellen Ausbildungsvorgabe DGUV-Information 205-003 vom Dezember 2020. Es eignet sich daher ideal zur Vorbereitung auf den Ausbildungslehrgang zum/zur Brandschutzbeauftragten.

Aus dem Inhalt:
- Rechtliche Grundlagen
- Brand- und Explosionslehre
- Baulicher Brandschutz
- Organisatorischer Brandschutz
- Anlagentechnischer Brandschutz
- Brandschutzmanagement

Der Autor Dr.-Ing. Wolfgang J. Friedl ist seit Jahrzehnten als Berater im Bereich des Brandschutzes tätig und verfügt über großes Fachwissen und viel Erfahrung. Er erläutert präzise und auf das Wesentliche konzentriert die Aufgaben von Brandschutzbeauftragten, ihre Qualifikation und juristische Verantwortung. Besonders hilfreich sind die zahlreichen Abbildungen, Grafiken, Tabellen und Piktogramme.

Das Werk enthält die Neuerungen der aktuellen ASR A2.2 vom Mai 2018 sowie ein umfassendes Stichwortverzeichnis. Mit kurzen Abschnitten und zusätzlichen Gliederungspunkten sind die einzelnen Kapitel besonders verständlich und übersichtlich gestaltet. Zu Beginn jedes Kapitels wird auf die Relevanz hingewiesen, die dem jeweiligen Thema in der schriftlichen Abschlussprüfung zukommt.

Prüfung für Brandschutzbeauftragte

800 Fragen und Antworten – Digitale Lernkartei

Von Dr.-Ing. Wolfgang J. Friedl, Gemeinschaftsprojekt der Brainyoo Mobile Learning GmbH und des Richard Boorberg Verlages, 29,80 Euro, ISBN 978-3-415-06794-3

Mit den digitalen Lernkarteikarten eignen Sie sich das notwendige Wissen für die Prüfung zum/zur Brandschutzbeauftragten einfach und effizient an. Alle Fragen und Antworten orientieren sich an der aktuellen Ausbildungsvorgabe DGUV-Information 205-003. Die Karteikarten enthalten überwiegend Multiple-Choice-Fragen sowie Fragen mit offenen Antwortfeldern und Fragen zu Abbildungen.

800 Prüfungsfragen und Antworten zu den Themen:
- Gesetze, Bestimmungen, Verordnungen, Vorschriften
- Brandlehre
- Brand-/Explosionsgefahren und Brandrisiken
- Baulicher Brandschutz
- Anlagentechnischer Brandschutz
- Handbetätigte Geräte zur Brandbekämpfung
- Organisatorischer Brandschutz
- Zusammenarbeit mit Behörden, Feuerwehren, Versicherungen
- Bebilderte Situationen
- Das Update enthält neben diversen Aktualisierungen und Ergänzungen neu eingefügte Fragen zur Brandgefahr bei Lithium-Ionen-Batterien.

Lernen leichtgemacht:
- Das Lernkartenset ist unabhängig von Zeit und Ort online sowie offline einsetzbar.
- Die Software passt sich dem individuellen Lerntempo der Benutzer an.
- Das steigert die Lernmotivation und damit den Lernerfolg.
- Einfach zu bedienen, auf mehreren Geräten einsetzbar, selbstsynchronisierend.
- Mit selbst erstellten Karteikarten lassen sich die Übungsaufgaben individuell ergänzen.

Die digitalen Karteikarten beinhalten die kostenlose Nutzung der wissenschaftlich erprobten Lernsoftware BRAINYOO zum effizienten Online-, Offline- und mobilen Lernen.

Wie sich die EU-Gesetzgebung zunehmend auf die Sicherheitswirtschaft auswirkt

Von Alexander Frank

Alexander Frank

Head of EU Affairs der CoESS – Confederation of European Security Services

www.coess.eu

Mit der Digitalisierung erlebt die Sicherheitswirtschaft eine Zeit des Wandels. Unternehmen integrieren zunehmend neue Technologien in ihre Dienstleistungen und verarbeiten dabei auch immer mehr Daten. Aber Achtung: Der Einsatz neuer Technologien wie Künstliche Intelligenz sowie Fragen des Datenaustauschs werden maßgeblich auf EU-Ebene reguliert. Für Unternehmen, die bei der Nutzung neuer Technologien für ihre Dienstleistungen ganz vorne mit dabei sein wollen, wird es daher immer wichtiger zu wissen, was in Brüssel passiert. Mit diesem Beitrag werfen wir einen Blick auf zwei der derzeit wichtigsten Dossiers: den EU Data Act und EU AI Act.

Der Einsatz neuer Technologien bei Sicherheitsdienstleistungen passt gut in das Konzept des „Neuen Sicherheitsunternehmens", das erstmals 2015 in einem entsprechenden Weißbuch von der CoESS und dem BDSW skizziert wurde. Neue Technologien wie KI und Drohnen können enorme Möglichkeiten zur Verbesserung der öffentlichen Sicherheit in Europa bieten, und zwar in Konvergenz mit und unter Kontrolle von Sicherheitsmitarbeitern.

Laut einer Umfrage, die im Rahmen des von der EU finanzierten INTEL-Projekts unter europäischen Sicherheitsunternehmen durchgeführt wurde, nimmt das „Neue Sicherheitsunternehmen" Gestalt an: Die Marktnachfrage nach neuen Sicherheitslösungen steigt langfristig – insbesondere in den Bereichen integrierte Videoüberwachung, Cybersicherheit, Datenanalyse und Drohnen.

Es ist wichtig zu beachten, dass viele dieser Technologien, wie KI und Drohnen, aber auch die Folgen ihres Einsatzes, z. B. beim Datenschutz und -austausch, zunehmend in Brüssel reguliert werden. Die Sicherheitsbranche muss daher ein Auge darauf haben, was auf EU-Ebene geschieht. Die CoESS als europäischer Vertreter der Sicherheitswirtschaft hat in dieser Hinsicht natürlich eine besondere Verantwortung, um sicherzustellen, dass die Gesetze von heute an die Sicherheitsdienstleistungen von morgen angepasst werden und den Unternehmen Rechtssicherheit bieten.

Das europäische Datengesetz (EU Data Act)

Ein in diesem Zusammenhang beispielhaftes Dossier, das die CoESS in den letzten zwei Jahren beschäftigt hat, ist der EU Data Act. Der von der Europäischen Kommission Anfang 2022 veröffentlichte Verordnungsvorschlag sollte Unternehmen dazu verpflichten, die Daten, die sie über ihre Dienstleistungen und Produkte sammeln, in Echtzeit auf elektronische Anfrage online und kontinuierlich mit ihren Kunden, und auf Anfrage mit Dritten, zu teilen. Aber ein Gesetzesvorschlag, der für einen Großteil von Branchen sinnvoll ist, hätte für die Sicherheitswirtschaft besorgniserregende Folgen gehabt.

In unserer Branche umgesetzt, wären Unternehmen verpflichtet gewesen, hochsensible Daten wie Alarmsignale, Videoüberwachungsmaterial oder operative Daten im Werttransport online in Echtzeit und ohne Beschränkungen mit ihren Kunden, und auf Anfrage mit Dritten, zu teilen. Die Aufhebung jeglicher Beschränkungen für die Weitergabe solch sensibler Daten, wie sie im ursprünglichen Vorschlag des EU Data Acts vorgesehen war, hätte zu erheblichen Sicherheitsrisiken für die Personen, Lieferketten, Organisationen und Infrastrukturen geführt, die unsere Unternehmen eigentlich schützen sollen.

Die CoESS sprach daher mit Parlamentariern und Vertretern der EU-Mitgliedstaaten, um dafür zu werben, dass der Rechtstext an die Realitäten in unserer Branche und an die Tätigkeiten von Sicherheitsunternehmen angepasst wird – mit Erfolg. Im Sommer 2023 einigten sich die EU-Institutionen auf einen Rechtstext, der Daten und Aktivitäten im Zusammenhang mit der öffentlichen Sicherheit vom Anwendungsbereich ausnimmt und zusätzliche technische und organisatorische Schutzmaßnahmen vorsieht, die Unternehmen einrichten können, wenn das Teilen von Daten zu Sicherheitsrisiken


Bild: Christian Lue / unsplash.com

führen würde. Dieser muss nun noch formell vom Europäischen Parlament und Rat angenommen werden.

Die europäische KI-Verordnung (EU AI Act)

Ein weiteres Dossier, das derzeit in Brüssel verhandelt wird, ist der sogenannte EU AI Act. Diesen sollten insbesondere Unternehmen im Auge behalten, die planen, KI-unterstützte Lösungen in ihre Dienstleistungen zu integrieren – z. B. bei der Zugangskontrolle und der Videoüberwachung, aber auch bei internen Prozessen.

Der Vorschlag für eine EU-KI-Verordnung wurde von der Kommission im April 2021 vorgelegt und seitdem sowohl von den EU-Mitgliedstaaten im Europäischen Rat als auch im Parlament diskutiert. Es ist der weltweit weitreichendste Versuch, die Entwicklung und den Einsatz von KI gesetzlich zu regeln.

Der Kommissionsvorschlag verfolgt einen risikobasierten Ansatz: Er verbietet den Einsatz bestimmter KI-Systeme und Anwendungsfälle. Am wichtigsten ist die Kategorie der sogenannten „hochriskanten" KI-Systeme und Anwendungsfälle, die in den Anwendungsbereich der künftigen Verordnung fallen. Im Sicherheitsbereich wären dies wohl zum Beispiel KI-Systeme in der Luftsicherheit und Fernüberwachung, KI-unterstützte Drohnen, sowie die Nutzung von KI in Bereichen des Personalmanagements.

Wenn ein Unternehmen solche Systeme entwickeln, vertreiben oder nutzen will, wird es in Zukunft mehrere Bestimmungen des EU AI Acts einhalten müssen – insbesondere Verpflichtungen in Bezug auf Risikomanagement, Daten-Governance, technische Dokumentation, Aufzeichnungspflichten, Transparenz, menschliche Aufsicht, Robustheit und Cybersicherheit.

Sowohl der Europäische Rat als auch das Parlament haben bereits wichtige Verbesserungen am Kommissionsvorschlag vorgenommen, die viele Forderungen der CoESS erfüllen, und somit die Rechtssicherheit des Texts deutlich erhöhen – z. B. welche Systeme in den Anwendungsbereich fallen. Darüber hinaus begrüßt die CoESS, dass beide Institutionen in ihren Änderungsanträgen klarstellen, dass die menschliche Aufsicht über „hochriskante" KI-Systeme nur Mitarbeitern übertragen werden soll, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen.

Der endgültige Rechtstext wird nun aktuell in den sogenannten „Trilogen" zwischen den EU-Institutionen verhandelt. Wie auch immer der konkrete Rechtstext am Ende aussehen mag, die Unternehmen müssen wissen, was sie in den nächsten Jahren zu beachten haben. Kohärenz mit bestehendem Recht und damit einhergehend ein angemessener Verwaltungsaufwand für Unternehmen sind enorm wichtig, um die Nutzung von KI zu fördern.

Wir als CoESS, aber auch die gesamte Sicherheitsgemeinschaft, spielen daher eine wichtige Rolle, um bereits heute das Bewusstsein für die Bedeutung der KI-Verordnung und seine möglichen künftigen Auswirkungen auf Unternehmen zu schärfen, die planen, diese Technologie in ihre internen Abläufe und Sicherheitsdienstleistungen zu integrieren.

Wechselwirkung zwischen nationaler und europäischer Ebene

Die Liste der Dossiers, die in Brüssel verhandelt werden und Auswirkungen auf die Sicherheitsbranche haben, ließe sich mit der EU-Drohnenstrategie 2.0 und der kürzlich verabschiedeten CER-Richtlinie, die derzeit in Deutschland umgesetzt wird, fortsetzen.

Aber bereits die Dossiers EU Data Act und AI Act zeigen, wie wichtig es für unsere Branche ist, den Gesetzgebungsprozess in Brüssel zu verfolgen – sowohl um Risiken für unsere Branche anzugehen, als auch um zukünftige Innovationen voranzutreiben. Innerhalb der CoESS übernimmt der Ausschuss für Fernüberwachung mit Experten aus ganz Europa die führende Rolle bei der ständigen Bewertung neuer Gesetzesvorschläge und Initiativen, die sich auf die künftige Integration von Technologien in Sicherheitsdienstleistungen auswirken.

Ebenso ist die kontinuierliche Arbeit mit unseren Mitgliedsverbänden auf nationaler Ebene entscheidend. Die Zusammenarbeit mit dem BDSW ist dabei vorbildlich, sowohl auf Vorstands- als auch Ausschussebene der CoESS. Die CoESS ist dabei auf den BDSW und seine deutschen Mitgliedsunternehmen angewiesen, um das notwendige technische Fachwissen bereitzustellen, während die CoESS eine Schlüsselrolle bei der Vertretung der Interessen der Branche in Brüssel und bei der Rückmeldung an die Basis spielt. Die derzeit laufende Zusammenarbeit im Rahmen des BDSW Fachausschusses Drohnen ist dafür ein exzellentes Beispiel.

Arbeitsrecht in Kürze

Von Rechtsanwältin Cornelia Okpara

RAin Cornelia Okpara

kommissarische Hauptgeschäftsführerin des Bundesverbandes der Sicherheitswirtschaft (BDSW)

Leiharbeit: gleiches Arbeitsentgelt – Abweichung durch Tarifvertrag

Bundesarbeitsgericht, Urteil vom 31. Mai 2023, AZ: 5 AZR

Von dem Grundsatz, dass Leiharbeitnehmer für die Dauer einer Überlassung Anspruch auf gleiches Arbeitsentgelt wie vergleichbare Stammarbeitnehmer des Entleihers haben („equal pay"), kann nach § 8 Abs. 2 AÜG ein Tarifvertrag „nach unten" abweichen mit der Folge, dass der Verleiher dem Leiharbeitnehmer nur die niedrigere tarifliche Vergütung zahlen muss. Ein entsprechendes Tarifwerk hat der Interessenverband Deutscher Zeitarbeitsunternehmen (iGZ) mit der Gewerkschaft ver.di geschlossen. Dieses genügt den unionsrechtlichen Anforderungen des Art. 5 Abs. 3 Richtlinie 2008/104/EG (Leiharbeits-RL).

Die Klägerin war aufgrund eines nach § 14 Abs. 2 TzBfG befristeten Arbeitsverhältnisses bei der Beklagten, die gewerblich Arbeitnehmerüberlassung betreibt, als Leiharbeitnehmerin in Teilzeit beschäftigt. Sie war im Streitzeitraum Januar bis April 2017 hauptsächlich einem Unternehmen des Einzelhandels als Kommissioniererin überlassen und verdiente zuletzt 9,23 Euro brutto/Stunde. Sie hat behauptet, vergleichbare Stammarbeitnehmer erhielten einen Stundenlohn von 13,64 Euro brutto, und mit ihrer Klage unter Berufung auf den Gleichstellungsgrundsatz des § 8 Abs. 1 AÜG bzw. § 10 Abs. 4 Satz 1 AÜG aF für den Zeitraum Januar bis April 2017 Differenzvergütung iHv. 1.296,72 Euro brutto verlangt. Sie hat gemeint, das auf ihr Leiharbeitsverhältnis kraft beiderseitiger Tarifgebundenheit Anwendung findende Tarifwerk von iGZ und ver.di sei mit Art. 5 Abs. 3 Leiharbeits-RL und der dort verlangten Achtung des Gesamtschutzes der Leiharbeitnehmer nicht vereinbar. Die Beklagte hat Klageabweisung beantragt und geltend gemacht, das Tarifwerk von iGZ und ver.di verstoße nicht gegen Unionsrecht, außerdem hat sie die Höhe der von der Klägerin behaupteten Vergütung vergleichbarer Stammarbeitnehmer des Entleihers mit Nichtwissen bestritten.

Die Vorinstanzen haben die Klage abgewiesen. Die Revision der Klägerin blieb vor dem Fünften Senat des Bundesarbeitsgerichts erfolglos. Um unionsrechtliche Fragen zu klären, hatte der Senat zunächst mit Beschluss vom 16. Dezember das Revisionsverfahren ausgesetzt und den Gerichtshof der Europäischen Union (EuGH) gemäß Art. 267 AEUV um Vorabentscheidung von Rechtsfragen im Zusammenhang mit der von Art. 5 Abs. 3 Leiharbeits-RL verlangten, aber nicht näher definierten „Achtung des Gesamtschutzes von Leiharbeitnehmern" ersucht. Diese hat der EuGH mit Urteil vom 15. Dezember 2022 (– C-311/21 – [TimePartner Personalmanagement]) beantwortet.

Nach Fortsetzung der Revisionsverhandlung hat der Senat heute die Revision der Klägerin als unbegründet zurückgewiesen. Die Klägerin hat keinen Anspruch auf gleiches Arbeitsentgelt, also auf ein Arbeitsentgelt, wie es vergleichbare Stammarbeitnehmer des Entleihers erhalten. Aufgrund des wegen der beiderseitigen Tarifgebundenheit auf das Leiharbeitsverhältnis Anwendung findenden Tarifwerks von iGZ und ver.di war die Beklagte nach § 8 Abs. 2 Satz 2 AÜG und § 10 Abs. 4 Satz 1 AÜG aF nur verpflichtet, die tarifliche Vergütung zu zahlen. Dieses Tarifwerk genügt, jedenfalls im Zusammenspiel mit den gesetzlichen Schutzvorschriften für Leiharbeitnehmer, den Anforderungen des Art. 5 Abs. 3 Leiharbeits-RL. Trifft der Sachvortrag der Klägerin zur Vergütung vergleichbarer Stammarbeitnehmer zu, hat die Klägerin zwar einen Nachteil erlitten, weil sie eine geringere Vergütung erhalten hat, als sie erhalten hätte, wenn sie unmittelbar für den gleichen Arbeitsplatz von dem entleihenden Unternehmen eingestellt worden wäre. Eine solche Schlechterstellung lässt aber Art. 5 Abs. 3 Leiharbeits-RL ausdrücklich zu, sofern dies unter „Achtung des Gesamtschutzes der Leiharbeitnehmer" erfolgt. Dazu müssen nach der Vorgabe des EuGH Ausgleichsvorteile eine Neutralisierung der Ungleichbehandlung ermöglichen. Ein möglicher Ausgleichsvorteil kann nach der Rechtsprechung des EuGH sowohl bei unbefristeten als auch befristeten Leiharbeitsverhältnissen die Fortzahlung des Entgelts auch in verleihfreien Zeiten sein. Anders als in einigen anderen europäischen Ländern sind verleihfreie Zeiten nach

deutschem Recht auch bei befristeten Leiharbeitsverhältnissen stets möglich, etwa wenn – wie im Streitfall – der Leiharbeitnehmer nicht ausschließlich für einen bestimmten Einsatz eingestellt wird oder der Entleiher sich vertraglich ein Mitspracherecht bei der Auswahl der Leiharbeitnehmer vorbehält. Das Tarifwerk von iGZ und ver.di gewährleistet die Fortzahlung der Vergütung in verleihfreien Zeiten. Außerdem hat der deutsche Gesetzgeber mit § 11 Abs. 4 Satz 2 AÜG für den Bereich der Leiharbeit zwingend sichergestellt, dass Verleiher das Wirtschafts- und Betriebsrisiko für verleihfreie Zeiten uneingeschränkt tragen, weil der Anspruch auf Annahmeverzugsvergütung nach § 615 Satz 1 BGB, der an sich abdingbar ist, im Leiharbeitsverhältnis nicht abbedungen werden kann. Auch hat der Gesetzgeber dafür gesorgt, dass die tarifliche Vergütung von Leiharbeitnehmern staatlich festgesetzte Lohnuntergrenzen und den gesetzlichen Mindestlohn nicht unterschreiten darf. Zudem ist seit dem 1. April 2017 die Abweichung vom Grundsatz des gleichen Arbeitsentgelts nach § 8 Abs. 4 Satz 1 AÜG zeitlich grundsätzlich auf die ersten neun Monate des Leiharbeitsverhältnisses begrenzt.

Streit über den Inhalt eines unstreitig zugegangenen Schreibens

Thüringer Landesarbeitsgericht, Urteil vom 7. Dezember 2022, AZ: 4 Sa 123/21

Weist eine Partei den Zugang einer Briefsendung bei der Gegenpartei nach und behauptet, Inhalt sei ein bestimmtes Schreiben (hier: Geltendmachung) gewesen, reicht einfaches Bestreiten des konkreten Inhaltes nicht aus; die Gegenpartei kann und muss erklären, welchen anderen Inhalt die Briefsendung gehabt haben soll.

Eine Krankenschwester, deren Arbeitsverhältnis sich nach dem Tarifvertrag für den öffentlichen Dienst (TVöD) richtete, hatte ihren Arbeitgeber auf eine tarifliche Jahressonderzahlung für 2019 verklagt. Gemäß einem auf den 23. April 2020 datierten Einlieferungsbeleg über die Aufgabe einer Briefsendung bei der Post mit einer bestimmten Sendungsnummer hatte die Krankenschwester ihrem Arbeitgeber ein Schreiben übersandt, und am folgenden 24. April 2020 hatte eine Angestellte des Arbeitgebers eine Briefsendung mit dieser Sendungsnummer angenommen. Die Krankenschwester behauptete, in der Briefsendung sei ein Schreiben gewesen, mit welchem sie den Arbeitgeber zur Auszahlung der Sonderzahlung für 2019 aufgefordert hatte. Das bestritt der Arbeitgeber und berief sich auf die sechsmonatige Ausschlussfrist gemäß § 37 Abs.1 Satz 1 Tarifvertrag für den öffentlichen Dienst (TVöD). Danach verfallen Ansprüche aus dem Arbeitsverhältnis, wenn sie nicht innerhalb einer Ausschlussfrist von sechs Monaten nach Fälligkeit schriftlich geltend gemacht werden. Dieses Argument überzeugte weder das Arbeitsgericht Nordhausen noch das Thüringer Landesarbeitsgericht (LAG), die den Arbeitgeber zur Zahlung verurteilten.

„Qualität funktional“ beschrieben: Preis oder Wirtschaftlichkeit?!

VK Südbayern; Beschluss vom 28. April 2023, AZ: 3194.Z3-3_01-22-57

Von Rechtsanwalt Alexander Nette

RA Alexander Nette, LL.M

NETTE Rechtsanwälte, Recklinghausen, ist Fachanwalt für Vergaberecht, Fachanwalt für Bau- und Architektenrecht sowie Lehrbeauftragter für Vergaberecht und Vertragsmanagement an der Westfälischen Hochschule. Er ist spezialisiert auf die Beratung von Bietern und öffentlichen Auftraggebern in Vergabe- und Nachprüfungsverfahren.

Weitere Informationen erhalten Sie unter:
www.vergaberecht.cc.

1. Sachverhalt

Im Rahmen eines EU-weiten offenen Verfahrens schreibt der Auftraggeber Dienstleistungen über Streamingdienste aus. Aufgeteilt in zwei Lose sollen in Los 1 die Erneuerung und der Betrieb einer Plattform für Liveübertragungen und in Los 2 die Verdolmetschung der Übertragung in Gebärdensprache realisiert werden. In den Bewerbungsbedingungen als Bestandteil der Vergabeunterlagen war festgelegt, dass das wirtschaftlichste Angebot zu 100 Prozent anhand der Angebotssumme pro Los ermittelt wird. Darüber hinaus waren insbesondere zu Los 1 Anforderungen definiert, die zu erfüllen waren; unter anderem sollten Maßnahmen für die Gewährleistung der Ausfallsicherheit sowie die technische Umsetzung der Plattform dargestellt werden. Auf eine entsprechende Nachfrage hin bestätigte der Auftraggeber, dass für den Zuschlag ausschließlich der Preis ausschlaggebend sein sollte, der Erfüllungsgrad der technischen Anforderungen werde nicht berücksichtigt. Einer der Bieter rügte dies als unzulässigen Verstoß gegen den Gleichbehandlungsgrundsatz. Der Verzicht auf einen Qualitätswettbewerb sei nachvollziehbar zu dokumentieren und von Nachprüfungsinstanzen auf Ermessensfehler zu überprüfen. Das Abstellen allein auf den Preis verhindere einen wirksamen Wettbewerb. Es sei nicht möglich, einen objektiven Vergleich der eingehenden Angebote vorzunehmen, da es sich nicht um standardisierte oder homogene Leistungen handle. Auch seien die qualitativen Leistungsanforderungen nicht detailgenau, erschöpfend und lückenlos festgelegt, sondern funktional beschrieben worden. Der Auftraggeber wies die Rüge als unbegründet zurück. Der Bieter stellte daraufhin einen Nachprüfungsantrag zur Vergabekammer.

2. Entscheidungsgründe

Die VK Südbayern weist den zulässigen Nachprüfungsantrag als unbegründet zurück. Sie führt aus, dass die Durchführung eines reinen Preiswettbewerbs keinen vergaberechtlichen Bedenken begegnet. § 127 Abs. 1 Satz 4 GWB i. V. m. § 58 Abs. 2 VgV sehe vor, dass neben dem Preis weitere Aspekte berücksichtigt werden könnten. Der Preis oder die Kosten dürften jedoch auch das alleinige Zuschlagskriterium sein. Maßgeblich sei die Sicht des Auftraggebers dahingehend, wie sich das beste Preis-Leistungs-Verhältnis bestimme. Entscheidend sei, wie der konkrete öffentliche Auftraggeber die wirtschaftlich beste Lösung beurteile. Die Überprüfung der Vergabekammer beschränke sich darauf festzustellen, dass der Sachverhalt zutreffend und vollständig

ermittelt wurde, Verfahrensgrundsätze eingehalten wurden, keine sachwidrigen Erwägungen in die Entscheidung eingeflossen seien und die zu berücksichtigenden Gesichtspunkte angemessen und vertretbar gewichtet wurden. Unter dieser Voraussetzung hat die Vergabekammer geprüft, ob die Festlegung auf den Preis als alleiniges Zuschlagskriterium im konkreten Fall das dem Auftraggeber zustehende Ermessen überschritten hatte. Zur Begründung für das Abstellen auf den Preis hatte der Auftraggeber ausgeführt, dass hinsichtlich der technischen Lösung bestimmte Mindestanforderungen zu erfüllen seien, jedoch eine Bewertung der Qualität darüber hinausgehender technischer Lösungen nicht zielführend sei. Darüber hinaus sei der Auftraggeber zur sparsamen Mittelverwendung verpflichtet und unter diesem Gesichtspunkt sei die Entscheidung getroffen worden, ausschließlich auf den Preis abzustellen unter Berücksichtigung technischer Mindestanforderungen, die jedenfalls erfüllt sein mussten. Diese Begründung lässt nach Auffassung der Vergabekammer erkennen, dass sich der Auftraggeber bewusst war, dass qualitative Unterschiede vorhanden sein könnten, die bei der Wirtschaftlichkeitsbetrachtung außer Acht bleiben würden. Es sei erkennbar, dass der Auftraggeber im Rahmen der gesetzten Anforderung(en) das günstigste System erwerben wollte. Dies sei von den Ermessensentscheidungen des Auftraggebers gedeckt. Es handle sich hier um eine Entscheidung, die im Rahmen des Leistungsbestimmungsrechtes des Auftraggebers zutreffend sei und durch die Vergabekammer letztlich nicht überprüft werden könne.

Die Vergabekammer führt weiter aus, dass sich das im Bereich der Bauvergaben im Anwendungsbereich der VOB/A geltende Regel-Ausnahmen-Verhältnis für konstruktive und funktionale Leistungsbeschreibungen nicht auf den Bereich der Liefer- und Dienstleistungen übertragen lasse. § 31 VgV begreife die Abfassung der Leistungsbeschreibung über Leistungs- oder Funktionsanforderungen oder eine Beschreibung der zu lösenden Aufgabe als gleichwertige Alternativen. Auch im Falle einer funktionalen Ausschreibung bleibe es daher beim Grundsatz, dass der Preis das alleinige Zuschlagskriterium sein kann.

Bild: # 1319879300 / istockphoto.com

Die Vergabekammer führt jedoch ausdrücklich aus, dass dies anders gesehen werden könne, wenn und soweit bei der Ausarbeitung der Angebote bestehende Gestaltungsspielräume zu qualitativ unterschiedlichen Lösungen führen können und dies für den Auftraggeber objektiv auf Basis der festgelegten Zielvorgaben einen Mehrwert bedeute. In diesem Fall sei der Auftraggeber hingegen verpflichtet, auch nicht preisliche Zuschlagskriterien festzulegen, um diese unterschiedlichen Qualitätsniveaus im Rahmen der Beurteilung des Preis-Leistungs-Verhältnisses zu bewerten.

Vorliegend wird der Nachprüfungsantrag jedoch unbegründet zurückgewiesen, der Abschluss des Vergabeverfahrens auf der Grundlage der reinen Preisbeurteilung in diesem Fall bestätigt.

3. Praxishinweise

Die Entscheidung zeigt, dass das Leistungsbestimmungsrecht des Auftraggebers weit zu fassen ist und die Vergabekammer nur eingeschränkte Überprüfungsmöglichkeiten hat. Für den Fall, dass der Auftraggeber ausschließlich auf einen (reinen) Preiswettbewerb setzt, muss jedoch das von ihm als ausreichend beurteilte Qualitätsniveau eindeutig bestimmt sein. Sobald der Auftraggeber zum Ausdruck bringt, dass er auch ein höheres Qualitätsniveau grundsätzlich wünscht, muss er dies im Rahmen der Zuschlagsentscheidung auch berücksichtigen. Insofern lohnt sich im Rahmen der Kalkulation eine eingehende Prüfung der Vergabeunterlagen, wenn eine funktionale Leistungsbeschreibung – wie häufig im Dienstleistungsbereich – vorliegt und das Zuschlagskriterium ausschließlich der Preis sein soll. Im Rahmen von Bieterfragen oder ggf. Rügen kann bzw. sollte dann geklärt werden, welches Mindestniveau an Qualität konkret geschuldet sein soll. Gegebenenfalls kann dem Auftraggeber auch aufgezeigt werden, dass eine Bewertung von Qualitätskriterien einen Vorteil bringt. Einen Anspruch auf Berücksichtigung weiterer Kriterien neben dem Preis hat der Bieter jedoch aktuell nicht in jedem Fall.

SÉCURITÉ ALLEMANDE FRANÇAISE

Auslandserfahrung in der Berufsausbildung

Von Angelika Böttcher

Angelika Böttcher

Bildungsgangleitung Schutz und Sicherheit an der Berufsbildenden Schule Hannah Arendt/ Bildungszentrum der Region Hannover für Wirtschaft und Verwaltung, Hannover

Drei Wochen fand im November 2022 und März 2023 erneut der deutsch-französische Austausch zwischen der Lycée Professionnel Le Marais Sainte Thérèse und der BBS Hannah Arendt bei den Service- und Fachkräften für Schutz und Sicherheit statt.

Vielfältige Einblicke in die französische Sicherheitsbranche

Am 20. November 2022 sind zehn Auszubildende der BBS Hannah Arendt bis zum 9. Dezember nach Saint-Étienne aufgebrochen, um sich fachlich, sprachlich und vor allem persönlich weiterzuentwickeln.

In diesem Jahr wartete in der ersten Woche neben dem Sprachkurs auch wieder ein abwechslungsreiches Programm auf die deutschen Gäste. So ging es unter anderem zu einer Führung in das Atomkraftwerk Bugey, in das Minenmuseum in Saint-Étienne und in eine der vielen, in Saint-Étienne ansässigen, Chocolaterien.

An dem darauffolgenden Montag begann der zweite Teil des Aufenthalts: das Praktikum in einem französischen Sicherheitsunternehmen. Dabei lernten die Auszubildenden trotz Sprachbarrieren viel über den Arbeitsalltag in Frankreich. Sie entdeckten Gemeinsamkeiten und Unterschiede im Berufsfeld und trafen auf viele offene Menschen, die sie an ihrem beruflichen Alltag teilhaben ließen: Von Museumssicherheit über die Bewachung von Einkaufszentren, den Veranstaltungsschutz bis hin zur Police Municipal war alles dabei.

Neben der Praktikumszeit haben die Auszubildenden an den Wochenenden Lyon erkundet, den Weihnachtsmarkt besucht oder ein Feuerwerk anlässlich des Sankt Barbara Festes bestaunt, welches jährlich an die Bergbauvergangenheit von Saint-Étienne erinnert.

Praxis hautnah im deutschen Sicherheitsdienst

Vom 5. bis zum 25. März kamen dann 21 französische Schülerinnen und Schüler nach Hannover und sind in die Arbeitswelt eines deutschen Sicherheitsunternehmens eingetaucht.

Der Austausch begann mit einer vielfältigen Kulturwoche zur Vorbereitung auf die Arbeitswelt in den zweiwöchigen Betriebspraktika. Neben dem täglichen Deutschsprachkurs haben die französischen Gäste spannende Einblicke in die Arbeit der mechanischen Sicherung bei der Polizei erhalten. Zudem standen verschiedene fachliche Exkursionen an: Es gab eine Führung durch die ZAG Arena und Heinz-von-Heiden-Arena. Dort erhielten die Gäste einen besonderen Einblick in den Veranstaltungsschutz. Die Besichtigung des Flughafens Hannover und der Niedersächsischen Wach- und Schließgesellschaft zeigte, wie vielfältig die Sicherheitsbranche ist.

Mit den vielen neuen Eindrücken aus der ersten Woche starteten die französischen Schülerin-

nen und Schüler in die Praktika bei: ISS Communication Services, Kieler Wach- und Sicherheitsgesellschaft, Protec, Tosa Security & Service, SDS J. Sinen GmbH, WAKO Nord, InSight Security und POWER PERSONEN-OBJEKT-WERKSCHUTZ GMBH. Aufgeteilt auf die acht teilnehmenden Unternehmen sammelten die Gäste zwei Wochen lang Arbeitserfahrungen und exklusive Einblicke in die unterschiedlichsten Bereiche. „Dieser eindrucksvolle Austausch ist nur mit der Unterstützung der verschiedenen Betriebe möglich!", bedankt sich Bildungsgangleiterin Angelika Böttcher.

ProTandem machts möglich

Träger des Austausches ist das deutsch-französische Programm ProTandem, das sich auf Partnerschaften in der Ausbildung beider Länder spezialisiert hat. Mit diesem Betriebspraktikum bieten die Unternehmen nicht nur kulturelle und sprachliche Möglichkeiten, sondern steigern auch die Attraktivität ihres Unternehmens. Beide Seiten wachsen an interkulturellen Kompetenzen und neue Perspektiven entstehen mit dem Blick über den Tellerrand. Das ist auch weiterhin das Ziel der deutsch-französischen Agentur ProTandem und der BBS Hannah Arendt: Förderung des Austauschs in der beruflichen Bildung, um Mobilität, Bildung und Selbstbewusstsein zu stärken. Bereits seit 2018 besteht diese Partnerschaft, die auch zukünftig weiter ausgebaut werden soll.

BBSHA Berufsbildende Schulen Hannah Arendt

PRO TANDEM

ISS COMMUNICATION SERVICES

KWS SICHERHEIT

POWER PERSONEN-OBJEKT-WERKSCHUTZ GMBH

SDS J. Sinen GmbH Sicherheits- und Dienstleistungs-Unternehmen in Schaumburg

protec service

WKO

primetec security · facility · services

ToSa SECURITY & SERVICE

LM Le Marais · St Thérèse

InSight Sicherheitsdienst · Detektei · Personaldienste

www.insight-security.de

ZAG arena

Gregor Lehnert feiert 70. Geburtstag

Am 20. Juli feierte der Präsident des BDSW, Gregor Lehnert, seinen 70. Geburtstag. „Im Namen des Präsidiums, des Vorstandes, aller Mitglieder des Verbandes und der Geschäftsführung gratuliere ich Gregor Lehnert recht herzlich zu seinem Ehrentag“, sagte Cornelia Okpara, kommissarische BDSW-Hauptgeschäftsführerin, in Bad Homburg. „Wir wünschen ihm persönlich alles Gute, vor allem aber eine gute Gesundheit.“

Gregor Lehnert wurde am 16. Mai 2013 in der Hansestadt Lübeck als Nachfolger von Wolfgang Waschulewski zum neuen Präsidenten gewählt. Am 18. Mai 2017 wählten ihn die Mitglieder des Verbandes in Berlin erneut, eine weitere Wiederwahl erfolgte am 8. Oktober 2021 in Saarbrücken. Durch seinen Vorsitz in der BDSW-Landesgruppe Rheinland-Pfalz/Saarland von 2004 bis 2021 war er bereits Mitglied im Vorstand des BDSW. Im Mai 2010 wurde er in Mainz zum Vizepräsidenten des Verbandes gewählt. Seit November 2013 ist er Mitglied des Präsidiums der Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA).

„Gregor Lehnert hat den Verband in den vergangenen zehn Jahren mit großer Weitsicht und Durchsetzungskraft geführt, wobei auch Krisen, wie die Pandemie, gut überstanden wurden“, sagte Okpara. Hier, wie auch in der Flüchtlingssituation 2015/16, habe sich die Flexibilität und Leistungsfähigkeit der Branche deutlich gezeigt.

„Wir sind stolz, eine auf der politischen und wirtschaftlichen Ebene so erfahrene und erfolgreiche Persönlichkeit als Präsidenten des BDSW zu haben. Wir wünschen Gregor Lehnert für seine weitere Arbeit als Präsident des Verbandes, aber auch als Unternehmer viel Erfolg“, so Okpara abschließend.

Gerhard Basko im Alter von 78 Jahren verstorben

Der ehemalige Vorsitzende der Landesgruppe Thüringen Gerhard Basko ist am 20. Juni im Alter von 78 Jahren gestorben. „Mit Gerhard Basko verlieren wir eine große Persönlichkeit, die die Verbandspolitik des BDSW in Thüringen maßgeblich mitgeprägt hat“, würdigte BDSW-Präsident Gregor Lehnert den Verstorbenen. „Unsere Gedanken sind bei seinen Angehörigen“, sagte er weiter.

Gerhard Basko wurde am 27. November 2007 zum Vorsitzenden der Landesgruppe Thüringen im BDSW und damit zum Nachfolger von Karl Rohrberg gewählt. Er hatte dieses Amt bis zum 25. Juni 2015 inne. Bereits vorher war er als Mitglied der Tarifkommission und des Landesgruppenvorstandes in der Landesgruppe aktiv. Gerhard Basko war bis zum 31. Juli 2015 Geschäftsführer der VSU Bewachungs- und Sicherheitsunternehmen GmbH Thüringen, Erfurt.

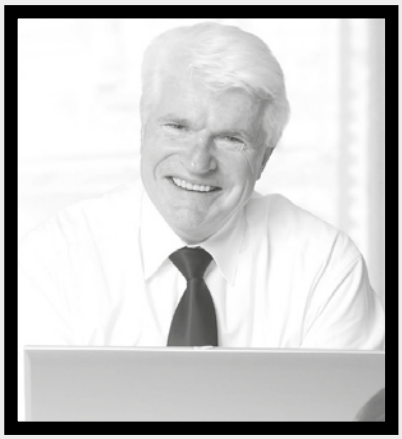
„Der BDSW, seine Mitglieder und Mitarbeiter trauern um einen engagierten Tarifpolitiker und ehrenamtlichen Verbandsvertreter“, sagte Lehnert abschließend. „Wir werden sein Engagement und seine positive Lebenseinstellung vermissen.“

Uwe-Dirk Uhlig ist verstorben

Im Alter von 81 Jahren ist am 9. August der ehemalige Vorsitzende der BDGW, Vizepräsident des BDSW und Vorsitzende der Landesgruppe Bayern des BDSW verstorben. „Uwe-Dirk Uhlig hat die Arbeit beider Verbände über Jahrzehnte geprägt", sagten Gregor Lehnert, Präsident des BDSW, und Michael Mewes, Vorsitzender der BDGW.

„Sein Tod reißt eine große Lücke." Aufgrund seiner vielfältigen Aktivitäten und großen Verdienste um das ‚Wohl der Allgemeinheit' bekam Uhlig vom Bundespräsidenten das Bundesverdienstkreuz am Bande verliehen. In Bayern, der zweitgrößten Landesgruppe des BDSW, wurde er zum Ehrenvorsitzenden ernannt. „Neben seinem Engagement und seinem Fachwissen wurde Herr Uhlig wegen seines freundlichen Wesens und seiner menschlichen Art von seinen Kollegen in beiden Verbänden hochgeschätzt", sagten Lehnert und Mewes weiter.

Uwe-Dirk Uhlig wurde am 12. Juli 1942 in Berlin geboren. Nach beruflichen Stationen in Kornwestheim, Stuttgart und Kirchheim/Ufr. wurde er am 1. Januar 1985 Geschäftsführer der Nürnberger Wach- und Schließgesellschaft. Von Beginn an engagierte er sich auch in der Verbandsarbeit. Er war über 25 Jahre Mitglied der Tarifkommission der BDSW-Landesgruppe Bayern. In den Vorstand wurde er 1992 gewählt, von 1998 bis 2010 war er Vorsitzender der zweitgrößten Landesgruppe des Verbandes. In dieser Eigenschaft leitete er auch die Tarifkommission.



Am 9. Mai 1995 wurde Uhlig in Saarbrücken in das BDWS-Präsidium gewählt, nach fast 15 Jahren trat er am 6. Mai 2010 nicht mehr zur Wiederwahl an. Auch in der Bundesvereinigung Deutscher Geld- und Wertdienste e. V. war Uhlig äußerst aktiv. Im Jahr 1992 wurde er zum stellvertretenden BDGW-Vorsitzenden gewählt. Von 2002 bis 2005 war er Vorsitzender.

Neben der ehrenamtlichen Tätigkeit für BDSW und BDGW engagierte sich Uhlig u. a. im Bayerischen Verband für Sicherheit in der Wirtschaft, in diversen Gremien der IHK Nürnberg sowie im Wirtschaftsbeirat der Union.

Seit dem 1. Januar 2011 war Uwe-Dirk Uhlig im Ruhestand. „Die Verbände BDSW und BDGW, ihre Mitglieder und Mitarbeiter trauern um einen großartigen Menschen, einen engagierten Tarifpolitiker und ehrenamtlichen Verbandsvertreter. Wir sind mit unseren Gedanken bei seiner Familie", endeten die Vertreter der Verbände.

Erfolgreicher Messeauftritt bei der SicherheitsExpo in München

Bereits zum vierten Mal war der Bundesverband der Sicherheitswirtschaft (BDSW) auf der SicherheitsExpo in München (28./29. Juni 2023) mit einem gemeinsamen Messestand mit dem BVSW vertreten.

Während der beiden Messetage konnten die Vertreter des BDSW-Landesgruppenvorstandes Bayern und der BDSW-Geschäftsstelle viele interessante Gespräche führen, bestehende Kontakte vertiefen und neue knüpfen.

(Vl.) Maximilian Kammermeier, Klaus Winkler, Gerhard Ameis, Innenminister Joachim Herrmann, Andreas Paulick und Ernst Steuger

„Wir blicken auf einen für uns äußerst erfolgreichen Messeauftritt bei der SicherheitsExpo in München zurück und freuen uns schon heute auf die nächstjährige Messe“, so RA Andreas Paulick, Geschäftsführer des BDSW.

BDSW trifft Innenminister Joachim Herrmann auf der SicherheitsExpo in München

Am Eröffnungstag der SicherheitsExpo 2023 trafen die anwesenden Vertreter des BDSW-Landesgruppenvorstandes Bayern und der BDSW-Geschäftsführung den Bayerischen Innenminister Joachim Herrmann beinahe schon traditionell auf ihrem Messestand.

Thema des Gesprächs war u. a. die Kooperationsvereinbarung der privaten Sicherheitswirtschaft in Bayern mit dem Bayerischen Staatsministerium des Innern. Herr Herrmann lobte die stetige Entwicklung der Kooperationsvereinbarung, die aus seiner Sicht einen bedeutenden Beitrag zur Stärkung der Inneren Sicherheit in Bayern leistet.

Gerhard Ameis (links) und Andreas Paulick

Werner Landstorfer (links) und Andreas Paulick

Tanja Staubach (links) und Andreas Paulick

(Vl.) Gerhard Ameis, Maximilian Kammermeier, Andreas Paulick und Klaus Winkler

Bayerischer Sicherheitstag

17./18. Oktober 2023 in München

Zum 9. Mal veranstalten der Bayerische Verband für Sicherheit in der Wirtschaft e. V. (BVSW) und der Bundesverband der Sicherheitswirtschaft e. V. (BDSW) den **Bayerischen Sicherheitstag**, bei dem wir Sie über verschiedenste Sicherheitsthemen informieren möchten.

Das Thema Sicherheit ist äußerst facettenreich und betrifft sowohl unseren privaten als auch unseren geschäftlichen Bereich. Auch die Politik legt großen Wert auf dieses Thema, da es soziale, wirtschaftliche und ökologische Aspekte umfasst. Gleichzeitig möchten wir Ihnen die Möglichkeit bieten, sich zu vernetzen und den Sicherheitsgedanken innerhalb der gesamten Community voranzutreiben.

Der Bayerische Sicherheitstag ist hierfür eine besonders gute Gelegenheit!

Wir freuen uns darauf, Sie am Bayerischen Sicherheitstag begrüßen zu dürfen und gemeinsam einen interessanten und außergewöhnlichen Tag zu erleben.

Sichern Sie sich jetzt
Ihren Platz unter
www.bayerischer-sicherheitstag.com

BAYERISCHER SICHERHEITSTAG München

Nürnberger Wach- und Schließgesellschaft feiert aus guten Gründen

Gregor Lehnert (links) und Gerhard Ameis

Videobotschaft des Bayerischen Staatministers für Inneres, Sport und Integration, Joachim Herrmann, MdL

Wichtige Ereignisse verlangen nach einem angemessenen Rahmen. 2022 beging die 1902 gegründete Nürnberger Wach- und Schließgesellschaft ihr 120-jähriges Bestehen, sagte aber den geplanten Festakt in Verantwortung für die Gesundheit der Gäste und Mitarbeiter aufgrund der damaligen Coronalage ab. „Aufgeschoben ist nicht aufgehoben" – selbstverständlich wurde dieses Versprechen gehalten, zumal die Firmenchronik 2023 ein weiteres wichtiges Ereignis aufweist: Der seit mehr als 25 Jahren bewährte Vorsitzende der Geschäftsführung, Gerhard Ameis, feierte im Juni seinen 60. Geburtstag.

120 Jahre NWS im Jahr 2022 und der 60. Geburtstag von Herrn Gerhard Ameis 2023 – das schienen mehr als angemessene Gründe, um auf Wunsch von Gerhard Ameis gemeinsam mit Kunden, Partnern und Mitarbeitern aller zur NWS-Gruppe zugehörigen Unternehmen zu feiern. Bei hochsommerlichen Temperaturen empfing der Gastgeber gemeinsam mit dem Inhaber und geschäftsführenden Gesellschafter Peter Stern, nebst Frau Robyn und seinen Geschäftsführungskollegen im Park des Faber-Castell'schen Schlosses in Stein bei Nürnberg. Zahlreiche namhafte Vertreter aus Wirtschaft, Politik haben es sich nicht nehmen lassen, persönlich zu gratulieren.

Den Auftakt zu den Feierlichkeiten im Ballsaal des Schlosses bildete die beeindruckende Videobotschaft des Bayerischen Staatsministers für Inneres, Sport und Integration, Joachim Herrmann, MdL, in der er sehr persönlich auf die zahlreichen Verdienste von Gerhard Ameis und der Nürnberger Wach- und Schließgesellschaft einging.

Auch die anwesenden Redner Dr. Michael Fraas (berufsmäßiger Stadtrat sowie Wirtschafts- und Wissenschaftsreferent der Stadt Nürnberg), Gregor Lehnert (Präsident des BDSW), Johannes Strümpfel (Vorstandsvorsitzender des BVSW) und Norbert Streveld (Vorstandsvorsitzender des Senats der Wirtschaft) lobten die erfolgreiche Führung der Nürnberger Wach- und Schließgesellschaft, sparten nicht an Anerkennung für Gerhard Ameis als eine der herausragenden Persönlichkeiten der bayerischen Wirtschaft und der Branche.

Bei der Mitgliederversammlung des BDSW in Berlin im Jahr 2017 wurde Gerhard Ameis erstmals zum Vizepräsidenten gewählt. Von 2013 bis 2022 war er außerdem Vorsitzender der Landesgruppe Bayern, nachdem er schon zuvor jahrelang in verschiedenen Positionen für die Landesgruppe tätig war. Bereits seit 2002 ist er aktives Mitglied der Tarifkommission Bayern und hat zahlreiche Verhandlungsrunden mit der Gewerkschaft begleitet und seine Meinung eingebracht.

Neben diesen Tätigkeiten hat er maßgeblich an der Organisation und Durchführung der Bayerischen Sicherheitstage mitgewirkt, die mittlerweile zum neunten Mal stattfinden. Diese Tage dienen als Plattform, um aktuelle Herausforderungen im Bereich der Sicherheit zu diskutieren und passende Lösungsansätze zu finden.

Gerhard Ameis hat das Präsidium und die Landesgruppe zu zahlreichen Anlässen vertreten,

Dr. Michael Fraas

Johannes Strümpfel

Gerhard Ameis (links) und Norbert Streveld

sowohl innerhalb des Verbands als auch gegenüber Behörden und anderen Institutionen. Dadurch konnte er die Interessen der Sicherheitswirtschaft als Ganzes und die Interessen der bayerischen Unternehmen im Besonderen stärken.

2010 übernahm er sein erstes offizielles Amt im Bayerischen Verband für Sicherheit in der Wirtschaft als Kassenprüfer. Verantwortungsvoll und gewissenhaft überwachte er die finanziellen Angelegenheiten des Verbandes bis 2013, als er in den Vorstand gewählt wurde. Seitdem prägt Gerhard Ameis mit seiner herausragenden Expertise und seinem hohen persönlichen Engagement die Geschicke des Verbandes maßgeblich mit. Ein wichtiger Meilenstein seiner Arbeit war die Kooperationsvereinbarung zwischen der Bayerischen Polizei und der privaten Sicherheitswirtschaft, die das Land Bayern bis heute dabei unterstützt, ein hohes Sicherheitsniveau zu halten. Durch diese Zusammenarbeit können Gefahren frühzeitig erkannt und das Entdeckungsrisiko für Straftäter erhöht werden, was zu einem Vorsprung in der Inneren Sicherheit führt. Die gemeinsame Nutzung von Ressourcen ermöglicht es, flexibel auf sich verändernde Sicherheitsherausforderungen zu reagieren und die Verbrechensbekämpfung zu verstärken.

Auch sein Engagement als ehrenamtlicher Finanzrichter am Finanzgericht Nürnberg soll erwähnt sein.

Die 1902 gegründete Nürnberger Wach- und Schließgesellschaft hat sich ihren heutigen Stand durch konstant hohe Qualität ihrer Dienstleistungen erarbeitet. Qualität ist die Basis für den Geschäftserfolg und das nachhaltige Wachstum des Unternehmens. So sprechen die veröffentlichten Kennzahlen der NWS Gruppe, die mit ihrem Hauptgesellschafter Peter Stern in vierter Generation im Kern immer ein Familienunternehmen geblieben ist, sowie die sehr vielfältigen Auszeichnungen dieser Unternehmensgruppe für sich allein bereits eine klare Botschaft.

Peter und Robyn Stern

Bei derzeit 16 Standorten in Deutschland und Österreich, über 2.000 Beschäftigten und einem Jahresumsatz von ca. 100 Mio. Euro gehört die Unternehmensgruppe zu den führenden der Branche und bringt ihr fachliches Know-how in Fachausschüssen, aber auch federführend in Qualitäts-Normungsgremien beim Deutschen Institut für Normung (DIN) für Sicherheitsdienstleistungen ein.

Doch nicht nur das Vergangene zeichnet das Unternehmen aus, auch für die Zukunft ist die Nürnberger Wach- und Schließgesellschaft bestens aufgestellt. Bekannt als fairer Arbeitgeber kann sie dem in der Branche viel beklagten Personalmangel gut begegnen. Dank der Integration neuer Technologien bietet sie ihren Kunden Leistungen mit modernsten Standards.

Für jeden in der Firmengruppe ist ehrliche Nachhaltigkeit wichtig, die bedeutet, in Generationen zu denken und diese zu verbinden. Die Nürnberger Wach- und Schließgesellschaft lebt den Einklang von Ökonomie, Ökologie und sozialen Belangen. Sie ist das erste klimaneutrale Sicherheitsunternehmen in Deutschland, hat mittlerweile den dritten Nachhaltigkeitsbericht vorgestellt und hat ihr Umwelt- und Energiemanagement zertifizieren lassen. Sie engagiert sich in sozialen Projekten und Partnerschaften vor Ort, unterstützt internationale Projekte ebenso wie die Charta der Vielfalt. Nicht verwunderlich, dass sie von der Steinbeis Augsburg Business School als „Company of the Year 2022: ESG“ geehrt wurde.

Sicherheit ist Unternehmenszweck und Sinn der Nürnberger Wach- und Schließgesellschaft: Sicherheitstechnik, Dienstleistungen an Bahn, Flughafen, Werkschutz, Verkehrsüberwachung oder Arbeitsschutz – es geht immer um Sicherheit und um Innovationsoffenheit in jeder Hinsicht. Denn nur durch stete Weiterentwicklung konnte die Nürnberger Wach- und Schließgesellschaft 121 Jahre alt werden. Entwicklung und Technologie werden auch künftig bei der Lösungsfindung helfen. Da überrascht es nicht, dass die Vertreter des Nürnberger Unternehmens die Feier der traditionsreichen Jubiläen zum Anlass nahm, ihre Vision, klare Strategie und Fähigkeit zur Resilienz unter Beweis zu stellen und eindrucksvoll ihre zukunftsfähigen Lösungen zu präsentieren.

(Vl.) Robyn Stern, Milexys Ameis und Gerhard Ameis

Gregor Lehnert (rechts) und Ernst Steuger (Mitte)

Ehrung für 20-jährige Mitgliedschaft in der DGQ für All Service Sicherheitsdienste GmbH

All Service Sicherheitsdienste GmbH freut sich, seine 20-jährige Mitgliedschaft in der Deutschen Gesellschaft für Qualität (DGQ) bekannt zu geben. Diese langjährige Partnerschaft ist ein herausragender Meilenstein für All Service Sicherheitsdienste und unterstreicht das Engagement des Unternehmens für Qualität und Exzellenz in der Sicherheitsbranche. Die DGQ ist als zentrale, deutsche Qualitätsgesellschaft erster Ansprechpartner für Qualität, Qualitätsmanagement und Qualitätssicherung.

„Wir sind stolz darauf, Teil der DGQ-Familie zu sein und diese bedeutende Auszeichnung für unsere 20-jährige Mitgliedschaft entgegenzunehmen", sagte Peter Haller, Geschäftsführender Gesellschafter All Service Sicherheitsdienste GmbH. „Diese Urkunde ist auch Ausdruck des unermüdlichen Einsatzes unseres engagierten Teams, das stets bestrebt ist, die Erwartungen unserer Kunden zu übertreffen. Wir werden weiterhin unsere Qualitätsstandards verbessern und uns auf Innovationen konzentrieren, um unseren Kunden die bestmöglichen Sicherheitslösungen zu bieten."

Die All Service Sicherheitsdienste GmbH unterstützt TSG 1957 Frankfurter Berg e. V.

All Service Sicherheitsdienste GmbH unterstützt die Sportgemeinschaft TSG 1957 Frankfurter Berg e. V. in Frankfurt am Main mit einer Spende. Von den Spendengeldern werden Trikots oder andere Sportbekleidungen für die jungen Spieler finanziert. Der Verein bietet neben Fußball auch weitere Sportaktivitäten für Jugendliche an.

Für die All Service Sicherheitsdienste GmbH ist soziales Engagement ein wichtiger Bestandteil der Unternehmenskultur. Regelmäßig unterstützt das Sicherheitsunternehmen Vereine aus der Region.

„Diese Vereine leisten einen wertvollen Beitrag für die Freizeitgestaltung der Jugendlichen. Es freut mich sehr, dass wir sie durch eine Spende unterstützen können", sagte Peter Haller, Geschäftsführender Gesellschafter der All Service Sicherheitsdienste GmbH.

www.all-service.de

Apleona sieht sich für weiteres Wachstum in Deutschland und Europa gestärkt

Die beiden Facility- und Immobiliendienstleister Apleona und Gegenbauer haben ihre Fusion zum 3. Juli 2023 erfolgreich vollzogen. Nach Zustimmung aller relevanten Behörden wird jetzt der operative Zusammenschluss der beiden Unternehmen zu einem europäischen Branchenführer mit 40.000 Beschäftigten und 3,5 Mrd. Euro Umsatz umgesetzt. Die Geschäfte werden künftig einheitlich für alle Sparten des Konzerns unter dem Namen Apleona geführt. Kerngeschäftsfeld ist das Integrierte Facility-Management mit einem starken Fokus auf technisches Gebäudemanagement sowie regional auf den DACH-Markt.

Apleona CEO Dr. Jochen Keysberg bekräftigte die ambitionierte Wachstumsstrategie des FM- und Immobiliendienstleistungskonzerns sowohl für Deutschland wie für Europa. „In Deutschland können wir unseren Kunden jetzt sowohl technische wie auch infrastrukturelle Dienstleistungen flächendeckend aus einer Hand anbieten. Immer mehr große Kunden erwarten von uns solche Integrierte Services komplett in Eigenleistung", erklärte er anlässlich des Closings.

www.apleona.com

CONDOR und DRZ – gemeinsam mehr erreichen!

Die CONDOR Gruppe gehört zu den Innovationstreibern der privaten Sicherheitswirtschaft Deutschlands. Der Einsatz von Drohnen-Technologie oder Künstlicher Intelligenz zur Verbesserung der Dienstleistungsqualität und Optimierung von Planungsprozessen gehören zur Unternehmenskultur. In Forschungsprojekten mit Hochschulen, Feuerwehr- und Rettungsdiensten sowie Technikpartnern, wie z. B. „INSPIRE" im nordrhein-westfälischen Paderborn oder „5G. Stadt. Land. Leben retten" im baden-württembergischen Ulm, bringt CONDOR ihre drohnenspezifische Hard- und Softwarekompetenz mit ein. Im Rahmen der Netzwerk- und Branchenentwicklung ist das mittelständische Familienunternehmen Mitglied im Deutschen Rettungsrobotik Zentrum e. V. (DRZ) Dortmund.

Der gemeinnützige Verein (DRZ) wurde im Jahre 2018 gegründet und verfolgt den Zweck, die Entwicklung von Robotersystemen zur Unterstützung bei Rettung und Schutz von Menschen und Sachwerten zu fördern. „Im Fokus des DRZ befinden sich Forschung und Entwicklung auf dem Gebiet der Rettungsrobotik. Hier können wir dank unserer langjährigen Erfahrungen aus den verschiedenen Forschungsprojekten zielführende Beiträge leisten", ist Cornelius Toussaint überzeugt. Zudem ziele das DRZ auch auf die Berufsbildung, die Rettung aus Lebensgefahr und Feuer-, Arbeits-, Bevölkerungsschutz sowie Unfallverhütung ab.

CONDOR Thüringen sichert 30. DomStufen-Festpiele in Erfurt

Zum 30. Mal fanden in diesem Jahr die weltberühmten DomStufen-Festspiele in Erfurt statt. Zum 30. Mal sicherte CONDOR Thüringen eines der kulturellen Ereignisse im Bundesland Thüringen. Für die Organisation der DomStufen-Festspiele ist das Theater Erfurt zuständig, mit dem CONDOR bereits seit 1993 zusammenarbeitet. Mit Einlass- und Taschenkontrollen sowie Evakuierungshelfern sorgt das CONDOR Team seit 1994 für Ordnung und Sicherheit auf dem Festspielgelände.

Über die Jahre wurde das Sicherheitskonzept durch die Erfahrungen aus dem jeweiligen Vorjahr verfeinert. Die größten Veränderungen am Sicherheitskonzept habe es jedoch nach den Anschlägen von Paris im Jahre 2015 gegeben. „Von da an stieg die Zusatzbewachung und es wurden Taschen auf

gefährliche Gegenstände intensiver durchsucht. Es wurde beispielsweise die Mitnahme von Glasflaschen auf das Gelände untersagt", so Einsatzleiter Wilfried Hamann, der ebenfalls zum 30. Mal als Einsatzleiter das CONDOR Team führte.

www.condor-sicherheit.de

Deutscher Schutz- und Wachdienst

DSW feiert Ausbildungserfolge am Frankfurter Standort

Seit Herbst 2022 ist der Deutsche Schutz- und Wachdienst (DSW) mit einem eigenen Schulungszentrum neben dem Frankfurter Flughafen vertreten. Zusammen mit seinem Recruiting-Partner, der GATE Aviation GmbH (GATE), bildet er dort neue Luftsicherheitsassistenten aus – mit großem Erfolg: Seit Beginn der Schulungen im Oktober liegt die Besteherquote bei 88 Prozent.

„Wir ziehen nach gut einem halben Jahr ein durchweg positives Fazit unserer Ausbildungsaktivitäten in Frankfurt. Die sehr guten Erfolgsquoten unserer Absolventen bestätigen die hohe Qualität unserer Trainer – hier konnten wir am Standort Frankfurt ganz neue Maßstäbe in puncto Schulungsdurchführung und Prüfungsergebnisse setzen", so Nicole Oppermann, DSW-Geschäftsführerin. Glenn Murphy, Director Aviation beim DSW, ergänzt: „Am Flughafen zu arbeiten ist spannend, aber auch herausfordernd. Dem enormen Druck und den steigenden Passagierzahlen können wir daher nur mit Qualität begegnen. Wir gehen während der Ausbildung sehr individuell auf die Teilnehmer ein, um diese optimal auf ihren zukünftigen Arbeitsplatz vorzubereiten."

www.piepenbrock.de

Dussmann

FACILITY MANAGEMENT

Dussmann investiert in Spezialisten für industrielle Digitalisierung, neogramm

Das international tätige Dienstleistungsunternehmen Dussmann investiert in den Spezialisten für industrielle Digitalisierung, neogramm. Mit einer Beteiligung von 25 Prozent an dem Mannheimer Unternehmen baut der Geschäftsbereich Dussmann Technical Solutions sein Angebot im Bereich Automatisierung weiter aus. „Durch die Beteiligung an neogramm umfasst unser Portfolio im technischen Anlagenbau nun auch Softwarelösungen für die industrielle Digitalisierung", sagt Dr. Tino Weber, Geschäftsführer Dussmann Technical Solutions.

Über 35 Spezialistinnen und Spezialisten entwickeln bei neogramm Softwarelösungen in den Bereichen IIoT, Automatisierungstechnik und KI-gestützte Bildverarbeitung für Industriekunden aus den Branchen Automotive, Elektronikfertigung, Holz- und Metallverarbeitung, Pharma sowie Maschinen- und Anlagenbau. „Ich freue mich auf die neuen vertrieblichen Anknüpfungspunkte über Dussmann Technical Solutions, den gegenseitigen Wissenstransfer und die wechselseitige Ergänzung unserer Services", so Kai Blümchen, Geschäftsführer neogramm. „Die Investition seitens Dussmann ermöglicht neogramm ein sicheres Wachstum des Bestandsgeschäfts und bringt gleichermaßen die Produktentwicklung maßgeblich voran", ergänzt der zweite neogramm-Geschäftsführer Stephan Könn.

www.dussmann.de

e-shelter security

Henrik Lüngen verstärkt das Managementteam der e-shelter security

Zum 1. August beginnt Henrik Lüngen bei der e-shelter security Gruppe als neues Mitglied der Geschäftsleitung. In seiner Position als Chief Customer Officer (CCO) übernimmt er die Verantwortung für den Bereich Vertrieb und Marketing.

Mit knapp 30 Jahren Erfahrung konnte er seine Führungsqualitäten und sein umfassendes Fachwissen im Großkundenvertrieb bei Siemens Building Technologies und zuletzt als Vice President Sales bei Thing Technologies unter Beweis stellen.

„Mit Henrik Lüngen gewinnen wir einen hoch qualifizierten Vertriebs- und Marketingexperten. Mit seinem Branchen-Know-how und Verständnis technischer Lösungen werden wir unsere Positionierung weiter ausbauen und die Verbindung zwischen Sicherheitstechnik und IoT vorantreiben", erklärt Dr. Tristan Haage, CEO e-shelter security.

Innovationspreis für e-shelter security

Der Frankfurter Systemintegrator e-shelter security technologies hat in der 30. Runde des Top 100 Wettbewerbs überzeugt und zählt damit zu den innovativsten Unternehmen Deutschlands. Am 23. Juni 2023 wurde das Unternehmen, mit Standorten in Frankfurt am Main, Berlin und München, offiziell mit dem Top 100-Siegel 2023 auf dem Deutschen-Mittelstands-Summit ausgezeichnet, welches von dem Wissenschaftsjournalisten Ranga Yogeshwar überreicht wurde.

„Bei Top 100 geht es um die Frage, welchen Stellenwert das Innovationsziel im Unternehmen einnimmt", sagt Prof. Dr. Nikolaus Franke, wissenschaftlicher Leiter des Wettbewerbs. „Dominieren Routinen und Gewohnheiten oder aber ist das Unternehmen in der Lage, Bestehendes zu hinterfragen, kreativ und neu zu denken und erfolgreich am Markt durchzusetzen? Wir analysieren diese Fähigkeit anhand von mehr als 100 Prüfkriterien", erläutert er. e-shelter security technologies entwickelt und implementiert ganzheitliche Lösungen für sichere, intelligente und nachhaltige Gebäude, indem sie digitale Technologien mit modernster Sicherheitstechnik kombiniert. Die Top 100 Jury hob vor allem die „Außenorientierung/Open Innovation" des Unternehmens hervor. Transparente Prozesse und eine vitale Außenorientierung machen das Unternehmen innovativ.

Die Geschäftsleitung bedankt sich herzlich bei dem gesamten Team der e-shelter security Gruppe. Ohne das Engagement der mehr als 300 Mitarbeiterinnen und Mitarbeiter wäre die Auszeichnung als eines der innovativsten Unternehmen Deutschlands nicht möglich gewesen. Innovationen entstehen nur durch Zusammenarbeit.

www.e-shelter.io

Klüh zum vierten Mal in Folge zum Top-Arbeitgeber gekürt

Der Multiservice-Anbieter Klüh gehört auch in diesem Jahr wieder zu den begehrtesten Arbeitgebern der deutschen Facility-Management-Branche. In der Studie „Deutschlands begehrteste Arbeitgeber 2023" des F.A.Z.-Instituts und des Instituts für Management- und Wirtschaftsforschung wurde das Düsseldorfer Familienunternehmen als eines von drei im Bereich infrastruktureller Dienstleistungen zum vierten Mal in Folge ausgezeichnet.

Christian Frank, Geschäftsführer und verantwortlich unter anderem für den Bereich Personal: „In Zeiten des Fachkräftemangels haben Arbeitnehmer mehr als zuvor die Möglichkeit, ihren Arbeitgeber kritisch und sorgfältig auszuwählen. Daher ist es für uns natürlich wichtiger denn je, als attraktiver Arbeitgeber wahrgenommen zu werden. Damit das so bleibt, werden wir weiterhin unser Bestes geben, um die Erwartungen unserer Mitarbeitenden zu erfüllen."

Klüh Security erhält siebten Comenius-Award in Folge

Klüh Security ist zum siebten Mal in Folge mit dem angesehenen Comenius-Edu-Media-Award der Gesellschaft für Pädagogik, Information und Medien e. V. (GPI) ausgezeichnet worden. Die Security-Sparte des Multiservice-Anbieters Klüh erhielt den Preis in der Kategorie „Berufliche Aus- und Weiterbildung" für ihr digitales Lernprogramm „Lagebedingter Erstickungstod". Klüh Security-Geschäftsführer Sven Horstmann: „Wir freuen uns sehr über die Auszeichnung und sind stolz, dass damit die didaktische und mediale Qualität unserer Arbeit auch von neutraler Expertenseite bestätigt und gewürdigt wird."

Klüh Security bildet seine Mitarbeitenden in Seminaren und Workshops der hauseigenen Akademie sowie Sicherheitsschule selbst aus. Darüber hinaus bietet die neue Rheinische Akademie für Sicherheit und Wirtschaft GmbH (RASW) ein umfangreiches Schulungsangebot für Aus- und Fortbildungsthemen des Sicherheitsgewerbes in den Bereichen Luftsicherheit, Gefahrgut und Personenschutz an, welches sich an alle Sicherheitsunternehmen richtet, die ihre Einsatzkräfte entsprechend qualifizieren möchten. Das web- und computerbasierte Lernmanagementsystem „DigiLearn" bietet hierbei eine innovative und moderne Ergänzung zum traditionellen Präsenzunterricht.

www.klueh.de

KÖTTER Security verstärkt die Führungsebene

Seit 1. Juli fungiert Jörg Marmann als neuer Geschäftsführender Direktor der KÖTTER Sicherheitssysteme SE & Co. KG. Jörg Marmann folgt auf Andreas Kaus, der seit der Ausgründung 2010 an der Spitze von KÖTTER Sicherheitssysteme stand und den Übergangsprozess nun flankierend begleitet. Parallel bereitet sich Kaus auf zusätzliche Führungsaufgaben in NRW vor.

Andreas Kaus wird dort zum 1. Januar 2024 die Nachfolge von Roland vom Brauck, der zum Jahresende in Ruhestand geht, als Geschäftsführender Direktor für die KÖTTER SE & Co. KG Security, Düsseldorf, und die KÖTTER Logistik & Service SE & Co. KG antreten.

Mit Roland vom Brauck wird ein „Urgestein" der Sicherheitswirtschaft von Bord gehen. Der 67-Jährige hat über drei Jahrzehnte Führungsfunktionen inne, davon 17 Jahre in der KÖTTER Security Gruppe.

Parallel hierzu hat auch die KÖTTER SE & Co. KG Security, München, ihre Führungsmannschaft ausgeweitet und einhergehend damit veränderte Strukturen geschaffen. So ist Lars Homann seit dem 1. Juli als neuer Geschäftsführender Direktor für die Region Bayern mit den Standorten Augsburg, Fürth, München, Nürnberg und Würzburg verantwortlich. Gleichzeitig ist mit Thomas Naßhan ein Eigengewächs aus der Führungsebene zum Geschäftsführenden Direktor aufgerückt. Er steuert in dieser Funktion seit Juli die Aktivitäten in Baden-Württemberg, Hessen, Rheinland-Pfalz und Saarland. Im Zuge der Umstrukturierung übernahm zudem der bisher für das Geschäft in Bayern zuständige Prokurist Sören Stübing die Vertriebsleiterposition. Die Gesamtverantwortung für die KÖTTER SE & Co. KG Security, München, trägt in seiner neuen Funktion als Vorsitzender der Geschäftsführung weiter der Geschäftsführende Direktor Dirk H. Bürhaus.

KÖTTER Unternehmensgruppe übernimmt Spezialanbieter MedGravity

Die KÖTTER Unternehmensgruppe treibt ihre strategische Ausrichtung als innovativer Partner für Smart Service Solutions weiter voran. Neuester Baustein ist die Übernahme aller Anteile am Aus- und Weiterbildungsspezialisten MedGravity mit Sitz in Hannover durch die KÖTTER Akademie GmbH & Co. KG. Die Transaktion tritt rückwirkend zum 1. Januar 2023 in Kraft.

Durch den Zusammenschluss baut die bundesweit tätige Dienstleistungsgruppe ihr Portfolio insbesondere um hochqualitative Spezialschulungen für Unternehmen, Rettungs- und Sanitätsdienste aus. Der Schwerpunkt liegt auf der Aus- und Weiterbildung von Ersthelfern sowie von Betriebs-, Rettungs- und Notfallsanitätern. Besonderer Pluspunkt aus Sicht von Auftraggebern und Teilnehmern sind spezifische Zusatzangebote, mit denen MedGravity überzeugt. So hält das Unternehmen u. a. die eLearning-Ausbildung für Rettungssanitäter genauso bereit wie die Teilzeitausbildung von Notfallsanitätern.

„Ich freue mich auf die erfolgreiche Zusammenarbeit mit dem MedGravity-Team. Sie bietet vielfältige Chancen, um gemeinsam weiterzuwachsen", sagte Friedrich P. Kötter, Verwaltungsrat der KÖTTER Security Gruppe.

koetter.de

m:con und LIEBLANG Gruppe setzen langjährige Partnerschaft fort

Die m:con – mannheim:congress GmbH und die Sicherheitssparte der LIEBLANG Gruppe setzen ihre langjährige Zusammenarbeit für weitere drei Jahre fort. Der Zuschlag für den Rahmenvertrag erfolgte im Zuge einer Ausschreibung für Personaldienstleistungen. Bereits seit 2016 erbringen die LIEBLANG Sicherheitsdienste als Generalunternehmer umfangreiche Dienstleistungen im Congress Center Rosengarten in Mannheim.

Frank Gilpert, als Geschäftsführer verantwortlich für das operative Geschäft der Sicherheitsdienste: „Die Vertragsverlängerung zeigt das große Vertrauen in unsere Kompetenz und Zuverlässigkeit, mit der wir die großartige Entwicklung des Congress Center Rosengarten seit vielen Jahren begleiten. Wir freuen uns auf weitere drei Jahre vertrauensvoller Zusammenarbeit."

LIEBLANG Gruppe übernimmt Heckermann Objektschutz

Die LIEBLANG Gruppe hat im Rahmen einer Unternehmensnachfolge das Ratinger Sicherheitsunternehmen Heckermann Objektschutz akquiriert. Der Dienstleister ist auf personelle und technische Sicherheitsdienstleistungen ausgerichtet. Mit Wirkung zum 6. April 2023 hat der Gründer Rainer Heckermann nach rund 50-jähriger Inhaberschaft die Geschäftsführung abgegeben und begleitet den Übergang nun in beratender Funktion. Neuer Geschäftsführer des Unternehmens ist Till Niesmann. Er wird unterstützt von den Prokuristen Benjamin Müller und Manfred Becker.

„Durch unsere Tochtergesellschaft sind wir in Nordrhein-Westfalen seit Jahrzehnten für unsere hohe Kompetenz in den Bereichen Werk- und Objektschutz, Revierwachdienste, Empfangsdienste, Arbeitssicherheit und Brandschutz bekannt", sagt der Geschäftsführende Gesellschafter der LIEBLANG Gruppe, Roman Großmann. „Mit dem Zukauf erweitern wir unser Portfolio um eine renommierte Notruf- und Serviceleitstelle und das Angebotsspektrum um die Option einer integralen, herstellerunabhängigen Gefahrenmeldetechnik."
www.lieblang.com

Uwe-Dirk Uhlig im Alter von 81 Jahren verstorben

Mit schwerem Herzen und tiefer Trauer müssen wir Abschied nehmen von unserem geschätzten ehemaligen Geschäftsführer Uwe-Dirk Uhlig. Von 1985 bis 2008 leitete er erfolgreich die Geschicke der Nürnberger Wach- und Schließgesellschaft. Sein unermüdlicher Einsatz und seine unvergleichlichen Leistungen haben uns zu dem gemacht, was wir heute sind: ein erfolgreicher und angesehener Akteur in der Branche. Seine Weitsicht und sein untrügliches Gespür für die Bedürfnisse unserer Kunden haben uns stets auf den richtigen Weg geführt.

Stark engagiert in der Verbandsarbeit übernahm er den Vorsitz des BDGW, war er über 25 Jahre Mitglied der Tarifkommission in der BDSW Landesgruppe Bayern. 1992 wurde er in den Vorstand gewählt und von 1998 bis 2010 war er Vorsitzender der zweitgrößten Landesgruppe des Verbandes. In dieser Funktion leitete er auch die Tarifkommission.

Dank seines bedeutenden Beitrags zur Verbesserung des „Gemeinwohls" wurde er vom Bundespräsidenten mit dem Bundesverdienstkreuz am Bande ausgezeichnet. Auf Landesebene in Bayern, der zweitgrößten Gruppe des BDSW, wurde ihm der Titel des Ehrenvorsitzenden verliehen.

Doch nicht nur als Geschäftsführer, sondern auch als Mensch war Uwe-Dirk Uhlig ein wertvoller Wegbegleiter für uns alle. Seine offene Art, seine Empathie und sein Sinn für Humor werden uns sehr fehlen. Wir sind dankbar für die Zeit, die wir mit ihm verbringen durften und werden ihn stets in ehrenvoller Erinnerung behalten.
www.nwsgmbh.de

Lünendonk®-Liste führt Piepenbrock auf dem sechsten Platz

Piepenbrock ist wieder unter den Top Ten der Lünendonk®-Liste „Führende Facility-Service-Unternehmen in Deutschland". Im Jahr 2022 erzielte das Familienunternehmen einen Umsatz von 779,5 Mio. Euro – und rückt damit im Ranking einen Platz nach vorne. Personal bleibt ein wichtiges Thema und treibt auch Piepenbrock um: „Die Steigerung des Branchenmindestlohns für die Gebäudereiniger im Oktober 2022 war ein wichtiges Signal, um den Arbeitskräftemangel nicht noch zusätzlich zu verschärfen. Herausfordernd bleibt er trotzdem – wir müssen den Veränderungen in der Arbeitswelt mit neuen Konzepten begegnen und unsere Arbeitgeberattraktivität weiter steigern", sagt Arnulf Piepenbrock, Geschäftsführender Gesellschafter der gleichnamigen Unternehmensgruppe. „Daran arbeiten wir bereits. Unter anderem mit unserem Konzept zur Reinigung während der Betriebszeiten. Das gelingt aber nur, wenn wir unsere Auftraggeber davon überzeugen, mit uns gemeinsam neue Wege zu gehen.
www.piepenbrock.de

Münchner U-Bahnwache sorgt weiter für Sicherheit

Vor Kurzem wurden zwischen den Stadtwerken München (SWM) und der Securitas Deutschland die neuen Verträge für die Bewachung der Münchner U-Bahn ab dem 1. Januar 2024 unterzeichnet.

Die neuen Verträge haben eine Laufzeit von zwölf Jahren und umfassen das gesamte Leistungsspektrum der U-Bahnwache. Dazu zählen insbesondere regelmäßige Streifengänge in Bahnhöfen und Zügen, teilweise gemeinsam mit der Polizei, die Bewachung von abgestellten U-Bahnen sowie Einsätze in Zivil. Darüber hinaus hilft

die U-Bahnwache bei Großveranstaltungen und allen Arten von Notfällen sowie bei Anliegen der Fahrgäste.

„Wir sind stolz darauf, diesen wichtigen Auftrag fortzuführen und unsere langjährige Partnerschaft mit den Stadtwerken München in der Münchner U-Bahn fortzusetzen", sagt dazu Werner Landstorfer, Area Director bei Securitas Deutschland. „Das langjährige Vertrauen des Vertragspartners zeigt uns, dass wir mit unserer Dienstleistung überzeugen konnten, und bestärkt uns in unserem Engagement für mehr Sicherheit im öffentlichen Raum."

www.securitas.de

Sicherheit in der Arena: FC Schalke 04 verlässt sich weiterhin auf Stölting

Ein sicheres Umfeld ist die Grundvoraussetzung für ein perfektes Stadionerlebnis voller Emotionen. Der FC Schalke 04 legt diese anspruchsvolle Aufgabe auch zukünftig in die bewährten Hände der Stölting Service Group. Die beiden Partner vereinbarten nun eine Verlängerung des laufenden Security-Vertrags bis zum Jahr 2026.

„Mit dem FC Schalke 04 verbindet uns nicht nur unsere Heimat Gelsenkirchen, sondern auch eine seit vielen Jahren bestehende Zusammenarbeit", erläutert Sebastian Mosbacher als CEO der Stölting Service Group. „Wir sind stolz darauf, dem Klub auch weiterhin als Premiumpartner und als zuverlässiger Dienstleister zur Seite zu stehen."

www.stoelting-gruppe.de

Die WISAG Sicherheit & Service ist neuer Dienstleister der Landesbank Baden-Württemberg

Die WISAG Sicherheit & Service Süd GmbH & Co. KG ist nun auch für die Landesbank Baden-Württemberg (LBBW) im Einsatz: Der Dienstleister sorgt künftig für die Sicherheit der Beschäftigten sowie der Immobilien – nicht nur am Zentralsitz des Finanzinstituts in Stuttgart, sondern auch an den Standorten in Leipzig, Karlsruhe, Mainz und Mannheim. Nach 18 Jahren hatte die LBBW den Auftrag erstmals wieder ausgeschrieben.

„Unser gesamtes Team freut sich sehr, dass sich die LBBW nach einem umfangreichen Ausschreibungsprozess für die WISAG entschieden hat. Schließlich gehört die LBBW zu den Unternehmen mit den größten Sicherheitsansprüchen in Südwestdeutschland", sagt Norman Ammon, Geschäftsführer der WISAG Sicherheit & Service Süd GmbH & Co. KG, die den Auftrag betreut.

WISAG Aviation erreicht Meilenstein: 1.000 CO_2-neutrale Abfertigungen am BER

Im Februar 2021 fiel der Startschuss für die Nachhaltigkeitsinitiative „Ready for Green" am Flughafen Berlin-Brandenburg. Ziel der WISAG Aviation ist es, die Emissionen bei Flugzeugabfertigungen durch die Umstellung auf elektrische Vorfeldgeräte signifikant zu reduzieren. Nun zieht das Unternehmen Bilanz: Zum 19. Juli verzeichnete man mehr als 1.000 CO_2-neutrale Abfertigungen am Hauptstadtflughafen für das Jahr 2023. Der Anteil der elektrisch betriebenen Vorfeldfahrzeuge konnte mittlerweile auf 55 Prozent ausgebaut werden. Dadurch wurden je Abfertigung durchschnittlich 33 Kilogramm CO_2 eingespart, was in Summe knapp 33 Tonnen in 2023 entspricht.

Bislang konnten am Flughafen Berlin-Brandenburg in 2023 mehr als 1.000 CO_2-neutrale Abfertigungen erreicht werden. Ein Abfertigungsprozess gilt als CO_2-neutral, wenn alle für den „Turnaround" benötigten Fahrzeuge und Geräte keine Emissionen erzeugen. Dies umfasst Gepäckschlepper und -bänder, Fahrgasttreppen, Pushback-Fahrzeuge und Bodenstromaggregate. Damit nimmt der Bodenverkehrsdienstleister WISAG Aviation mit Hauptsitz in Frankfurt am Main erneut eine Vorreiterrolle ein.

„Nachhaltigkeit hat für uns als WISAG Aviation, aber auch übergreifend im Konzern, oberste Priorität. Denn neben der reinen Emissionsreduzierung profitieren auch unsere Mitarbeitenden vom Gebrauch der elektrischen Vorfeldgeräte, da diese wesentlich geräuschärmer sind und fast keine Schadstoffe produzieren. Am BER haben wir mittlerweile 55 Prozent davon im Einsatz. Wir bedanken uns bei unseren Airline-Partnern, insbesondere bei Norwegian, und dem Flughafen, mit denen wir diesen Meilenstein erreichen konnten. Ich freue mich sehr auf unsere nächsten, gemeinsamen Schritte", betont Carmen Ruck, COO der WISAG Aviation.

www.wisag.de

Bayerns Best 50

Das Bayerische Staatsministerium für Wirtschaft, Landesentwicklung und Energie ehrt in diesem Jahr wieder die 50 wachstumsstärksten, innovativsten und gleichzeitig nachhaltigsten mittelständischen Unternehmen mit der Auszeichnung BAYERNS BEST 50.

In einer Feierstunde im Schloss Oberschleißheim wurde am 24. Juli 2023 durch den Staatssekretär Roland Weigert die WWD Dienstleistung GmbH als Preisträger 2023 ausgezeichnet. Im Rahmen der Veranstaltung nahmen Geschäftsführung und Geschäftsleitung den Preis entgegen.

„Dieser Preis zeigt, dass die WWD Dienstleistung GmbH auf dem richtigen Weg ist." Geschäftsleiter Patrick Mathieu betonte, dass diese Auszeichnung Ehre und Verpflichtung zugleich sei und uns darin bestärke, den eingeschlagenen Weg insbesondere bezüglich Nachhaltigkeit und Innovation weiter zu begehen. Gleichzeitig machte er aber klar, dass dies eine Auszeichnung für alle Mitarbeiter sei, die sich tagtäglich an den Objekten und in den Verwaltungen für die WWD einsetzen. Sie alle können stolz auf diese Auszeichnung sein und ihnen allen gilt sein besonderer Dank.

www.wwd-dienstleistung.de

Dienstleistungen unserer Mitglieder

Alarmaufschaltung

FSO GmbH
Am Patentbusch 6A, 26125 Oldenburg
Tel.: +49 441 68066, Fax: 939001-939
Mail: info@fso.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Alarmservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

Piepenbrock Sicherheit GmbH + Co. KG
Hannoversche Str. 91–95, 49084 Osnabrück
Tel.: +49 541 5841-441, Fax: 5841-464
Mail: sicherheit@piepenbrock.de
Web: www.piepenbrock.de/sicherheit

ZIEMANN SICHERHEIT GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Alarmempfangsstelle EN 50518

FSO GmbH
Am Patentbusch 6A, 26125 Oldenburg
Tel.: +49 441 68066, Fax: 939001-939
Mail: info@fso.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Alarmservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

Alarmprovider

FSO GmbH
Am Patentbusch 6A, 26125 Oldenburg
Tel.: +49 441 68066, Fax: 939001-939
Mail: info@fso.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

Alarmverfolgung

IKS Industrie- und Kommunalservice GmbH
August-Bebel-Str. 20, 33602 Bielefeld
Tel.: +49 521 137878, Fax: 137880
Web: www.iks-sicherheitsdienst.de
Mail: info@iks-sicherheit.de

Industriewerkschutz GmbH
Magnolienweg 30, 63741 Aschaffenburg
Tel.: +49 6021 380330, Fax: 380354
Mail: info@iws-ab.de

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Alarmservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Trierer Wachdienst Jakob Pauly GmbH
Bruchhausenstr. 10, 54290 Trier
Tel.: +49 651 97834-0, Fax: 97834-20
Mail: info@twd-sicherheit.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

WUI Werk- und Industrieschutz GmbH & Co. KG
An der Grube Camphausen 1, 66287 Quierschied
Tel.: +49 6897 919417, Fax: 55228
Mail: info-wui@ugl-sicherheit.de

ZIEMANN SICHERHEIT GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Altennotruf

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

Arbeitssicherheit

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

Nürnberger Wach- und Schließgesellschaft mbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Aufzugsnotruf

IKS Industrie- und Kommunalservice GmbH
August-Bebel-Str. 20, 33602 Bielefeld
Tel.: +49 521 137878, Fax: 137880
Mail: info@iks-sicherheit.de
Web: www.iks-sicherheitsdienst.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Alarmservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Ausbildung

AST Akademie für Sicherheit und Technik –
Saarbrücker Werkschutzschule – GmbH & Co. KG
An der Grube Camphausen 1, 66287 Quierschied
Tel.: +49 6897 919417, Fax: 55228
Mail: info-ast@ugl-sicherheit.de

A|S|S Akademie für Schutz und Sicherheit GmbH
Willy-Brandt-Platz 10, 90402 Nürnberg
Tel.: +49 911 51996550
Mail: info@ass-nuernberg.de
Web: www.ass-nuernberg.de

Dresdner Wach- und Sicherungs-Institut GmbH
Zur Wetterwarte 29, 01109 Dresden
Tel.: +49 351 8836-0, Fax: 8836-250

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

BDSW-Modulkonzept

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

Fachkraft für Schutz und Sicherheit

A|S|S Akademie für Schutz und Sicherheit GmbH
Willy-Brandt-Platz 10, 90402 Nürnberg
Tel.: +49 911 51996550
Mail: info@ass-nuernberg.de
Web: www.ass-nuernberg.de

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Geprüfte Schutz- und Sicherheitskraft

A|S|S Akademie für Schutz und Sicherheit GmbH
Willy-Brandt-Platz 10, 90402 Nürnberg
Tel.: +49 911 51996550
Mail: info@ass-nuernberg.de
Web: www.ass-nuernberg.de

Dresdner Wach- und Sicherungs-Institut GmbH
Zur Wetterwarte 29, 01109 Dresden
Tel.: +49 351 8836-0, Fax: 8836-250

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Interventionskraft VdS

A|S|S Akademie für Schutz und Sicherheit GmbH
Willy-Brandt-Platz 10, 90402 Nürnberg
Tel.: +49 911 51996550,
Mail: info@ass-nuernberg.de
Web: www.ass-nuernberg.de

Dresdner Wach- und Sicherungs-Institut GmbH
Zur Wetterwarte 29, 01109 Dresden
Tel.: +49 351 8836-0, Fax: 8836-250

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Leitende NSL-Fachkraft VdS

A|S|S Akademie für Schutz und Sicherheit GmbH
Willy-Brandt-Platz 10, 90402 Nürnberg
Tel.: +49 911 51996550
Mail: info@ass-nuernberg.de
Web: www.ass-nuernberg.de

Dresdner Wach- und Sicherungs-Institut GmbH
Zur Wetterwarte 29, 01109 Dresden
Tel.: +49 351 8836-0, Fax: 8836-250

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

Justizvollzug

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

Krisenmanagement

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Ausbildung

Krisenkommunikation

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Maritime Sicherheit

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

Meister für Schutz und Sicherheit

A|S|S Akademie für Schutz und Sicherheit GmbH
Willy-Brandt-Platz 10, 90402 Nürnberg
Tel.: +49 911 51996550
Mail: info@ass-nuernberg.de
Web: www.ass-nuernberg.de

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

Servicekraft für Schutz und Sicherheit

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

Sicherheitskonzepte

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

STI SECURITY TRAINING INTERNATIONAL GmbH
Ostring 3, 65205 Wiesbaden
Tel.: +49 6122 598340, Fax: 5983469
Mail: info@sti-training.com
Web: www.sti-training.com

Vorbereitung auf Sachkundeprüfung nach § 34a GewO

A|S|S Akademie für Schutz und Sicherheit GmbH
Willy-Brandt-Platz 10, 90402 Nürnberg
Tel.: +49 911 51996550
Mail: info@ass-nuernberg.de
Web: www.ass-nuernberg.de

Dresdner Wach- und Sicherungs-Institut GmbH
Zur Wetterwarte 29, 01109 Dresden
Tel.: +49 351 8836-0, Fax: 8836-250

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Baustellensicherheit

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

UTS Sicherheit & Service GmbH
Europa-Allee 11, 54343 Föhren
Tel.: + 49 6502 9969991
Mail: info@uts-sicherheit.de

BDSW-zertifizierte Sicherheitsfachschule

A|S|S Akademie für Schutz und Sicherheit GmbH
Willy-Brandt-Platz 10, 90402 Nürnberg
Tel.: +49 911 51996550
Mail: info@ass-nuernberg.de
Web: www.ass-nuernberg.de

KÖTTER Akademie
Wilhelm-Beckmann-Str. 7, 45307 Essen
Tel.: +49 201 2788-513, Fax: 2788-8513
Mail: akademie@koetter.de
Web: koetter.de/akademie

Betrieblicher Brandschutz

Hier könnte Ihr Firmeneintrag stehen!

Bodycam

NetCo Professional Services GmbH
Am Mönchenfelde 13, 38889 Blankenburg (Harz)
Tel.: +49 3944 950-0, Fax: +49 3944 950-70
Mail: info@netco.de; anna-lena.nolte@netco.de
Web: www.body-worn-cam.de

Brandschutzdienste

GUARD Service Bewa GmbH
Frankfurter Allee 196, 10365 Berlin
Tel.: +49 30 6700 1383, Fax: 6700 1378
Mail: guard.berlin@t-online.de

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Bundeswehr

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Consulting/Unternehmensberatung

German Business Protection
Am Borsigturm 100, 13507 Berlin
Tel.: +49 30 63967027-0, Fax: 63967027-99
Mail: info@gbp-security.com
Web: www.gpbp-security.com

Reinhard Rupprecht, Dipl.-Volksw. und Jurist
Tel.: +49 2228 7000
Mail: rerupprecht@t-online.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Datensicherheit

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Detektei

Hier könnte Ihr Firmeneintrag stehen!

Diskothekenschutz

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

Einlasskontrollen

GUARD Service Bewa GmbH
Frankfurter Allee 196, 10365 Berlin
Tel.: +49 30 6700 1383, Fax: 6700 1378
Mail: guard.berlin@t-online.de

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Empfangsdienste

GUARD Service Bewa GmbH
Frankfurter Allee 196, 10365 Berlin
Tel.: +49 30 6700 1383, Fax: 6700 1378
Mail: guard.berlin@t-online.de

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

Piepenbrock Sicherheit GmbH + Co. KG
Hannoversche Str. 91–95, 49084 Osnabrück
Tel.: +49 541 5841-441, Fax: 5841-464
Mail: sicherheit@piepenbrock.de
Web: www.piepenbrock.de/sicherheit

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WWS Westfälischer Wachschutz GmbH & Co. KG
Herzogswall 30, 45657 Recklinghausen
Tel.: +49 2361 90422-0, Fax: 90422-29
Mail: info@wws-security.de
Web: www.wws-security.de
Ansprechpartner: Herr Huerkamp

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

ZIEMANN SICHERHEIT GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Empfangskontrolle

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Fachkraft für Schutz und Sicherheit

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Facility-Management

KÖTTER Services
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Gefahrenmeldung

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Alarmservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Geld- und Werttransporte

WWS Westfälischer Wachschutz GmbH & Co. KG
Herzogswall 30, 45657 Recklinghausen
Tel.: +49 2361 90422-0, Fax: 90422-29
Mail: info@wws-security.de
Web: www.wws-security.de
Ansprechpartner: Herr Huerkamp

ZIEMANN CASHSERVICE GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Geldbearbeitung

Prosegur Cash Services Germany GmbH
Kokkolastr. 5, 40882 Ratingen
Tel.: +49 2102 1248-351
Mail: welcome@prosegur.com
Web: www.prosegur.de

ZIEMANN CASHSERVICE GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Hersteller Geld- und Werttransportfahrzeuge

Apprich Secur GmbH
Gottlieb-Daimler-Str. 5, 14974 Ludwigsfelde
Tel.: +49 3378 80540
Mail: info@apprich-secur.de

Revisionstätigkeiten nach MaRisk

ZIEMANN CASHSERVICE GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Sorten- und Edelmetallhandel

ZIEMANN VALOR GmbH
Siegelsdorfer Str. 31, 90431 Nürnberg
Tel.: +49 911 98207000
Mail: info@ziemann-valor.de
Web: www.ziemann-valor.de

Technische Bankdienste

ZIEMANN CASHSERVICE GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Hausmeisterdienste

KÖTTER Cleaning
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Hostessenservice

Hier könnte Ihr Firmeneintrag stehen!

Hundeausbildung/Sprengstoffhunde

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

IT-Beratung und Software

Bite AG
Im Köller 3, 70794 Filderstadt
Tel.: +49 711 380155-00, Fax: +49 711 380155-102
Mail: info@bite.de
Web: www.bite.de

Justizdienste

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Kassiertätigkeit

GUARD Service Bewa GmbH
Frankfurter Allee 196, 10365 Berlin
Tel.: +49 30 6700 1383, Fax: 6700 1378
Mail: guard.berlin@t-online.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

WAB Wach- und Alarmbereitschaft GmbH,
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Konferenzdienste

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Kurierdienste

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Luftfahrtsicherheitsdienste

DSW Deutscher Schutz- und Wachdienst GmbH + Co. KG
Hannoversche Str. 91–95, 49084 Osnabrück

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

Nürnberger Wach- und Schließgesellschaft mbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

STI SECURITY TRAINING INTERNATIONAL GmbH
Ostring 3, 65205 Wiesbaden
Tel.: +49 6122 598340, Fax: 5983469
Mail: info@sti-training.com
Web: www.sti-training.com

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Maritime Sicherheit

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Messedienste

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WAB Wach- und Alarmbereitschaft GmbH,
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Mobile Videoüberwachung

LivEye GmbH
Europa-Allee 56b, 54343 Föhren
Tel.: +49 6502 4034722
Mail: info@liveye.com
Web: www.liveye.de

Museumsdienste

GUARD Service Bewa GmbH
Frankfurter Allee 196, 10365 Berlin
Tel.: +49 30 6700 1383, Fax: 6700 1378
Mail: guard.berlin@t-online.de

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

Rheinland Kultur GmbH
Ehrenfriedstr. 19, 50259 Pulheim
Tel.: +49 2234 9921263, Fax: 82841971
Mail: info@rheinlandkultur.de
Web: www.rheinlandkultur.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WAB Wach- und Alarmbereitschaft GmbH,
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Notruf-/Serviceleitstelle

FSO GmbH
Am Patentbusch 6A, 26125 Oldenburg
Tel.: +49 441 68066, Fax: 939001-939
Mail: info@fso.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Alarmservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

ZIEMANN SICHERHEIT GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Objektschutz

FSO GmbH
Am Patentbusch 6A, 26125 Oldenburg
Tel.: +49 441 68066, Fax: 939001-939
Mail: info@fso.de

GUARD Service Bewa GmbH
Frankfurter Allee 196, 10365 Berlin
Tel.: +49 30 6700 1383, Fax: 6700 1378
Mail: guard.berlin@t-online.de

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

PLURAL security GmbH
Tel.: +49 511 709000
Web: www.plural.de

Objektschutz

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Trierer Wachdienst Jakob Pauly GmbH & Co. KG
Bruchhausenstr. 10, 54290 Trier
Tel.: +49 651 97834-0, Fax: 97834-20
Mail: info@twd-sicherheit.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

WWS Westfälischer Wachschutz GmbH & Co. KG
Herzogswall 30, 45657 Recklinghausen
Tel.: +49 2361 90422-0, Fax: 90422-29
Mail: info@wws-security.de
Web: www.wws-security.de
Ansprechpartner: Herr Huerkamp

ZIEMANN SICHERHEIT GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Parkhausservice

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Parkplatzeinweisung

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Parkraumbewirtschaftung

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Personenschutz

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

WAB Wach- und Alarmbereitschaft GmbH,
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Pförtnerdienste

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

WWS Westfälischer Wachschutz GmbH & Co. KG
Herzogswall 30, 45657 Recklinghausen
Tel.: +49 2361 90422-0, Fax: 90422-29
Mail: info@wws-security.de
Web: www.wws-security.de
Ansprechpartner: Herr Huerkamp

Post- und Empfangsdienste

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Revierkontrolle

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

ZIEMANN SICHERHEIT GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Schutz von Flüchtlingsunterkünften

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Servicekraft für Schutz und Sicherheit

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Servicetelefon

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Sicherheitsanalyse/Beratung

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Sicherheitsdienste im Einzelhandel

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Sicherheitsdienste im ÖPV

DB Sicherheit GmbH
Köthener Str. 4, 10963 Berlin
Tel.: +49 30 0297-24871
Mail: vertrieb.dbsicherheit@deutschebahn.com
Web: www.dbsicherheit.com

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Sicherungsposten

Nürnberger Wach- und Schließgesellschaft mbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

UTS Sicherheit & Service GmbH
Europa-Allee 11, 54343 Föhren
Tel.: + 49 6502 9969991
Mail: info@uts-sicherheit.de

Software für Sicherheitsunternehmen

DISPONIC – ein Produkt der Bite AG
Im Köller 3, 70794 Filderstadt
Tel.: +49 711 380155-00, Fax: +49 711 380155-102
Mail: info@disponic.de
Web: www.disponic.de

Technische Meldung

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Überwachung im ruhenden Verkehr

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Veranstaltungsdienste

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

ZIEMANN SICHERHEIT GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Versicherung

ATLAS Versicherungsmakler
für Sicherheits- und Wertdienste GmbH
Industriestr. 155, 50999 Köln
Mail: bernd.schaefer@atlas-vsw.de
Web: www.atlas-vsw.de

Werkfeuerwehr

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

Werkschutz

K & C Security Service GmbH
Erfurter Str. 28, 44143 Dortmund
Tel.: +49 231 53338016
Herner Str. 28, 44807 Bochum
Tel.: +49 234 33865551
Mail: info@kc-security.de
Web: www.kc-security.de

KÖTTER Security
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

Piepenbrock Sicherheit GmbH + Co. KG
Hannoversche Str. 91–95, 49084 Osnabrück
Tel.: +49 541 5841-441, Fax: 5841-464
Mail: sicherheit@piepenbrock.de
Web: www.piepenbrock.de/sicherheit

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Peter-Jakob-Busch-Str. 5, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstr. 3, 60528 Frankfurt
Tel.: +49 69 505044-354, Fax: 505044-228
Mail: andre.manecke@wisag.de
Web: www.wisag.de

WWS Westfälischer Wachschutz GmbH & Co. KG
Herzogswall 30, 45657 Recklinghausen
Tel.: +49 2361 90422-0, Fax: 90422-29
Mail: info@wws-security.de
Web: www.wws-security.de
Ansprechpartner: Herr Huerkamp

ZIEMANN SICHERHEIT GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0, Fax: 9720-88
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Wirtschaftsschutz

German Business Protection
Am Borsigturm 100, 13507 Berlin
Tel.: +49 30 63967027-0, Fax: 63967027-99
Mail: info@gbp-security.com
Web: www.gpbp-security.com

Zertifiziert nach DIN EN 9001 ff.

A|S|S Akademie für Schutz und Sicherheit GmbH
Willy-Brandt-Platz 10, 90402 Nürnberg
Tel.: +49 911 51996550
Mail: info@ass-nuernberg.de
Web: www.ass-nuernberg.de

KÖTTER Services
Wilhelm-Beckmann-Str. 7, 45307 Essen
Hotline: +49 201 2788-388, Hotfax: 2788-488
Mail: info@koetter.de
Web: koetter.de

NWS Alarmservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

NWS Sicherheitsservice GmbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

Nürnberger Wach- und Schließgesellschaft mbH
Fraunhoferstr. 10, 90409 Nürnberg
Tel.: +49 911 519960
Mail: info@nwsgmbh.de
Web: www.nwsgmbh.de

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Straße 36, 65189 Wiesbaden
Telefon: +49 611 18141-0, Fax: 18141-99
E-Mail: sicherheit@samsic.de
Internet: www.samsic.de

Impressum

ISSN 0934-3245

Herausgeber:
BDSW Bundesverband der Sicherheitswirtschaft
Postfach 12 11 · 61282 Bad Homburg
Mail: mail@bdsw.de · Web: www.bdsw.de

BDGW Bundesvereinigung Deutscher
Geld- und Wertdienste
Postfach 14 19 · 61284 Bad Homburg
Mail: mail@bdgw.de · Web: www.bdgw.de

BDLS Bundesverband der Luftsicherheitsunternehmen
Postfach 14 08 · 61284 Bad Homburg
Mail: mail@bdls.aero
Web: www.bdls.aero

Verlag:
DSA GmbH
Am Weidenring 56 · 61352 Bad Homburg
Postfach 12 01 · 61282 Bad Homburg
Tel.: +49 61 72-94 80 50 · Fax: +49 61 72-45 85 80
Mail: dsa@bdsw.de

Redaktion:
RAin Cornelia Okpara (Chefredakteurin)
RAin Andrea Faulstich-Goebel
RA Andreas Paulick
Ass. jur. Martin Hildebrandt
RA Dr. Berthold Stoppelkamp
Tanja Staubach (Redaktionsassistenz)

Anzeigenbetreuung:
Tanja Staubach · Tel.: +49 61 72-94 80 52 · Mail: staubach@bdsw.de

Bildernachweis: Stockbilder von
stock.adobe.com, pixelio.de, istockphoto.com, unsplash.com

Design & Umsetzung:
Fronz Daten Service GmbH & Co. KG
Marktweg 42 · 47608 Geldern
Tel.: +49 28 31-9 76 39-0 · Fax: +49 28 31-9 76 39-15
Mail: info@fronz-daten-service.de
Web: www.fronz-daten-service.de

Druck:
L.N. Schaffrath GmbH & Co. KG DruckMedien
Marktweg 42–50 · 47608 Geldern

Anzeigen:
zzt. gültige Mediadaten vom 01.01.2023

75. Jahrgang 2023 | Auflage: 11.000 Exemplare

Der DSD – Der Sicherheitsdienst erscheint viermal jährlich.

Abonnements
Für Mitglieder der Sicherheitsverbände BDSW, BDGW und BDLS ist der Bezug für je ein Exemplar je Ausgabe im Mitgliedsbeitrag enthalten.
Bezugspreis je weiteren Exemplar für Mitglieder der Verbände der Sicherheitswirtschaft: 22,00 Euro jährlich zzgl. ges. MwSt.
Bezugspreis für Nichtmitglieder: 39,00 Euro jährlich einschl. ges. MwSt.
Einzelpreis für Nichtmitglieder: 7,50 Euro zzgl. ges. MwSt.
Auslandsbezug: 49,90 Euro einschl. ges. MwSt.

Auszubildende im Sicherheitsgewerbe

Von Rechtsanwältin Cornelia Okpara

RAin Cornelia Okpara

kommissarische Hauptgeschäftsführerin des Bundesverbandes der Sicherheitswirtschaft (BDSW)

Kürzlich wurde mir ein Leitartikel aus WELT Online zum Thema „Deutschland in der Azubi-Krise" weitergeleitet. Hieraus geht hervor, dass jede vierte Ausbildungsstelle vorzeitig vertraglich gelöst wird. Die Daten basieren auf dem, in der Regel im August eines Jahres erscheinenden, Datenreports des Bildungsinstitutes für Berufsbildung (BiBB). Im Jahr 2021, aktueller Erhebungsstand, lag die durchschnittliche sogenannte Vertragslösungsquote bei 26,7 Prozent, bezogen auf alle Ausbildungsberufe. Im Sicherheitsgewerbe lag sie mit 47,5 Prozent deutlich darüber. Im Vergleich zu den vergangenen Jahren war diese Quote schon niedriger, bewegte sich aber immer auf vergleichsweise hohem Niveau. Es stellt sich die Frage, warum die Vertragsauflösungsquote in unserer Branche so hoch ist und ob und wie man diese Situation verbessern kann.

Die deutsche Sicherheitswirtschaft bietet seit 20 Jahren die Möglichkeit, die Tätigkeit von Grund auf im Rahmen eines dualen Ausbildungsberufs zu erlernen. Seit 2002 bilden die Unternehmen Fachkräfte für die Branche aus und konnten so bereits rund 14.285 Beschäftigten einen qualifizierten Einstieg in die vielseitigen Tätigkeiten der deutschen Sicherheitswirtschaft ermöglichen. Mittlerweile bietet die Branche zwei duale Ausbildungsberufe – die dreijährige Ausbildung zur Fachkraft und die zweijährige zur Servicekraft für Schutz und Sicherheit. Besonders in Zeiten von Fachkräfte- und Personalmangel wird die Qualifikation der Beschäftigten immer wichtiger. Denn die Zukunft der Dienstleistung wird in erheblichem Maße aus integralen Lösungen von Sicherheitsdiensten und -technik bestehen und dazu bedarf es ausgebildeter und qualifizierter Mitarbeiter. Ich sehe in der Unterstützung der beiden zwei- und dreijährigen Berufsausbildungen in der Sicherheitswirtschaft eine große Chance, der Arbeitskräfteknappheit der Branche entgegenzuwirken. Junge Fachkräfte sind die Zukunft der Branche, deshalb verleiht der BDSW auch bereits seit 13 Jahren den Ausbildungspreis an Ausbildungsbetriebe, die sich in besonderer Weise im Bereich Ausbildung engagieren. Mit dem Ausbildungspreis möchten wir noch stärker dazu beitragen, dass der hohe Stellenwert qualifizierter Berufsausbildungen für die Sicherheitswirtschaft deutlich wird. Der Preis wird im Rahmen der Ausbildungstagung verliehen, die zum sechsten Mal gemeinsam mit der Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA) stattfindet und bereits 2010 ins Leben gerufen wurde, damals noch ohne Beteiligung der BDA. Hier besteht die Möglichkeit zu einem fachlichen Austausch über wichtige Aspekte und Herausforderungen rund um das Thema Ausbildung.

Bild: # 1573249868 / istockphoto.com

Eine bundesweit einmalige Initiative startete mit dem Ausbildungsjahr 2018/2019 in Hamburg – die sognannte Exzellenzinitiative des BDSW. Die Initiative soll den Auszubildenden dabei helfen, einen Ausbildungsplatz in einem qualifizierten und leistungsfähigen Sicherheitsunternehmen zu finden. Der BDSW hat sich deshalb mit der ASW Norddeutschland, der Gewerkschaft ver.di, der Handelskammer Hamburg und der Berufsschule 27 auf diese Initiative verständigt. Ein wichtiges Element der Initiative ist die Bestellung einer Ombudsperson. Diese Person ist in Problemfällen das unabhängige Bindeglied zwischen den Auszubildenden und den Berufsschulen, den Ausbildungsbetrieben sowie der Kammer. Gerade die Abbrecherquote in Hamburg ist seitdem deutlich zurückgegangen, aber auch die Zufriedenheit der Auszubildenden hat sich verbessert. Dieses Beispiel zeigt, dass es Wege gibt, die Ausbildungssituation in unserer Branche zu verbessern. Dieses Ziel sollten wir alle verfolgen.

BDSW

6.-7. November 2024
in Mönchengladbach

TECHNIKTAGUNG

des Fachausschuss Technik des
Bundesverbandes der Sicherheitswirtschaft (BDSW)

Ergreifen Sie die Chance, sich über topaktuelle Themen und Neuerungen aus dem Bereich Sicherheitstechnik zu informieren und sich mit anderen Experten zu vernetzen und auszutauschen. Die Techniktagung 2024 steht unter dem Motto

„TECHNIK UND MEHR“
Techniktrends, Digitalisierung, Normierung

Merken Sie sich den Termin bereits heute vor!

Bei Interesse, Rückfragen und weiteren Informationen steht Ihnen die Veranstaltungsassistentin **Regina Sarezki** unter **Tel. +49 6172 948051** oder E-Mail **sarezki@bdsw.de** zur Verfügung.

Aktuelle Veranstaltungsinformationen inklusive Agenda und Anmeldeformular werden Ihnen zeitnahe zum Download auf **www.bdsw.de** bereitgestellt.

6.-7. März 2024

13. LUFTSICHERHEITSTAGE

des BDLS Bundesverband der Luftsicherheitsunternehmen
und dem Bundespolizeipräsidium

im Holiday Inn Berlin Airport Conference Centre
in Schönefeld bei Berlin

Bitte merken Sie sich den Termin bereits vor!

Ergreifen Sie die Chance sich über topaktuelle Themen der Luftsicherheitsbranche zu informieren und nutzen Sie die Gelegenheit, sich mit Experten aus dem Bereich Luftsicherheit zu vernetzen.

Bei Interesse, Rückfragen und für weitere Infos steht Ihnen die Veranstaltungsassistentin **Manuela Blum** unter **Tel. +49 6172 948065** oder E-Mail **blum@bdls.aero** zur Verfügung.

BUNDESPOLIZEI

BUNDESVERBAND DER LUFTSICHERHEITS-UNTERNEHMEN BDLS