DSD
3 | 2025
DER SICHERHEITSDIENST
Fachmagazin für die Sicherheitswirtschaft
77. Jahrgang

SICHERHEITSTECHNIK

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

22. – 25. September 2026

SECURE YOUR BUSINESS

Die Leitmesse für Sicherheit

BUCHEN SIE JETZT!

Zum 1. Mal parallel:
die EURO DEFENCE EXPO –
die neue internationale Fachmesse
der Verteidigungsindustrie

security essen 26
the number one

www.security-essen.de

MESSE ESSEN

100 Tage im BDSW

Sehr geehrte Damen und Herren,
liebe Leserinnen und Leser,

die ersten 100 Tage als Präsident des Bundesverbandes der Sicherheitswirtschaft waren für mich nicht nur intensiv und erkenntnisreich, sondern auch von einer Vielzahl an Begegnungen geprägt – innerhalb unseres Verbandes ebenso wie mit politischen Entscheidungsträgern und Partnern in ganz Deutschland. Auch wenn ich unsere Branche seit vielen Jahren aus unterschiedlichen Perspektiven kenne, bringt die Rolle des Präsidenten doch eine neue, erweiterte Sichtweise mit sich: Der Blick wird breiter, die Verantwortung umfassender und die Themenvielfalt wächst spürbar.

Von Beginn an war es mir ein zentrales Anliegen, den direkten, persönlichen Austausch mit den handelnden Personen im Verband zu suchen – in den Landesgruppen, in den Gremien und im Präsidium. Dabei habe ich erlebt, mit wie viel Engagement, Fachwissen und Ideenreichtum unsere Mitglieder ihre Aufgaben wahrnehmen. Dieser interne Dialog ist für mich das Fundament unserer Arbeit: Nur wenn wir im Inneren gemeinsam und geschlossen agieren, können wir nach außen mit einer klaren, überzeugenden Stimme sprechen.

Auf politischer Ebene ist es gelungen, erste Akzente zu setzen. Sowohl in Berlin als auch in den Ländern spüre ich ein wachsendes Interesse an unserer Branche. Gleichzeitig wird deutlich: Es gibt noch immer Informationslücken – insbesondere in Bezug auf unser breites Leistungsspektrum, die Qualifikationsstandards unserer Beschäftigten und unseren wichtigen Beitrag zur öffentlichen Sicherheit. Diese Lücken zu schließen, sehe ich als eine der Kernaufgaben für die kommenden Jahre.

Besonders interessant war für mich, manche bekannten Gesprächspartner aus der neuen Perspektive des Präsidenten neu kennenzulernen. Unternehmen, öffentliche Auftraggeber, politische Institutionen, Partnerverbände und Vertreter der Wirtschaft – all diese Akteure bringen eigene Sichtweisen, Erwartungen und Rahmenbedingungen mit. Unsere Aufgabe als Verband ist es, diese unterschiedlichen Perspektiven in einer klaren Strategie zu verbinden und daraus tragfähige Lösungen zu entwickeln.

Sehr positiv stimmt mich die Bereitschaft vieler Mitglieder, sich aktiv einzubringen – sei es in fachlichen Diskussionen, bei der Entwicklung von Positionen oder durch die Weitergabe erprobter guter Praxis. Hier zeigt sich die Stärke unserer Gemeinschaft: Wir verfügen über eine solide Basis, auf der sich Zukunft gestalten lässt. Aus dieser Basis erwächst nicht nur Stabilität, sondern auch die Chance, gemeinsam neue Wege zu gehen.

Das Motto meiner Kandidatur „Besser zusammen" begleitet mich in jeder dieser Begegnungen. Ich bin überzeugt, dass gerade in den großen Herausforderungen unserer Zeit die größte Chance und das größte Potenzial in der Zusammenarbeit liegen – in der Verbindung unterschiedlicher Kompetenzen, Erfahrungen und Perspektiven.

Für die kommenden Monate habe ich mir vorgenommen, die Sichtbarkeit unserer Branche weiter zu erhöhen – in der Politik, in der breiten Öffentlichkeit und in allen relevanten gesellschaftlichen Debatten. Wir wollen zeigen, dass die Sicherheitswirtschaft nicht nur unverzichtbar ist, sondern auch modern, innovativ und lösungsorientiert arbeitet.

Nähe entsteht nicht zufällig. Sie wächst durch kontinuierlichen, verlässlichen Dialog, durch klare Botschaften und durch ein gemeinsames Ziel: die Zukunft unserer Branche aktiv und nachhaltig zu gestalten. Genau daran möchte ich – gemeinsam mit Ihnen – arbeiten.

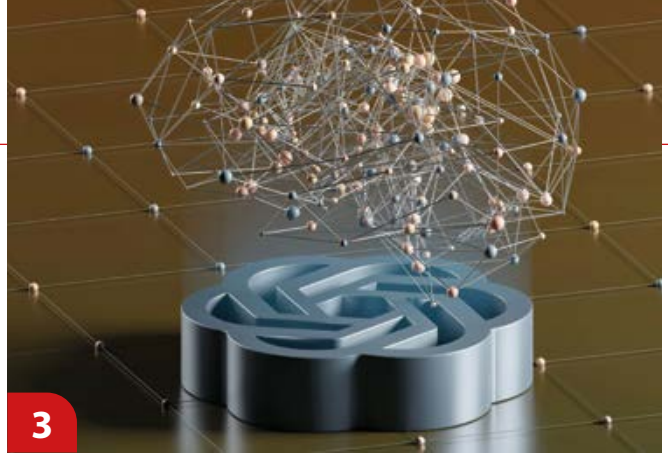
#besserzusammen

Ihr

Werner Landstorfer

Werner Landstorfer
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.

BDSW-Techniktagung 2025 in Raunheim: „KI – und jetzt?“

Von Stefan Rauschen

Ich freue mich, dass ich erneut für unseren BDSW-Fachausschuss Technik zur Techniktagung einladen darf. Am **4. und 5. November 2025** sind im **Hotel NH Frankfurt Airport West** (Kelsterbacher Straße 19, 65479 Raunheim) die Räume und Übernachtungsmöglichkeiten reserviert. Für unser Lunch-to-Lunch-Format hat der Vorstand des Fachausschusses Technik wieder spannende Themen und Vorträge sowie eine große Begleitausstellung organisieren können.

„KI – und jetzt?“ Chancen und Risiken für die Sicherheitswirtschaft – so lautet das Leitmotiv unserer Tagung.

Was erwartet die Teilnehmer an den beiden Tagen?

Am 4. November 2025 treffen wir uns ab 11 Uhr im Ausstellerbereich. Neben den Ausstellungspartnern und dem Networking erwartet uns auch eine erste Stärkung. Um 12 Uhr starten wir in das Tagesprogramm.

Wir freuen uns ganz besonders, dass BDSW-Präsident Werner Landstorfer seine Teilnahme zugesagt hat. Er möchte sich persönlich ein Bild von unserer Arbeit machen und auch für ein Grußwort konnten wir ihn gewinnen.

Gegen 12:30 Uhr können wir einen Gast aus Brüssel begrüßen. Alexander Frank, stellv. Generaldirektor des europäischen Dachverbandes des privaten Sicherheitsgewerbes, der CoESS – Confederation of European Security Services, hat seinen Vortrag „Der EU AI Act und die Sicherheitswirtschaft: Europäische Perspektiven und Leitlinien“ überschrieben. Wir sind auf die Aus- und Einblicke in die europäische Sichtweise gespannt.

Ab 13 Uhr freuen wir uns auf die Präsentation der Firma Jungmann Systemtechnik GmbH & Co. KG. Oliver Bender nimmt uns mit in eine innovative Leitstelle. „Der Kontrollraum der Zukunft im Spannungsfeld von Demografie, Digitalisierung und KI“ lautet sein Thema.

Stefan Rauschen

Vorsitzender des Fachausschusses Technik im BDSW und Geschäftsführer der Wach- und Schließgesellschaft mbH & Co. KG, Mönchengladbac h

Bild: Igor Omilaev / unsplash.com

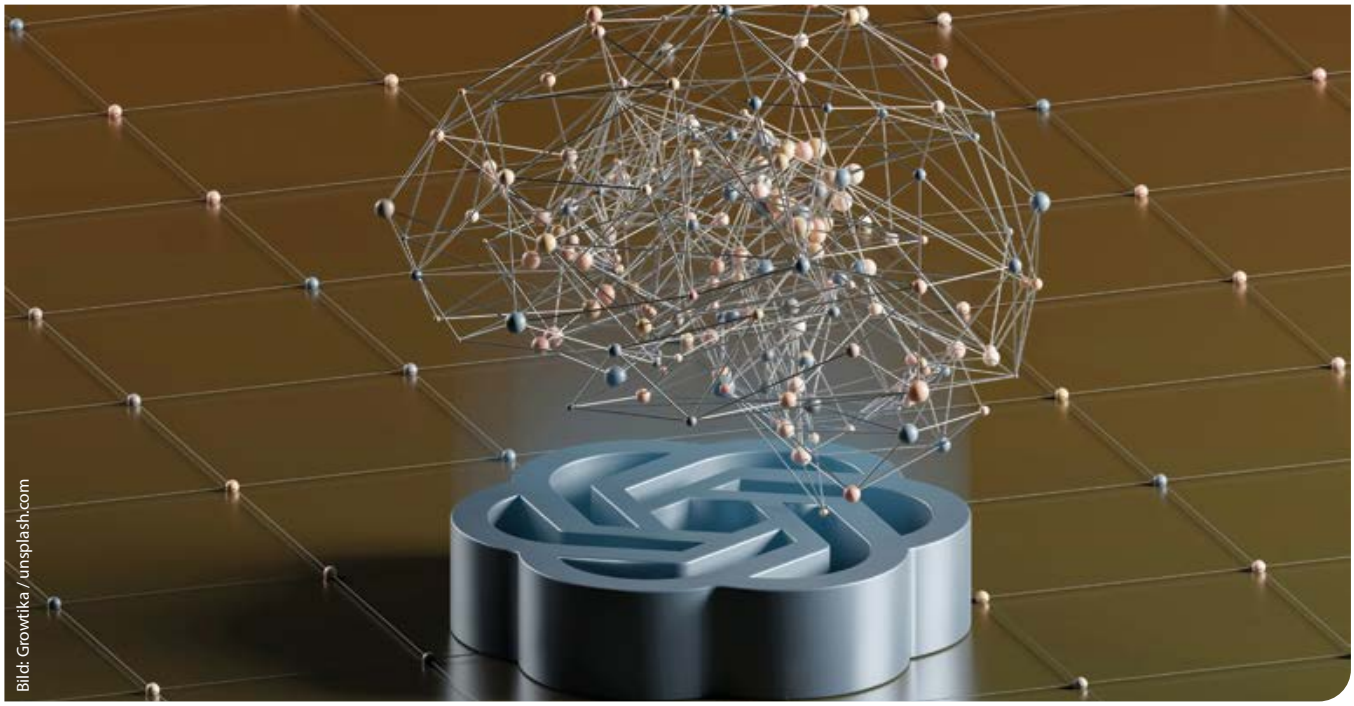


Bild: Growtika / unsplash.com

Nach einer Kommunikationspause wird ab 14:15 Uhr Dirk H. Bürhaus von der Kötter Security Gruppe über die Gefahren, Risiken und Aufgaben für unser Gewerbe berichten. Sein Vortrag „Cybersecurity – Herausforderungen für die private Sicherheitswirtschaft" wird uns in ein sehr wichtiges Themenfeld führen. Vielleicht ist auch Zeit für einen kurzen Ausflug zum neuen BDSW-Arbeitskreis „Cybersicherheit".

Ab 14:45 Uhr nimmt uns Peter Monte von der Firma Sitasys AG in die aktuellen Entwicklungen bei „Übertragung von personalisierten Daten bei der Zutrittskontrolle und Videoüberwachung" mit. Diese Problemstellung hat sich in komplett automatisierten Supermärkten und einer 24-stündigen Öffnungszeit ergeben. Herr Monte hat hier Lösungsmöglichkeiten im Portfolio.

Nach einer weiteren Kommunikationspause wird um 15:15 Uhr Günter Roggensack von der Firma Cyber Investigate das Wort ergreifen. Er wird uns den „Schutz von Netzwerken und Daten" näherbringen und auch die Wirksamkeit von Penetrationstests aufzeigen. Hier können wir uns auf praxisnahe Berichte freuen.

Im Anschluss läuten wir den Tagungsausklang ein, begrüßen die Teilnehmer noch einmal im Ausstellungsbereich zum kühlen Feierabendgetränk und widmen uns erneut dem Networking. Ab 18 Uhr laden wir dann zum gemeinsamen Abendessen und Tagesausklang im Tagungshotel ein.

Am 5. November 2025 treffen wir uns ab 9 Uhr im Ausstellungsbereich und starten dann ab 9:30 Uhr in das Tagungsprogramm.

Um 9:45 Uhr berichtet uns Ralf Hettesheimer, Vice President Nonindustry Solutions, von der Empolis Information Management GmbH vom Forschungsprojekt „SPELL – KI in der vernetzten Leitstelle der Zukunft". Wir versprechen uns hier einen spannenden Blick in die Zukunft.

Ab 10:15 Uhr wird uns Markus Schroth, ATS Elektronik GmbH, aus Sicht eines Software Engineers den Blick auf „KI in modernen Einsatzleitstellen" schärfen. KI aus Sicht eines Anbieters eines Gefahrenmanagementsystems GMS verspricht weitere spannende Einblicke.

Nach einer ersten Kommunikationspause lautet der Vortrag „Gefahren aus der 3. Dimension". Patrick Sielski von der Securiton GmbH wird uns das Bedrohungsszenario und vermutlich auch Lösungsmöglichkeiten aufzeigen.

Nach der Verabschiedung wartet noch ein Imbiss im Ausstellerbereich und eine letzte Stärkung vor der Heimreise.

Wir können auch in diesem Jahr ein breites Themenfeld anbieten und sind sehr gespannt auf die Vorträge sowie auf neuen Input und auf inspirierende Fragerunden nach den Vorträgen.

Das Team des BDSW und der Vorstand des Fachausschusses Technik freuen sich auf die beiden Tage in Raunheim … und natürlich auf das Salz in der Suppe: auf viele gut gelaunte Teilnehmerinnen und Teilnehmer, Top-Networking und einen lebendigen Austausch.

Herzliche Grüße aus Mönchengladbach,
Stefan Rauschen

VdS 2311:2025-06 – Was ist neu? Was hat sich geändert?

Von Manuel Fritz-Lafrenz

Bei der turnusmäßig anstehenden Überarbeitung der VdS-Richtlinien für Planung und Einbau von Einbruchmeldeanlagen (EMA), den bekannten VdS 2311, standen diesmal drei Ziele im Vordergrund: Verbesserung der Lesbarkeit und Verständlichkeit, Einarbeitung von Erfahrungen aus der Errichterpraxis und Wünschen von Polizei, Versicherern und Verbänden sowie eine generelle Fokussierung der Inhalte. Dieser Beitrag stellt die wichtigsten Änderungen der neuen Auflage vor.

Bessere Unterscheidbarkeit bei den Abweichungen

Eine wichtige Rolle in den Richtlinien VdS 2311 spielt die Unterscheidung zwischen den sogenannten „zulässigen Abweichungen" und „unzulässigen Abweichungen". Zulässige Abweichungen sind – wie der Name bereits vermuten lässt – Abweichungen von den Richtlinien VdS 2311, die akzeptabel sind, um die Absicherung eines Objekts an die konkrete Risikolage anzupassen. Unzulässige Abweichungen hingegen sind selbst dann nicht akzeptabel, wenn alle Beteiligten (Betreiber, Versicherer etc.) bereit wären, sie zu tolerieren. In diesen Fällen darf kein VdS-Attest ausgestellt werden. Die Unterscheidung zwischen zulässig und unzulässig war bislang nur anhand beispielhafter Listen in den Anhängen ersichtlich und daher häufig Gegenstand kontroverser Diskussionen.

Neu: Klarstellung durch farbliche Hervorhebung

In der neuen Auflage wurde nun ein wenig Farbe ins Spiel gebracht, um den Errichterunternehmen die Unterscheidung von zulässigen und unzulässigen Abweichungen zu erleichtern: Alle Anforderungen, von denen abgewichen werden darf (also bei denen Abweichungen zulässig sind), sind wie bisher schwarz gedruckt. Anforderungen, von denen nicht abgewichen werden darf, werden zukünftig in blauer Schrift hervorgehoben. Dadurch ist nun auf den ersten Blick erkennbar, an welcher Stelle Abweichungen zulässig sind und an welcher nicht. Selbstverständlich müssen die zulässigen Abweichungen auch weiterhin dokumentiert werden und alle Beteiligten damit einverstanden sein.

Notstromversorgung

Praxiserfahrungen und Labortests haben gezeigt, dass selbst VdS-anerkannte Batterien zur Notstromversorgung von EMA aufgrund von Alterungsprozessen unvermeidbare Kapazitätsverluste erleiden. Die Produktnormen für diese Batterien fordern, dass sie am Ende der vom Hersteller angegebenen maximalen Lebensdauer noch über mindestens 80 Prozent der Nennkapazität verfügen müssen.

Diesem Umstand wurde in den neuen VdS 2311 Rechnung getragen: Bei der Auslegung der Notstromversorgung muss die Mindestkapazität um 25 Prozent überdimensioniert werden. Damit soll sichergestellt werden, dass auch nach vier Jahren noch die in den VdS 2311 geforderte Überbrückungszeit für Stromausfälle voll gewährleistet ist.

Akustische Signalgeber außen nun zulässig

Das Thema der akustischen Signalgeber an der Außenseite des überwachten Objekts (von Laien gerne Alarmsirenen genannt) war lange umstritten und daher auch in den VdS 2311 über die Jahre einem Wechsel unterworfen. Mal waren sie erlaubt, mal nicht, zuletzt waren sie eine zulässige Abweichung. Dieser Komplexität tritt VdS nun entgegen: In VdS 2311:2025 ist die Außeninstallation grundsätzlich erlaubt, es muss keine zulässige Abweichung mehr vereinbart werden.

Fernzugriff auf EMA möglich

Bisher war der Zugriff auf eine EMA von Ferne nur bei Anwesenheit eines Mitarbeiters der Errichterfirma dieser Anlage vor Ort zulässig. Das stellte sich in der Praxis als nicht besonders praktikabel heraus und es gab schon lange Überlegungen,

Manuel Fritz-Lafrenz
Leiter der Abteilung Firmen und Fachkräfte bei der VdS Schadenverhütung GmbH

Die Erstveröffentlichung des Beitrags erfolgte in der Ausgabe 2/2025 der Zeitschrift s+s report.

https://vds.de/vds-verlag/s-s-report-das-vds-fachmagazin

Wir bedanken uns für die Abdruckgenehmigung.

Dieser QR-Code führt zur Übersichtsseite E-Learning des VdS-Bildungszentrum:

wie man Zugriffe aus der Ferne (auch Ferndienste oder Remote Services genannt) sicher möglich machen könnte. 2022 wurde mit der Normierung der „Anforderungen an die Bereitstellung von sicheren Ferndiensten für Brandsicherheitsanlagen und Sicherheitsanlagen“ in der DIN EN 50710 der Grundstein für sichere und damit auch für VdS akzeptable Fernzugriffe gelegt.

Regelung der Ferndienste in den Richtlinien VdS 2311:2025

Grundsätzliche Voraussetzung für den Fernzugriff auf eine VdS-anerkannte EMA nach VdS 2311 ist, dass der Errichter die Einhaltung der DIN EN 50710 nachweisen kann. Zusätzlich zum normgerechten Ferndienst wird gefordert, dass der Betreiber eine Freigabe für den Zugriff erteilt hat (zulässige Abweichung).

Keine Zukunft ohne Ferndienste

Für VdS ist klar, dass in Zukunft kein Weg um Remote Services herumführen wird. Denn Remote Services bieten Errichtern Vorteile wie Unterstützung in verschiedenen Phasen der Installation, Inspektion und Wartung, Erhöhung der Erfolgsquote bei Instandsetzungen und optimierte Ressourcennutzung. Betreiber von Sicherheitstechnik profitieren durch geringere Störungen, reduzierte Ausfallzeiten und schnellere Reaktionen auf Ereignisse.

Mit der neuen Auflage der VdS 2311 ist ein weiteres wichtiges VdS-Regelwerk zukunftsfähig gemacht worden.

Internsignalgeber ohne Abweichung zulässig

Bislang waren Internsignalgeber nicht für Externalarmierung im Innenbereich zugelassen. Zum Verständnis: „Intern-“ und „Extern-“ beziehen sich hier nicht auf den Montageort, sondern darauf, ob ein Signalgeber bei intern oder extern scharfer Anlage ausgelöst wird.

Wegen ihrer meist gefälligeren Optik wurden seit Jahren im Innenbereich gerne Internsignalgeber installiert, obwohl sie aufgrund ihrer technischen Spezifikationen die Anforderungen für die Externalarmierung nicht erfüllten und daher nicht zulässig waren. Diese Einschränkungen wurden nun aufgehoben und Internsignalgeber zur Externalarmierung sind grundsätzlich ohne Abweichung zulässig.

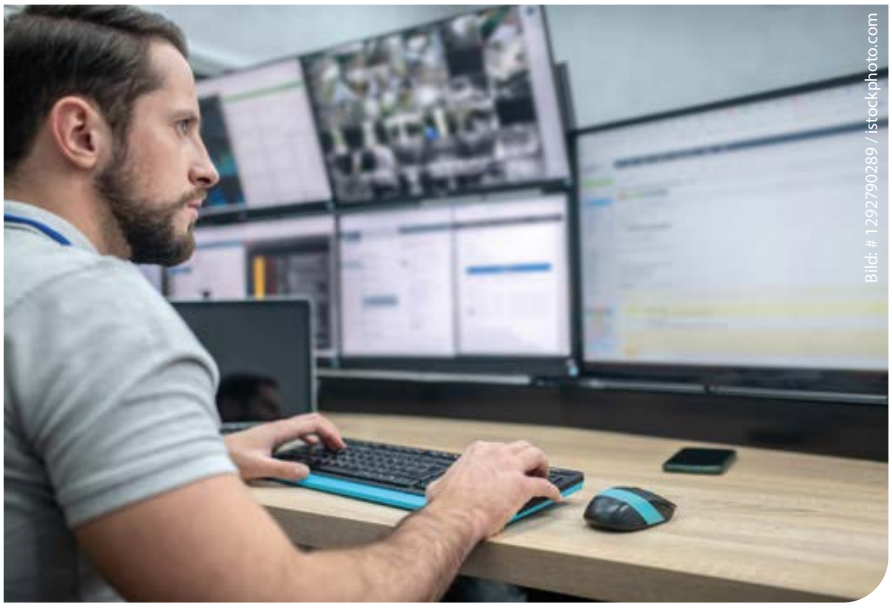


Bild: # 1292790289 / istockphoto.com

Die VdS 2311 gestatten Errichtern den Fernzugriff auf eine EMA, solange die Einhaltung der DIN EN 50710 nachgewiesen werden kann und der Betreiber seine Freigabe für den Zugriff erteilt hat.

Fallenmäßige Überwachung

Unter fallenmäßiger Überwachung von Räumen versteht man die Möglichkeit, einen unbemerkt eingedrungenen Täter mithilfe von Bewegungsmeldern innerhalb der Räume zu detektieren und doch noch zu „erwischen“. Dies erhöht die Sicherheit deutlich, daher ist die fallenmäßige Überwachung bei der Planung und Errichtung einer EMA ab Klasse B-SG2 in Zukunft zwingend notwendig (unzulässige Abweichung, blau gedruckt).

Weitere Änderungen in Kürze

Da es nicht möglich ist, hier alle Änderungen ausführlicher zu besprechen, folgen noch einige weitere Beispiele in Kurzform:

- Technische Meldergruppen dürfen nicht zur Detektion von Einbruchmeldungen verwendet werden. Dies war nach VdS 2311 schon immer unzulässig, in der Praxis wurde jedoch häufiger versucht, mithilfe der Technischen Meldung einen nicht VdS-konformen Einsatz von VdS-Meldern zu legitimieren. In den neuen VdS 2311 wird dies explizit ausgeschlossen.
- Die Scharf-/Unscharfschaltung von EMA via Sperrzeitsteuerung ist ersatzlos gestrichen worden. Dies war ohnehin ein Sonderfall, der beispielsweise bei Juwelieren relevant, aber selbst dort nicht sehr verbreitet war.
- Die Überwachung von Verteilern auf Öffnen wird als Anforderung von EMA der Klasse C auch auf Klasse B erweitert. Die Beschränkung dieser aus sicherheitstechnischer Sicht sinnvollen Funktion stammte noch aus einer Zeit, in der für jede Funktion separate Leitungsadern erforderlich waren, was zusätzliche Kosten verursachte.

Bild: # 1192103258 / istockphoto.com

Die Richtlinien VdS 2311, die die Planung und den Einbau von Einbruchmeldeanlagen regeln, sind im Juni 2025 in einer neuen Auflage erschienen, die viele Änderungen mit sich bringt.

- Mit der DIN EN 13306 wurde eine Norm für „Begriffe der Instandhaltung“ festgeschrieben, deren Neudefinition einiger Fachbegriffe aber das Verständnis für den Leser nicht wirklich erleichtern. Sie werden daher in den neuen VdS 2311 nur der Vollständigkeit halber aufgeführt. In den VdS-Richtlinien werden weiterhin die bisher gebräuchlichen Bezeichnungen wie Inspektion, Wartung oder Begehung verwendet.

Verschlankungskur

Wie schon mehrfach angeklungen ist, wurde bei der Überarbeitung der VdS 2311 darauf geachtet, unnötigen „Ballast" loszuwerden. So wurden Passagen, die lediglich erläuternden oder Hinweischarakter hatten, in die Technischen Kommentare Einbruchmeldetechnik (VdS 3134-2) überführt. Diese enthalten Hinweise, Erläuterungen und Klarstellungen zu Themen rund um die Einbruchmeldetechnik und können über **www.vds.de/techkomm** kostenlos bezogen werden. [Anmerkung der Redaktion: Weitere Informationen zu den Technischen Kommentaren auch im Beitrag auf Seite 45–47, s+s report 2/2025]

Fokussierung auf Planung und Errichtung

Eine weitere Maßnahme zur Straffung der Richtlinien war die Streichung produktspezifischer Anforderungen der Hersteller. Montagehinweise der Hersteller sind per Definition bindend, sodass diese nicht zusätzlich in einer VdS-Richtlinie erwähnt werden müssen. Zudem sind diese Hinweise heute z. T. so speziell, dass daraus häufig keine allgemeingültigen Anforderungen formuliert werden können.

Fazit

Die drei eingangs genannten Ziele bei der Überarbeitung der VdS-Richtlinien für Planung und Einbau von Einbruchmeldeanlagen sind eindeutig erreicht worden. Die neuen VdS 2311 sind lesbarer geworden, und der Einsatz von Farbe erleichtert das Verständnis. Sie sind nun deutlich fokussierter auf errichterspezifische Inhalte und praxisnäher. So stellt die neue Auflage der VdS 2311 einen wichtigen Schritt in die Zukunft für Errichter und VdS dar.

Online-Workshops für Errichter

Auch in diesem Jahr wird VdS wieder Online-Workshops zu Themen rund um Einbruchmeldetechnik anbieten. Diese Workshops richten sich an alle VdS-anerkannten EMAErrichter, die ihr Wissen erweitern und von den praktischen Erfahrungen aus dem VdS-Umfeld profitieren möchten. Natürlich wird dort auch auf die wichtigsten Änderungen und Neuerungen der VdS 2311 eingegangen. Alle Termine der hilfreichen Kurse werden auf der Seite des VdS-Bildungszentrums im Bereich „E-Learning" veröffentlicht: **https://bildung.vds.de/de/search.xhtml?tab=elearning** (siehe QR-Code), wo auch die Anmeldung stattfindet.

Die fallenmäßige Überwachung von Räumen mit Bewegungsmeldern ist in Zukunft ab Klasse B-SG$_2$ zwingend erforderlich.

Gültigkeit

Wichtig: Die neue Auflage der VdS 2311 ist ab dem 1. Juni 2025 gültig. Wie immer gibt es eine Übergangsfrist, die diesmal bis zum 31. Dezember 2025 läuft. Bis zu diesem Datum dürfen sich Errichter bei ihrer Arbeit noch an der Vorgängerversion der Richtlinien orientieren. Ab dem 1. Januar 2026 ist das dann nicht mehr möglich.

Bezug

Die neue Auflage der VdS 2311 „VdS-Richtlinien für Einbruchmeldeanlagen, Planung und Einbau" ist wie gewohnt im VdS-Webshop **www.vds-shop.de** erhältlich. Abonnenten der Richtlinien haben die neue Auflage bereits automatisch erhalten.

Vom Wachmann zum Hightechpartner

Die Transformation der Sicherheitswirtschaft

Von Ernst Steuger

Ernst Steuger

Geschäftsführer der Nürnberger Wach- und Schließgesellschaft mbH (NWS)

https://digital.nwsgmbh.de/

Die deutsche Wirtschaft steht an einem Wendepunkt. Der Mangel an Arbeitskräften ist kein temporärer Ausrutscher in einer sonst stabilen Lage – er ist ein strukturelles Phänomen, das nahezu alle Branchen dauerhaft verändern wird. Besonders betroffen ist die Sicherheitswirtschaft. Sie ist nicht nur Dienstleister, sondern tragende Säule für industrielle Abläufe, Kritische Infrastrukturen und die öffentliche Sicherheit. Ohne sie stünden Produktionslinien still, sensible Daten wären gefährdet und öffentliche Einrichtungen weniger geschützt.

Unsere Erfahrung bei der Nürnberger Wach- und Schließgesellschaft (NWS) zeigt die Dimension des Problems: Rund 2.500 Mitarbeiter sichern heute Objekte, Anlagen und Prozesse – und über 80 Stellen bleiben unbesetzt. Das ist kein Einzelfall, sondern Ausdruck eines Trends, den Prognosen noch verschärfen: Jährlich könnten bis zu 500.000 Menschen aus dem deutschen Arbeitsmarkt ausscheiden. Für eine personalintensive Branche wie die unsere ist das ein unüberhörbares Alarmsignal.

Die Kernfrage lautet: Wie halten wir unser Leistungsniveau, wenn die personellen Ressourcen schwinden?

Technologie als Partner – nicht als Ersatz

Unsere Antwort ist klar: Durch intelligente Kombination von menschlicher Expertise und technologischer Unterstützung. Robotik, Digitalisierung und künstliche Intelligenz (KI) sind keine Bedrohung, sondern strategische Werkzeuge. Sie entlasten bestehendes Personal, optimieren Prozesse und schaffen die Basis für nachhaltiges Wachstum – ohne den Menschen aus der Gleichung zu nehmen.

Sicherheitstechnik aus einer Hand

Unser technologisches Engagement beginnt mit modernster Sicherheitstechnik. Wir bieten unseren Kunden ein breites Portfolio – von hochauflösenden Videoüberwachungssystemen über intelligente Zutrittskontrollen bis hin zu vernetzten Gefahrenmeldesystemen. Unser Ansatz ist dabei ganzheitlich: Wir analysieren die individuellen Anforderungen eines Standorts, entwickeln maßgeschneiderte Sicherheitskonzepte und integrieren Hard- und Software so, dass ein reibungsloses Zusammenspiel aller Komponenten gewährleistet ist.

Sicherheit verstehen wir nicht als starres Konstrukt, sondern als dynamischen Prozess, der sich permanent an neue Bedrohungslagen, gesetzliche Vorgaben und technologische Möglichkeiten anpasst.

Eigene Entwicklung von Sicherheitsrobotern

Ergänzend zu dieser Sicherheitstechnik haben wir nach fast fünf Jahren intensiver Entwicklungsarbeit unsere eigenen Sicherheitsroboter zur Einsatzreife gebracht. Diese autonomen Systeme können auf weitläufigen Arealen selbstständig Patrouillen durchführen, Auffälligkeiten in Echtzeit erkennen und unmittelbar an die Leitstelle melden.

Sie sind zuverlässig, witterungsunabhängig und skalierbar – und vor allem: Sie ermöglichen es, hoch qualifiziertes Sicherheitspersonal gezielt dort einzusetzen, wo menschliche Präsenz unverzichtbar ist. So entsteht eine neue Arbeitsteilung, in der Roboter Routineaufgaben übernehmen und unsere Fachkräfte sich auf anspruchsvolle, situationsabhängige Tätigkeiten konzentrieren können.

Parallel dazu haben wir eine digitale Pförtnerlösung entwickelt, die das klassische Besuchermanagement neu denkt. Prozesse wie Identitätsprüfung, Ausweiserstellung und Dokumentation lassen sich heute vollständig digital und mobil abwickeln. Das spart nicht nur Kosten, sondern schafft operative Flexibilität – ein Vorteil, den Industrieunternehmen ebenso schätzen wie öffentliche Institutionen.

Automatisierung im eigenen Haus

Der Wandel macht auch vor internen Abläufen nicht halt. KI-gestützte Dokumentenverwaltung, digitale Assistenten und selbstlernende Prozesse helfen uns, Routineaufgaben zu reduzieren und die Reaktionsgeschwindigkeit in operativen Einsätzen zu erhöhen. Dadurch gewinnen wir Zeit – und Zeit ist in der Sicherheitswirtschaft oft der entscheidende Faktor zwischen Vorfall und Schadensvermeidung.

KI ist für uns kein Selbstzweck. Wir begreifen sie als Werkzeug, das menschliche Arbeit aufwertet. Die Frage ist nicht, ob sie genutzt wird, sondern wie – und mit welchem Ziel. Richtig eingesetzt, kann sie die Arbeit nicht nur effizienter, sondern auch menschlicher machen, weil sie Routine und Monotonie reduziert und Freiraum für komplexe, zwischenmenschliche Aufgaben schafft.

Neue Rolle der Sicherheitswirtschaft

Die technische Modernisierung allein reicht nicht aus. Die Sicherheitswirtschaft muss sich strategisch neu positionieren: Als unverzichtbarer Bestandteil unternehmerischer und gesellschaftlicher Resilienz. In einer Welt, in der geopolitische Spannungen, Cyberbedrohungen und Abhängigkeiten von digitalen Infrastrukturen zunehmen, ist Sicherheit ein Wettbewerbsfaktor. Investoren, Unternehmen und staatliche Einrichtungen erwarten heute, dass Schutzmaßnahmen jederzeit verlässlich funktionieren – ob im Forschungszentrum, am Produktionsstandort oder im Versorgungsbetrieb.

Damit rückt die Branche vom Rand in das Zentrum der Wertschöpfungsketten. Diese neue Rolle erfordert eine stärkere Vernetzung mit anderen Wirtschaftszweigen, eine fundierte Auseinandersetzung mit technologischen Standards und klare politische Rahmenbedingungen. Wirtschaft und Politik müssen den Beitrag der Sicherheitswirtschaft zur Standortattraktivität erkennen und aktiv fördern. Hier entscheidet sich, ob Deutschland seine Sicherheitsbranche als global wettbewerbsfähigen Innovationsmotor aufstellt oder ob wir bei der technologischen Transformation ins Hintertreffen geraten.

Der Mensch bleibt im Zentrum

Trotz aller Automatisierung bleibt eines klar: Sicherheit ist und bleibt ein zutiefst menschliches Bedürfnis – und die Verantwortung dafür lässt sich nicht vollständig an Maschinen delegieren. Technologie ist unser Partner, nicht unser Ersatz. Sie erweitert unsere Fähigkeiten, ersetzt aber nicht den geschulten Blick, die Erfahrung und das Urteilsvermögen unserer Fachkräfte.

In diesem Sinne bedeutet der Roboter in der Nachtschicht nicht das Ende menschlicher Arbeit, sondern ihren nächsten Entwicklungsschritt. Wenn wir diesen Weg bewusst gestalten, können wir die Sicherheitswirtschaft nicht nur stabilisieren, sondern sie zu einem Innovationsträger machen, der weit über seine eigene Branche hinaus wirkt – und damit nicht nur für Sicherheit, sondern auch für Vertrauen und Zukunftsfähigkeit steht.

CEIA OPENGATE®

Mobiles Waffendetektionssystem für Großveranstaltungen, Events und Kritische Infrastrukturen

Ein neues Maß an modernster und effizienter Waffendetektionstechnologie. OPENGATE ist ein mobiles und vollautomatisches elektromagnetisches Detektionssystem, konzipiert für eine schnelle sowie präzise Sicherheitskontrolle für Events, Stadien, Großveranstaltungen, Kritische Infrastrukturen und mehr.

Das portable und kontaktlose Waffenerkennungssystem ist nicht nur innovativ und revolutionär – es ist eine bewährte Technologie, die bereits weltweit an verschiedensten Zugangskontrollstellen erfolgreich eingesetzt wird.

Neben dem flexiblen und offenen Charakter des OPENGATE war es die Zielsetzung, höchste Personendurchsätze zu ermöglichen und gleichzeitig schwerwiegende Bedrohungen wie großkalibrige Schusswaffen oder metallhaltige Sprengvorrichtungen zu detektieren. Durch die Akkulaufzeit bis zu 14 Stunden ist das System ideal einsetzbar, um flexibel überall dort die Sicherheit zu erhöhen, wo größere Personenströme schnellstmöglich kontrolliert werden sollen, ohne persönliche Gegenstände ablegen zu müssen. Dies trägt dazu bei, dass die Warteschlangen in Bewegung bleiben, ohne dass die Leute ihre Taschen leeren oder Gegenstände entfernen müssen, was den Einlass schneller und reibungsloser macht.

Die Herausforderung bei der Entwicklung des Systems lag darin, eine hohe Detektionsleistung auf größere metallhaltige Gefahrenquellen bei gleichzeitiger höchster Diskriminierung von Objekten wie Smartphones, Uhren, Gürtel, aber auch Gepäckstücken, Rucksäcken, Taschen und deren Inhalt wie bspw. Notebooks, Tablets, Thermoskannen usw. zu garantieren, sodass praktisch keine Störalarme durch persönliche Gegenstände ausgelöst werden.

Die Darstellung von Alarmen erfolgt akustisch und visuell über eine 360°-LED-Anzeige und über eine eigene App, in der alle Einstellungen bzw. Detektionsparameter angepasst werden können. Grundsätzlich ist keine aufwendige und zeitintensive Installation notwendig. OPENGATE misst sich selbstständig auf den Standort ein und ist innerhalb weniger Sekunden einsatzbereit. Während des Betriebs führt das System ständige Selbstdiagnosen durch, um eine reibungslose Funktion während der Nutzung sicherzustellen.

Die Einsatzmöglichkeiten von OPENGATE erstrecken sich von Fußballarenen, Museen, Themenparks, Festivals, Messen, Kongressen, Bahnhöfen bis hin zu diversen Großveranstaltungen unterschiedlichster Art. Zudem kann das System für Pre-Screenings vor den eigentlichen Personenkontrollen am Eingang genutzt werden (z. B. am Flughafen), um auch in bisher unkontrollierten Bereichen die Sicherheit zu erhöhen. Das System lässt sich innerhalb von einer Minute aufstellen, sodass man kurzfristig auf veränderte Situationen schnell reagieren kann.

CEIA hat in intensiver Zusammenarbeit mit amerikanischen Sicherheitsbehörden ein flexibles, mobiles und smartes System entwickelt, das die heute beste-

henden Limitierungen hinter sich lässt. Es entspricht der Empfehlung der EU-Kommission 2023/1468 in den Normen 1 und 2. Zusammenfassend hilft das OPENGATE bei jeglichen Anwendungsfällen, bei denen größere Menschenansammlungen vorzufinden sind, die schnell, einfach und bei höchstem Durchsatz mit Sicherheitspersonal kontrolliert werden sollen. Gerne berät Sie die CEIA GmbH bei Rückfragen und sendet weitere detailliertere Informationen zu.

Einführung in automatisierte, kontaktlose und unaufdringliche Personenkontrolle

Durch die Technologie ist es möglich, Personen kontaktlos, schnell sowie ohne das Ablegen von persönlichen Gegenständen wie Smartphones, Gürtel, Schmuck oder Schlüssel ohne aufkommende lange Warteschlangen auf Gefahren wie metallhaltige Waffen, große Messer/Beile oder Sprengkörper (IED) zu überprüfen.

Vielseitig und mobil, da keine Festinstallation notwendig

Das ca. 12 kg leichte System wird durch zwei Hochleistungsakkus betrieben und ist dadurch äußerst mobil, tragbar und schnell einsetzbar. Die hohe Portabilität erlaubt den schnellen und einfachen Standortwechsel. OPENGATE ist vielseitig einsetzbar für In-/Outdooranwendungen.

Technologischer und zeitsparender Fortschritt

Das OPENGATE ermöglicht einen extrem hohen Personendurchsatz mit bis zu 3.000 Personen pro Stunde. Durch die Ausblendung von persönlichen Gegenständen ist die Sicherheitskontrolle wesentlich schneller im Vergleich zu einer Handkontrolle und zweifelsohne sicherer, da hier alle Körperzonen von Kopf bis Fuß vollumfänglich detektiert werden.

Integration von Web Access/ Remote-Steuerung

Mit der CEIA OPENGATE-App ist es möglich, individuelle Einstellungen wie z. B. Änderung des Alarmtons oder Sicherheitslevel vorzunehmen, um auf mögliche eintretende Veränderungen sofort reagieren zu können. Mit einem Cloud-Verwaltungssystem kann OPENGATE zudem extern gesteuert und überwacht werden. Es ermöglicht die begleitende digitale Verwaltung einzelner oder mehrerer Standorte. Der Zugriff ist von jedem Smartgerät oder Computer mit Webzugriff möglich. Zusätzlich ist das System mit einem hochpräzisen Durchgangszähler für spätere Statistikauswertung ausgestattet.

Zusätzliche Nutzung als Werbefläche möglich

CEIA OPENGATE bietet zudem die Option als Werbe-/Sponsorfläche. Mittels passgenauer Sleeves können die Säulen verkleidet werden und dienen als unübersehbare Werbung.

CEIA ist als weltweit führendes Unternehmen der Metalldetektionstechnologie und Entwicklung aktiv und fertigt seit über 50 Jahren patentierte Hochleistungsdetektoren für verschiedenste Anwendungen und Kunden. Die Produktpalette umfasst u. a. Metalldetektoren zum Schutz von sensiblen Gebäuden, Events/Großveranstaltungen wie Festivals oder Messen, Flugseehäfen, Gerichte, Haftanstalten sowie Systeme zur Vermeidung von Diebstahl in industriellen Umgebungen.
CEIA bietet ein weltweites Netzwerk aus Ansprechpartnern und ergänzt dies durch zertifizierte Schulungsangebote, die in Kombination die bestmögliche Nutzung und Wartung Ihrer Geräte garantieren.
Die CEIA GmbH mit Sitz in Wiesbaden steht für Rückfragen gerne für Sie zur Verfügung.

Kontakt:
CEIA GmbH
Peter-Sander-Straße 37A
55252 Wiesbaden
Tel.: +49 61 34/2 10 99-0
Mail: info@ceia.net
Web: www.ceia.net

Wie VR und KI die Sicherheitsbranche verändern

Von Pavel Druzhkov

Pavel Druzhkov
Geschäftsführer der SkillCampVR

www.skillcampvr.com

Viele kennen das: Es steht mal wieder eine Fortbildung im Arbeitsalltag an. Stundenlang im Seminarraum sitzen und aufmerksam dem Dozenten und seinem Vortrag folgen – sieht so nicht bis heute der allgemeine Schulungsalltag aus? Es werden zwar wichtige Inhalte vermittelt, die eigentlich als Basis für die tägliche Arbeit dienen. Doch bleibt oft die Frage: Wie lässt sich das Gelernte praktisch anwenden? Und gelingt es, das Wissen später im Arbeitsalltag umzusetzen?

Eine Antwort ist: Schulungen mithilfe von virtueller Realität (VR) zu erleben. Plötzlich ändert sich die Situation grundlegend. Statt nur zuzuhören und zu beobachten, kann direkt interaktiv gelernt und Theorie in Praxis umgesetzt werden. In der VR werden Szenarien simuliert, die sonst selten so realistisch erlebt werden können. Fehler können gemacht werden und bieten so die Möglichkeit, daraus zu lernen und die eigenen Fähigkeiten gezielt zu verbessern.

Die fortschreitende Entwicklung von VR und künstlicher Intelligenz (KI) verändert zunehmend die Arbeitswelt. Auch in der Sicherheitsbranche eröffnen diese Technologien neue Chancen für flexiblere und wirksamere Formen der Schulung.

Klassische Schulungen in der Sicherheitsbranche stoßen an ihre Grenzen

Viele Schulungen konzentrieren sich noch immer hauptsächlich auf theoretisches Wissen und bieten kaum Möglichkeiten für praktische Übungen. Für Sicherheitskräfte ist das problematisch, da ihre Arbeit den sicheren Umgang mit oft unvorhersehbaren Situationen verlangt. Reine Theorie reicht nicht aus, um in kritischen Momenten richtig und effektiv zu handeln.

Auszug aus einem Training, in dem Sicherheitspersonal lernt, auf Notfälle zu reagieren – eine Situation, die in der Realität nur schwer trainierbar ist.

Hinzu kommt, dass Zeit und Ressourcen für praktische Übungen oft fehlen. Gefährliche Situationen können nur eingeschränkt trainiert werden, da die Sicherheit der Teilnehmenden und der Umgebung gewährleistet sein muss. So erleben viele Beschäftigte die tatsächlichen Anforderungen erst im Einsatz.

Auch die Ansprüche von Behörden und Kunden wachsen stetig. Trainings müssen umfassender und praxisnäher werden, was mit klassischen Methoden zunehmend schwieriger umzusetzen ist.

Außerdem macht der Fachkräftemangel die Situation noch schwieriger, weil neue Mitarbeiter schneller eingearbeitet werden müssen. Das wirkt sich nicht nur auf die Qualität der Arbeit aus, sondern erhöht auch das Risiko von Fehlern im Einsatz.

Virtual Reality hilft dabei, diese Herausforderungen zu überwinden

VR eröffnet Mitarbeitenden ganz neue Wege, praktische Erfahrungen zu sammeln. Sie werden in typische, aber auch seltene Einsatzszenarien versetzt und trainieren wichtige Entscheidungen und Handlungen ohne Gefährdung der realen Umgebung. Fehler sind dabei nicht nur erlaubt, sondern werden zum wertvollen Lerninstrument, denn sie können in der virtuellen Welt genau analysiert und gezielt verbessert werden.

Das Lernen macht mehr Spaß und hilft, konzentriert zu bleiben. Die Trainings können überall und jederzeit stattfinden, sodass sie gut in den Arbeitsalltag passen. Gerade jüngere Mitarbeitende sind oft offener für neue Technologien und profitieren besonders von der interaktiven und immersiven Gestaltung der Trainings.

Virtual Reality verändert das Training in der Luftfahrtsicherheit

Die komplexen Abläufe an Flughäfen und die hohen Sicherheitsanforderungen erfordern eine intensive Vorbereitung des Personals. Hier kommt VR ins Spiel: In einer realitätsnahen Umgebung trainieren Mitarbeitende und Auszubildende die Kontrolle von Personen und Gepäck, üben die Prüfung von Waren und lernen, gefährliche oder verbotene Gegenstände sicher zu erkennen.

Mit VR lassen sich Ausbildungsstandards leichter erreichen und Prüfungen werden seltener nicht bestanden. Spielerische Elemente steigern die Motivation und realistische Simula-

tionen nehmen die Angst vor der Prüfung. Unternehmen profitieren doppelt: Sie sparen Kosten und entlasten ihre Trainer. Gleichzeitig steigt die Attraktivität als Arbeitgeber – ein echter Pluspunkt bei Ausschreibungen.

Genau das betont auch Markus Krügl, Head of Training bei der Securitas Aviation Akademie: *„Wir nutzen die VR-Lösungen in Zukunft als Erweiterung des Methodenkoffers für unsere Ausbilderinnen und Ausbilder – als Angebot und Möglichkeit, Lernen ganz neu zu erfahren – spannend, intuitiv und nachhaltig – so werden Lernpfade bei unseren Teilnehmenden ganz neu besetzt. Das Lernen der Zukunft."*

Auch klassische Sicherheitsdienste nutzen Virtual Reality

Im Bereich der klassischen Sicherheitsdienste, wie Objektschutz und Veranstaltungssicherheit, wird VR-Training ebenfalls genutzt. Unternehmen wie All Service Sicherheitsdienste und secura protect nutzen VR-Module, um grundlegende Abläufe und unterschiedliche Einsatzsituationen effektiv zu trainieren.

Serife Tülay Alkan-Haller, Prokuristin der All Service Sicherheitsdienste, lobt vor allem den unkomplizierten Ablauf der Kooperation und den Praxisbezug der Inhalte: *„Die Zusammenarbeit ist unkompliziert und äußerst flexibel. Die Trainingsinhalte sind fundiert und praxisnah. Besonders der Einsatz der VR-Brille hat sich als motivierendes Zusatztool für unsere Mitarbeitenden erwiesen."*

Bei secura protect richtet sich der Blick verstärkt auf den generationsübergreifenden Einsatz der Technologie. Geschäftsführer Vladimir Korneev beschreibt, wie sich VR in Teams mit ganz unterschiedlichen Erfahrungsstufen etabliert: *„Natürlich sehen wir, dass jüngere Mitarbeitende besonders schnell mit VR zurechtkommen. Aber auch erfahrene Kolleginnen und Kollegen sind offen und oft sogar überrascht, wie selbsterklärend das Bedienen von den Brillen ist."*

Mit KI und VR in eine neue Trainingsdimension

Gemeinsam mit Securitas entwickelt SkillCamp einen intelligenten Assistenten, der Trainings nicht nur begleitet, sondern aktiv mitgestaltet. Das Besondere: Der smarte Assistent beantwortet unmittelbar fachliche Fragen, liefert situationsbezogene Antworten und greift auf zertifizierte Inhalte wie die DIN 77200, den § 34a GewO oder firmeninterne Standards zurück.

Während des Trainings erkennt das Programm automatisch typische Lernmuster, analysiert Leistungsdaten und macht Vorschläge für gezielte Weiterbildungen. Was vor Jahren noch nach einer Vision klang, wird Realität und bietet direkte Vorteile für Unternehmen und Mitarbeiter.

„Der Assistent bietet schnelle, situationsbezogene Unterstützung direkt vor Ort bei Unsicherheiten, Nachfragen oder in kritischen Momenten. Gleichzeitig erkennt er individuelle Lernbedarfe und empfiehlt passgenaue Ergänzungstrainings, abgestimmt auf Standort, Aufgabenbereich, Verantwortungsniveau und den konkreten Einsatzort der Securitas Mitarbeiter", sagt Dominik Contes, Leiter der Securitas Sicherheitsfachschule.

Wer frühzeitig auf diese Technologien setzt, profitiert von einer besseren Qualifikation ihrer Mitarbeitenden und einer höheren Anpassungsfähigkeit an die Herausforderungen der modernen Sicherheitslandschaft.

SPELL – KI im Einsatz- und Lagemanagement

Von Ralf Hettesheimer

Ralf Hettesheimer

hat an der Universität Kaiserslautern Informatik studiert und verantwortet als Vice President Delivery bei der Empolis Intelligent Views GmbH, Darmstadt Entwicklungsprojekte für große Behördenkunden.

www.empolis.com

Leitstellen sind das Nervenzentrum vieler kritischer Infrastrukturen – von Rettungsdiensten über Industrieanlagen bis hin zu großen Gebäudekomplexen. Schon im normalen Betrieb müssen sie bis zu 200 Meldungen pro Stunde verarbeiten. Tritt jedoch eine Großschadenslage ein, sind schnelle Entscheidungen über Sektor- und Organisationsgrenzen hinweg gefragt – und das unter Einhaltung aller gesetzlichen Vorgaben. Globale Entwicklungen wie Klimawandel, Urbanisierung und weltweite Vernetzung lassen Krisen häufiger auftreten und ihre Auswirkungen schwerwiegender werden. Fehlen in solchen Momenten integrierte Informationsflüsse, steigt das Risiko von Überlastung und Fehlentscheidungen deutlich. Ein wirksames Krisenmanagement muss deshalb Gefahrenabwehr, Infrastruktur, Wirtschaft, Lieferketten und Bevölkerung gemeinsam in den Blick nehmen. Dafür sind präzise Analysen in Echtzeit und vernetzte Systeme entscheidend – doch in der Praxis überwiegen bislang Insellösungen, und künstliche Intelligenz wird bestenfalls innerhalb der Insellösungen genutzt. Genau an diesem Punkt setzte das vom BMWK Bundesministerium für Wirtschaft und Klimaschutz (Heute: BMWE Bundesministerium für Wirtschaft und Energie) geförderte Forschungsprojekt SPELL an. SPELL startete im Juni 2021 und war auf eine Dauer von drei Jahren ausgelegt. Empolis war als Technologiepartner an SPELL beteiligt.

SPELL ist die Semantische Plattform zur intelligenten Entscheidungs- und Einsatzunterstützung in Leitstellen und Lagezentren. Ziel ist es, in Krisensituationen (beispielsweise Großschadensereignissen, Pandemien, Naturkatastrophen oder flächendeckenden Stromausfällen) Maßnahmen zur Gefahrenabwehr, Nothilfe und Versorgung für die Bevölkerung schneller und situationsgerecht zu koordinieren. Dies soll mithilfe von künstlicher Intelligenz erreicht werden.

Es ist notwendig, dass wir in Krisensituationen unsere Ressourcen richtig verteilen und auf Basis der vorhandenen Informationen die richtigen Entscheidungen treffen. Eine Voraussetzung dafür ist eine umfassende Übersicht aller relevanten Informationen als Gesamtlagebild und die Vernetzung aller Beteiligten. Das zeigte uns auch gerade die Coronapandemie. Eine fundierte und gute Entscheidung braucht viele Daten für ein umfassendes Lagebild – eine Krise verlangt hingegen nach schnellen Entscheidungen. In diesem Spannungsfeld zwischen guten und schnellen Entscheidungen kann künstliche Intelligenz einen wesentlichen Beitrag leisten, indem durch die KI eine umfangreiche Datenlage berücksichtigt und für die Entscheidungsfindung kompakt aufbereitet dargestellt werden kann.

Der Einsatz von KI im Bereich der Unterstützung von Leitstellen und Sicherheitsbehörden hat das Potenzial, die Sicherheit der Bevölkerung erheblich zu verbessern. Die Produkte und Technologien von Empolis spielen eine entscheidende Rolle bei der Bereitstellung innovativer Lösungen für eine effektive Reaktion auf Notfälle und die Gewährleistung einer sicheren Umgebung.

Durch den Einsatz von KI können Behörden proaktiv agieren, effizient kommunizieren und ihre Ressourcen optimal nutzen. Es ist klar, dass KI einen tiefgreifenden Einfluss auf die Zukunft der Sicherheit hat und die Bevölkerung in vielerlei Hinsicht schützen kann.

Präzise Lagebewertung und Situationsanalyse

Die Fähigkeit, komplexe Daten in Echtzeit zu analysieren, ist entscheidend für die effektive Entscheidungsfindung in Notfallsituationen.

Eine schnelle Entscheidungsfindung in Krisensituationen ist entscheidend, da sie direkten Einfluss auf den Verlauf und die Auswirkungen der Krise hat. Krisen entwickeln sich dynamisch und unvorhersehbar. Das unterscheidet sie von normalen Notfallsituationen. Durch rasche Entscheidungen können potenzielle Schäden mini-

miert, Menschenleben gerettet und effektive Maßnahmen zur Bewältigung der Krise ergriffen werden. Verzögerungen können hingegen schwerwiegende Folgen für den weiteren Krisenverlauf haben: Verschlimmerung der Situation, Ressourcenverschwendung oder erhöhtes Risiko für Betroffene. Eine schnelle Entscheidungsfindung basierend auf allen verfügbaren Informationen und Expertisen ist daher essenziell, um in einer Krisensituation angemessen zu handeln.

Empolis bietet Lösungen, die mithilfe von KI-Verfahren große Mengen an Informationen aus unterschiedlichen Quellen sammeln, verarbeiten und analysieren können. Dadurch werden Leitstellen in die Lage versetzt, eine präzise Lagebewertung durchzuführen und umfassende Situationsanalysen vorzunehmen. Dies ermöglicht es den Sicherheitsbehörden, fundierte Entscheidungen zu treffen und ihre Einsatzkräfte optimal zu koordinieren.

Effektive Kommunikation und Informationsverteilung

Eine nahtlose und schnelle Kommunikation zwischen den Sicherheitsbehörden in Krisensituationen ist von entscheidender Bedeutung, da sie die Effektivität der Reaktion und Bewältigung der Krise maßgeblich beeinflusst. Eine reibungslose Zusammenarbeit ermöglicht den Informationsaustausch, den Abgleich von Daten und die Koordination von Ressourcen in Echtzeit.

Empolis bietet intelligente Kommunikationslösungen, die es den Leitstellen ermöglichen, wichtige Informationen in Echtzeit zu teilen. Dies verbessert die Zusammenarbeit zwischen verschiedenen Einsatzkräften und ermöglicht eine effiziente Verteilung von Aufgaben und Ressourcen.

Datenschutz und Ethik

Bei der Implementierung von GenAI im Sicherheitsbereich ist der Schutz von Daten und die Wahrung ethischer Grundsätze von größter Bedeutung. Sicherheitsbehörden verarbeiten sensible Informationen, und der Missbrauch dieser Daten kann schwerwiegende Folgen für Einzelpersonen und die Gesellschaft haben. Der Einsatz von GenAI kann potenziell neue Datenschutzrisiken mit sich bringen. Es ist daher unerlässlich, robuste Sicherheitsvorkehrungen zu implementieren, um den unbefugten Zugriff zu verhindern. Ebenso müssen ethische Grundsätze wie Fairness, Transparenz und Verantwortungsbewusstsein bei der Entwicklung und Anwendung von GenAI-Technologien gewahrt werden, um mögliche Diskriminierung und unerwünschte Konsequenzen zu vermeiden.

Empolis legt großen Wert auf Datenschutz und die Einhaltung rechtlicher Vorschriften. Die von Empolis entwickelten Produkte und Technologien stellen sicher, dass personenbezogene Daten vertraulich behandelt und nur für legitime Sicherheitszwecke verwendet werden.

Ergebnis des Projekts

Mit SPELL ist es gelungen, viele sehr unterschiedliche Partner an einen Tisch zu bringen und gemeinsam an einer neutralen Plattformidee zu arbeiten, die sektorenübergreifend nutzbar ist. In einem föderal geprägten Land wie Deutschland ist eine solche Lösung entscheidend, um bei großen Ereignissen schnell, koordiniert und vernetzt handeln zu können. Besonders bei der Datenintegration und den ersten KI-Diensten wurden wichtige Grundlagen geschaffen – ein Schritt hin zu besserer Zusammenarbeit im Krisenfall.

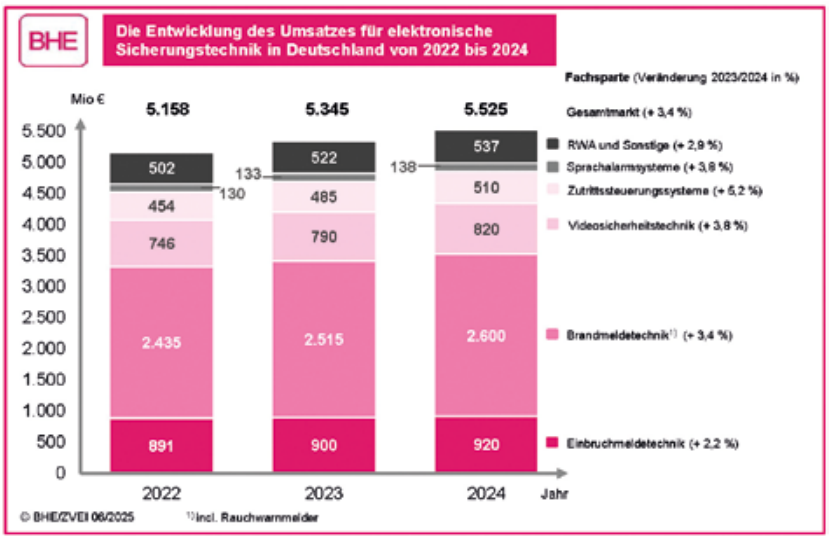
Wachstumstrend in der elektronischen Sicherheitstechnik setzt sich leicht abgeschwächt fort

www.bhe.de

Im vergangenen Jahr 2024 konnte der Markt für elektronische Sicherheitstechnik in Deutschland ein Umsatzplus von 3,4 Prozent auf etwas mehr als 5,5 Mrd. Euro verzeichnen.

„Die Sicherheitstechnik in Deutschland wächst in der Summe erneut etwas geringer als im Vorjahr", sagt Dirk Dingfelder, Vorsitzender des ZVEI-Fachverbands Sicherheit. „Das lässt sich auf die noch immer stockende Baukonjunktur zurückführen. Hier ist erst allmählich Erholung in Sicht", erklärt Axel Schmidt, Vorstandsvorsitzender des BHE Bundesverband Sicherheitstechnik e. V., die aktuelle Situation.

Die Zeichen für den Bau hellen sich aktuell etwas auf: „Die Baugenehmigungen im Neubau sind zuletzt um vier Prozent angestiegen, allerdings von einem sehr niedrigen Niveau ausgehend", so Schmidt. Im Zweckbau und im öffentlichen Sektor laufe die Erholung erst langsam an. „Gegenwärtig profitiert die Branche von Sanierungen und Baumaßnahmen im Bestand", ergänzt Dingfelder. „Insofern begrüßen wir das Sondervermögen für Infrastruktur. Allerdings brauchen wir mehr Tempo. Regulatorische Hürden müssen abgebaut werden, damit schnell und effizient gehandelt werden kann."



Vernetzung und Digitalisierung spielen eine maßgebliche Rolle in der sicherheitstechnischen Industrie. Die Branche gestaltet diese unter anderem in Normen. Hier werden zum Beispiel entsprechende Regelungen für Dienstleistungen aus der Ferne – sogenannte „remote services" – verankert.

Eine besondere Herausforderung für die Entwicklung der Branche bleibt der Rechtsrahmen. „Die europäische Bauprodukte-Verordnung stellt uns in der Normung vor neue Prozesse mit neuen Kriterien. Der digitale Produktpass wird kommen; das Thema Nachhaltigkeit wird implementiert werden", so Dingfelder. Schmidt ergänzt: „Die Digitalisierung kann neben neuen Services und Lösungen auch dazu beitragen, die Lücken durch den bestehenden Fachkräftemangel etwas auszugleichen. Schließen kann sie sie nicht. Er wird eine offene Flanke der Branche bleiben."

Unterschiede beim Wachstum zwischen den einzelnen Gewerken

Der Umsatz mit Brandmeldetechnik – dem mit Abstand größten Gewerk der Sicherheitstechnik, das zudem stark von der Baukonjunktur abhängig ist – wuchs 2024 um 3,4 Prozent auf 2,6 Mrd. Euro. Die Sprachalarmanlagen steigerten ihren Umsatz um 3,8 Prozent auf 138 Mio. Euro.

Die Videosysteme verzeichneten einen Anstieg von 3,8 Prozent auf 820 Mio. Euro. Die vielfältigen Einsatzmöglichkeiten und die Flexibilität der Videosicherheitstechniken in Kombination mit anderen Technologien sorgen für ein stetiges Wachstum.

Bemerkenswert ist der positive Trend im Bereich der Zutrittssteuerungssysteme, die mit einem Plus von 5,2 Prozent auf 510 Mio. Euro ein überdurchschnittliches Wachstum aufwiesen.

Etwas verhaltener zeigte sich hingegen die Entwicklung bei Überfall- und Einbruchmeldeanlagen: Zwar konnte der Umsatz 2024 auf 920 Mio. Euro gesteigert werden, was einem moderaten Plus von 2,2 Prozent entspricht; doch bleibt das Ergebnis erneut unter dem Marktdurchschnitt.

Rauch- und Wärmeabzugsanlagen inklusive der natürlichen Lüftung (RWA/NL) stagnierten bei 177 Mio. Euro. Hingegen haben die sonstigen Technologien wie Rufanlagen nach DIN VDE 0834, Fluchttürsysteme, Personenhilferuf sowie weitere Systeme und Komponenten mit einem Plus von 4,3 Prozent deutlich zugelegt.

Anzeigen

Who is Who der Sicherheitstechnik

– nach Postleitzahlen geordnet –

Bild: # 215383852 / istockphoto.com

DIAS GmbH - Deutsches Institut für Ausbildung und Sicherheit

Fraunhoferstr. 8
04178 Leipzig
www.dias-bildung.de

Security Robotics Development & Solutions GmbH

Mühlweg 44
04319 Leipzig
www.security-robotics.de

LeCA Jobtraining UG (haftungsbeschränkt)

Am Borsigturm 13
13507 Berlin
www.security-personal.de

Klüh Security GmbH

Am Wehrhahn 70
40211 Düsseldorf
www.klueh.de

Anzeigen

KÖTTER Sicherheitssysteme SE & Co. KG

Wilhelm-Beckmann-Straße 7
45307 Essen
koetter.de

Westdeutscher Wachdienst GmbH & Co. KG

Neckarstr. 22 - 24
45478 Mülheim an der Ruhr
www.vollmergruppe.de

Westfälischer Wachschutz GmbH & Co. KG

Herzogswall 30
45657 Recklinghausen
www.wws-security.de

W.I.S. Technik GmbH & Co. KG

Robert- Bosch-Straße 43
50769 Köln
www.wis-sicherheit.de

LivEye GmbH

Europa Allee 56b
54343 Föhren
www.liveye.com

NSTR by LivEye

Europa Allee 56b
54343 Föhren
www.nstr.security

Convergint Technologies GmbH

Im Breitspiel 21
69126 Heidelberg
www.convergint.com

Securiton Deutschland Alarm- und Sicherheitssysteme

Von-Drais-Str. 33
77855 Achern
www.securiton.de

Nürnberger Wach- und Schließgesellschaft mbH

Fraunhoferstr. 10
90409 Nürnberg
www.nwsgmbh.de

Anzeigen

DIAS GmbH – Ihr Sprungbrett in die Sicherheitsbranche

Seit über zehn Jahren sorgt das Deutsche Institut für Ausbildung und Sicherheit (DIAS) für bestens qualifiziertes Personal in der Sicherheitswirtschaft. Mehr als 4.000 ausgebildete Kräfte, 1,4 Millionen Ausbildungsstunden pro Jahr und Standorte in ganz Deutschland sprechen für sich.

Unsere praxisnahen Schulungen sind topaktuell und richten sich nach den Anforderungen des Marktes. Ob Sachkunde § 34a GewO, TQ1, Ersthelfer, Brandschutzhelfer, Interventionskraft, Waffensachkunde, Personenkontrolle, Drohnenführung, technische Kontrollen oder die Ausbildung von Servicekräften und Fachkräften für Schutz und Sicherheit – wir bieten das volle Programm.

Unser Portfolio an Firmenschulungen wird stetig erweitert, damit Unternehmen genau die Qualifikationen erhalten, die sie für ihr Team brauchen.

Erfahrene Ausbilder, hohe Erfolgsquoten und beste Jobchancen machen DIAS zu Ihrem idealen Partner für den Karrierestart oder die Aus- und Weiterbildung Ihrer Mitarbeiter.

In Leipzig, Hannover, Magdeburg und weiteren Städten – oder direkt bei Ihnen vor Ort – bringen wir Sie auf Erfolgskurs. Sicherheit ist nicht nur unser Job. Es ist unsere Mission. Starten Sie jetzt – mit DIAS auf die sichere Seite!

Kontakt:
Viktor Mertjan
DIAS GmbH - Deutsches Institut
für Ausbildung und Sicherheit
Fraunhoferstr. 8 · 04178 Leipzig
Tel.: +49 341 49 27 72 30
Mail: **info@dias-bildung.de**
Web: **www.dias-bildung.de**

Moderne Sicherheitstechnik durch autonome Systeme

Sicherheitstechnologien entwickeln sich schnell. Klassische Maßnahmen wie Kameras oder Barrieren reichen oft nicht mehr aus. Durch die Digitalisierung und den Mangel an Fachkräften setzen Unternehmen immer öfter auf autonome Systeme: Sicherheitsroboter, Drohnen und smarte Plattformen.

Diese Technologien übernehmen monotone, gefährliche oder schwer zugängliche Aufgaben – zuverlässig, präzise und rund um die Uhr. Systeme wie „Spot“ (ein vierbeiniger Laufroboter) oder „Argus“ (ein radgetriebener Patrouillenroboter) sind bereits im Einsatz und zeigen, wie Robotik klassische Sicherheitsdienste ergänzt.

Sie werden über unsere ACUDA-Plattform gesteuert, die zentrale Koordination, Datenanalyse und Integration ermöglicht. Dabei haben wir zentrale Anforderungen berücksichtigt und konsequent umgesetzt: die Einhaltung aktueller regulatorischer Vorgaben trotz wachsender Anforderungen an autonome mobile Sicherheitssysteme, ein ganzheitliches Angebot aus Technologie, Wartung, Installation, Support und Beratung – sowie nachhaltige Konzepte durch systemübergreifenden und aufgabenübergreifenden Einsatz unserer Robotiklösungen.

Robotik entlastet das Personal, steigert die Effizienz und bietet Lösungen für komplexe Sicherheitsanforderungen. Dabei gilt: Mensch und Maschine arbeiten nicht gegeneinander, sondern Hand in Hand – der Mensch trifft die Entscheidungen, der Roboter liefert die Daten.

Kontakt:
Security Robotics Development & Solutions GmbH
Mühlweg 44 · 04319 Leipzig
Tel.: +49 341 2569 3369
Mail: **info@security-robotics.de**
Web: **www.security-robotics.de**

Anzeigen

Personalentwicklung und -vermittlung sind unsere Stärken

Wir bieten Weiterbildungen mit Karrierechancen z. B. in den Bereichen:

- Sicherheit (z. B. Sachkundeprüfung gem. § 34a GewO)
- IHK-geprüfte Schutz- und Sicherheitskraft
- Waffensachkunde
- Intervention/Alarmverfolgung gem. VdS
- Umgang mit Drohnen

Sie wollen Spaß beim Lernen und eine erfolgreiche Weiterbildung?
Dank der Kombination aus Präsenzunterricht und dem Einsatz unserer Lern-App und einer VR-Brille ist das bei uns möglich. Weiterbildungen in Teil- und Vollzeit oder berufsbegleitend, eine bis zu hundertprozentige Förderung durch die Agentur für Arbeit auch für Beschäftigte möglich, Jobcenter, Rentenversicherung oder Berufsgenossenschaften, BFD.

Kontakt:
LeCA Jobtraining UG (haftungsbeschränkt)
Am Borsigturm 13 · 13507 Berlin
Tel.: +49 30 459764-46
Mail: **info@leca.biz**
Web: **www.security-personal.de**

Klüh Security gibt Sicherheit. Mit zukunftsfähigen Lösungen.

Mit 75 Jahren Unternehmensgeschichte verbindet Klüh Security gewachsene Erfahrung mit zukunftsgerichteter Innovationskraft – und entwickelt sein Portfolio kontinuierlich entlang neuer Anforderungen weiter. Jüngster Meilenstein ist die Inbetriebnahme einer eigenen Alarmempfangsstelle und Notruf- und Serviceleitstelle, die als digitale Steuerzentrale klassische Sicherheitsdienste mit innovativer Technologie verknüpft.

Die hochvernetzte offene Plattform WinGuard der Firma Advancis, die in Zusammenarbeit mit dem Technologiepartner TAS durch Klüh Security als zertifizierter Control Room Partner betrieben wird, ermöglicht eine Koordination verschiedenster Systeme rund um die Uhr – von Gefahrenmeldesystemen, Gebäudeleittechnik und Kommunikationstechnik bis zur effizienten Steuerung und Kontrolle von kritischen Prozessen. Innovative und KRITIS-fähige Technologien wie KI-gestützte Alarmfilterung, IoT-Anbindung und Drohnentechnik sorgen für höchste Effizienz und Reaktionsschnelligkeit.

Gestützt wird das digitale Leistungsportfolio bundesweit durch rund 3.600 qualifizierte Mitarbeitende an 23 Standorten – für Kundennähe und passgenaue Lösungen in Bundeswehr, Energie, Industrie, Banken, Gesundheitswesen und Verkehrsinfrastruktur.

Aus- und Weiterbildung erfolgen über die eigene Sicherheitsschule, die TÜV-zertifizierte Klüh Akademie und prämierte E-Learning-Tools. So entsteht integrierte Sicherheit mit Zukunft.

Kontakt:
Sven Horstmann
Klüh Security GmbH
Am Wehrhahn 70 · 40211 Düsseldorf
Tel.: +49 211 9068-533
Mail: **s.horstmann@klueh.de**
Web: **www.klueh.de**

Anzeigen

KÖTTER Security

Technisches Sicherheits- und Gebäudemanagement – ganzheitlich & zukunftssicher

Die Bedrohung durch hybride Risiken wächst rasant: In Deutschland haben sich die Gesamtschäden der Wirtschaftskriminalität binnen zehn Jahren auf etwa 267 Milliarden Euro verfünffacht. In dieser Gefahrenlage sind ganzheitliche Schutz- und Managementkonzepte essenziell – ein wesentlicher Bestandteil sind dabei verschiedenste Systeme aus dem Bereich der Sicherheitstechnik.

KÖTTER Sicherheitssysteme kombiniert modernste Schutztechnologien (Einbruch- und Brandmeldesysteme, Videoüberwachung, Zutrittskontrolle, Perimetersicherung) mit umfassenden Technical Facility Services: von Not- und Sicherheitsbeleuchtung über Feuerlösch- und Entrauchungsanlagen bis hin zu Tür-, Tor- und Raumtrennsystemen. Gleichzeitig wird sichergestellt, dass sicherheitstechnische und prüfpflichtige technische Anlagen nicht nur installiert, sondern auch regelmäßig gewartet und betriebssicher gehalten werden. So lassen sich Gefahren und Risiken für Menschen, Gebäude und Daten minimieren.

Als herstellerunabhängiger Anbieter entwickelt KÖTTER maßgeschneiderte Konzepte – mit Fokus auf Effizienz, Flexibilität und Schutz von Investitionen. Die Anbindung an die nach EN 50518 und VdS 3138 zertifizierte Notruf- und Serviceleitstelle (NSL) ermöglicht rund um die Uhr Alarm-Vorprüfung, z. B. per Video-Live-Schaltung durch geschulte Fachkräfte. Mit dem Betreibermodell KÖTTER SYMTO übernimmt das Familienunternehmen zudem Planung, Investition, Betrieb und Wartung – damit entsteht eine Rundum-Lösung aus einer Hand.

Kontakt:
KÖTTER Sicherheitssysteme SE & Co. KG
Wilhelm-Beckmann-Straße 7 · 45307 Essen
Tel.: +49 201 2788-388
Mail: **info@koetter.de**
Web: **koetter.de**

vollmergruppe dienstleistung

Mit Videoüberwachung erfolgreich Schäden minimieren

Die selbst konzipierten mobilen Videoüberwachungseinrichtungen der Vollmergruppe erhalten von allen Auftraggebern ausschließlich positives Feedback. Die Einbruch- und Vandalismusschäden an den jeweiligen Einsatzorten der VollmerView© Videotürme und fastsolution-Videoboxen haben massiv abgenommen, da potenzielle Täter schon frühzeitig detektiert und über die installierten Lautsprecher gezielt angesprochen werden. In einigen Fällen konnten die potenziellen Täter auf frischer Tat gefasst werden.

Die Einsatzorte sind vielfältig in ihren Anforderungen. Die Videoüberwachungseinheiten bieten vier unterschiedliche Detektionsbereiche (Sensorik), werden nicht nur auf Baustellen, sondern beispielsweise auch an Schulen, Bahnhöfen, Lebensmittelbetrieben, Tankanlagen, Leerstandimmobilien, Großhandel- und Logistikunternehmen, etc. eingesetzt. Jeder Videoturm ist quasi eine mobile Gefahrenmeldeanlage und verfügt über eine Dome- und drei Thermalkameras (mit Wärmesensoren), die an einem bis zu 6 Meter hohen ausfahrbaren Mast befestigt sind. Zusätzlich können an die installierte Gefahrenmeldeanlage weitere Alarmsensoren angeschlossen werden.

Die intelligente Videosoftware detektiert dabei, nahezu fehlalarmfrei, mögliche Schadensereignisse (Einbruch, Vandalismus, Feuer etc.) und überträgt diese zur 24/7-besetzten VdS-zertifizierten Notruf- und Service-Leitstelle (NSL) der Vollmergruppe.

Mittels der integrierten Gefahrenmeldeanlage können auch Objekteinrichtungen außerhalb des Kameraüberwachungsbereichs (z. B. Baucontainer, Büro- und Lagerflächen etc.) in das jeweilige Schutzkonzept eingebunden werden.

Kontakt:
Andreas Brink, Geschäftsführer
Westdeutscher Wachdienst GmbH & Co. KG
Neckarstr. 22–24 · 45478 Mülheim an der Ruhr
Tel.: +49 208 588577
Mail: **info@vollmergruppe.de**
Web: **www.vollmergruppe.de**

Anzeigen

Modernste Sicherheitstechnik mit persönlichem Ansatz

Der **Westfälische Wachschutz (WWS)** bietet mit über 90 Jahren Erfahrung eine lückenlose Symbiose aus moderner Gebäudetechnik und menschlichem Know-how.

Das WWS-Full-Service-Konzept umfasst:

1. **Einbruch-, Brand- und Überfallmeldeanlagen –** zentral gesteuert, optional mit Fernalarm zur eigenen Notruf- und Serviceleitstelle (NSL), die rund um die Uhr besetzt ist.
2. **Videoüberwachung –** stationär oder mobil etwa auf Baustellen – mit intelligenter Videoanalyse und automatischer Alarmweiterleitung an die NSL.
3. **Elektronische Zutrittssysteme –** von Chipkarten über PIN bis hin zu Metalldetektoren oder Röntgenprüfungen, stets begleitet von geschultem WWS-Personal.

Dieses Sicherheitskonzept folgt einem vierstufigen Prozess: Analyse der Schwachstellen, individuelle Beratung, fachgerechte Installation und regelmäßige Wartung – alles optional vervollständigt durch die 24/7-NSL-Anbindung. Besonders überzeugen die mobilen Video-Trailer für temporäre Einsätze sowie die abschreckende Wirkung integrierter Systeme – geeignet für Baustellen, Events oder Gewerbeobjekte. Zutrittskontrollen werden diskret umgesetzt, mit Fokus auf Privatsphäre und rechtssichere Prozesse.

Mit dieser Kombination aus Technik, Effizienz, persönlichem Service und regionaler Präsenz im Ruhrgebiet und Münsterland gelingt dem WWS ein wirkungsvoller Schutz vor Einbruch, Vandalismus, Brand und unbefugtem Zutritt – verlässlich, individuell und direkt mit der eigenen NSL verzahnt.

Kontakt:
Westfälischer Wachschutz GmbH & Co. KG
Herzogswall 30 · 45657 Recklinghausen
Tel.: +49 2361 90422-0
Mail: **info@wws-security.de**
Web: **www.wws-security.de**

W.I.S. Technik – Ihr Partner für neueste, KI-gestützte Sicherheitslösungen

Für uns bei der W.I.S. Technik steht die individuelle Beratung im Mittelpunkt, denn jeder Kunde hat einzigartige Sicherheitsbedürfnisse. Wir entwickeln maßgeschneiderte und zuverlässige Lösungen, wofür andere keine Katalognummern finden.

Unsere Expertise umfasst die gesamte Prozesskette: Von der bedarfsgerechten Planung über die fachgerechte Umsetzung und Wartung bis hin zur kontinuierlichen Optimierung Ihrer Sicherheitsinfrastruktur. Dabei setzen wir auf ein umfangreiches, technisches Portfolio und wählen bei Bedarf die wirtschaftlichste Technologie für Ihre Bedürfnisse. Unsere Ingenieure, Meister und Techniker verfügen über langjährige Erfahrung und handwerkliche Kompetenz, um Ihre Systeme zuverlässig zu bauen und zu pflegen.

Unser Leistungsspektrum umfasst:
– Sicherheitsberatung & Ingenieurleistungen
– Entwicklung maßgeschneiderter Konzepte für Zutrittslösungen, Videotechnik, Einbruchmeldesysteme und Brandmelde- sowie Sprachalarmierungsanlagen
– KI-Innovationen und technische Planungen für kritische Infrastrukturen (KRITIS)
– Skalierbare IT-Services für sichere Netzinfrastrukturen

Verlassen Sie sich auf unsere Kombination aus technischer Kompetenz und handwerklicher Präzision. Vertrauen Sie auf die W.I.S. Technik – für Sicherheit, die wirkt.

Kontakt:
W.I.S. Technik GmbH & Co. KG
Robert-Bosch-Str. 43 · 50769 Köln
Tel.: +49 221 2726 9100
Mail: **wis-service@wis-sicherheit.de**
Web: **www.wis-sicherheit.de**

Anzeigen

LivEye – Smarte Videoüberwachung

Seit 2018 zählt die LivEye GmbH zu den führenden Anbietern mobiler Videosicherheitslösungen in Europa. Mit modernster Kameratechnik, unterstützender KI und 24/7 besetzter Leitstelle mit Sitz in Deutschland schützt das Unternehmen aus Föhren zuverlässig temporäre Risikozonen wie Baustellen, Industrieareale oder Großveranstaltungen.

Die Kamerasysteme erkennen Bewegungen auf bis zu 400 Meter Entfernung. Erspähen die Kameras Verdächtiges, bewertet die KI-gestützte Analysesoftware Bewegungsmuster und filtert irrelevante Ereignisse wie Tiere automatisch heraus. Wird eine Person oder ein Fahrzeug erfasst, erfolgt eine sofortige Alarmmeldung an die Leitstelle. Das geschulte Personal bewertet die Lage und reagiert umgehend nach Kundenwunsch, z.B. mit Live-Lautsprecheransage.

Das Full-Service-Konzept erfüllt unterschiedliche Sicherheitsansprüche vom Gewerbebetrieb bis zum großen Kraftwerk: Vom kompakten LivEye One+ über das energieautarke LivEye ProSolar bis hin zum besonders flexiblen LivEye Falcon – jedes System ist schnell einsetzbar, individuell skalierbar und auf höchste Sicherheitsanforderungen ausgelegt.

Die Option „Smart by Day" ermöglicht es, die Videoüberwachungssysteme tagsüber als virtuelle Baustellenansicht zu verwenden. Qualitätssicherung, Produkt- sowie Designentwicklung und Tests finden vor Ort in Rheinland-Pfalz statt. Kurze Wege, regionale Partner und die ISO-14001-Zertifizierung unterstreichen den Anspruch an Nachhaltigkeit.

Kontakt:
LivEye GmbH
Europa Allee 56b · 54343 Föhren
Tel.: +49 6502 4034722
Mail: **info@liveye.com**
Web: **www.liveye.com**

NSTR.security – Sicherheit neu gedacht

NSTR ist eine KI-gestützte Sicherheitslösung für kritische Infrastrukturen und sensible Gewerbeflächen – 100 % Made in Germany: entwickelt, produziert und betrieben am Standort Deutschland.

Das System kombiniert moderne Kameratechnik mit intelligenter Videoanalyse: Irrelevante Auslöser wie Tiere oder Wettereinflüsse werden automatisch herausgefiltert. Nur echte sicherheitsrelevante Ereignisse werden an die rund um die Uhr besetzte Leitstelle in Deutschland übermittelt – für sofortige Reaktion im Ernstfall.

Besonders: NSTR funktioniert ohne aufwendige Installation oder externes Fachpersonal. Über ein digitales Planungstool erfassen Nutzer ihr Gelände, positionieren Kameras virtuell und bestellen die Systeme direkt online. Nach der Lieferung ist die Inbetriebnahme in wenigen Minuten möglich – lediglich ein Stromanschluss wird benötigt. Die Montage erfolgt eigenständig vor Ort – ganz nach dem Plug-&-Play-Prinzip.

Per App lassen sich Alarmzeiten, Zonen und Systeme intuitiv steuern. Alle Ereignisse werden DSGVO-konform dokumentiert und im digitalen Wachbuch archiviert.

NSTR bringt moderne Sicherheit dorthin, wo sie gebraucht wird – einfach, skalierbar und souverän.

Kontakt:
NSTR by LivEye
Europa Allee 56b · 54343 Föhren
Tel.: +49 6502 4034722
Mail: **info@liveye.com**
Web: **www.nstr.security**

Anzeigen

convergint

Convergint: Ihr Partner für Sicherheit, der weiterdenkt

Convergint ist der weltweit führende Systemintegrator für Sicherheitstechnik und Building Technology Solutions mit dem Anspruch, für unsere Kunden mehr zu leisten als Standard. Seit über 20 Jahren entwickeln wir maßgeschneiderte Sicherheitslösungen, die modernste Technologie, langjährige Erfahrung und persönliche Betreuung verbinden.

Unser Portfolio umfasst elektronische Sicherheitssysteme, Videoüberwachung, Zutrittskontrolle, Brandmeldetechnik, Perimeterschutz sowie integrierte Leitstellenlösungen. Dabei arbeiten wir herstellerunabhängig und stets mit Blick auf die individuellen Anforderungen jedes Projekts – ob Industrie, Behörden, Kritische Infrastrukturen oder Handel.

Mit mehr als 11.000 Kolleginnen und Kollegen weltweit und einem starken Netzwerk in Deutschland stehen wir für Verlässlichkeit, kurze Reaktionszeiten und höchste Qualitätsstandards. Unsere Kundennähe zeigt sich nicht nur in der technischen Umsetzung, sondern auch in unserer Kultur: Wir handeln nach klaren Werten, setzen auf langfristige Partnerschaften und übernehmen Verantwortung; für Sicherheit, Nachhaltigkeit und den Erfolg unserer Kunden.

Convergint: lokal verbunden, global vernetzt, kompromisslos engagiert für Ihre Sicherheit.

Kontakt:
Convergint Technologies GmbH
Im Breitspiel 21 · 69126 Heidelberg
Tel.: +49 6181 427 550
Web: **www.convergint.com**

SECURITON

Der findigste Anwendungsspezialist für Sicherheit

Securiton Deutschland ist Ihr Partner rund um den Einsatz intelligenter Alarm- und Sicherheitssysteme. Seit mehr als 45 Jahren bieten wir für jedes Anwendungsumfeld individuelle Lösungen für den umfassenden Brand-, Objekt- und Perimeterschutz.

Im Bereich Safety sind wir mit unseren Brandmeldesystemen und unseren Sonderbrandmeldetechniken der Sicherheitspionier für Brandfrüherkennung. Elektroakustische Systeme tragen im Ernstfall maßgeblich zu einer sicheren Sprachalarmierung und Notfallwarnung bei.

Im Bereich Security sichern wir nicht nur den Boden, sondern auch den Luftraum. Unser Konzept heißt „Dome Security", weil wir eine Art Schutzschirm über die Areale und Gebäude unserer Kunden legen. Die Hauptbestandteile bilden Videosicherheitssysteme mit intelligenter Videoanalyse und marktführende Systemlösungen zur Drohnendetektion und -abwehr. Aber auch ein hochintegrales Sicherheitsmanagement, Zaundetektions- und Zutrittskontrollsysteme, Einbruch- und Gefahrenmeldeeinrichtungen sowie Robotiksicherheitssysteme kommen für einen kompletten Rundumschutz zum Einsatz.

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 ganz 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

Sicherheit neu gedacht – von Tradition zu Hightech

Die Nürnberger Wach- und Schließgesellschaft hat sich in 123 Jahren vom klassischen Bewacher zum technologisch ausgerichteten Kompetenzzentrum für Sicherheitslösungen entwickelt. Wir sind überzeugt, dass die gezielte Kombination von qualifiziertem Personal und modernster Sicherheitstechnologie den höchsten Schutzgrad gewährleistet. Neben personellen Sicherheitsdienstleistungen und Alarmservices der nach DIN EN 50518 zertifizierten Alarmempfangsstelle bieten wir im NWS-Verbund die Errichtung moderner Sicherheitstechnik an. Das Portfolio reicht von der Planung und Installation komplexer Gefahrenmeldesysteme über Videoüberwachungslösungen mit intelligenter Analytik bis hin zu Zutrittskontrollsystemen.

Im Bereich Robotik bieten wir Sicherheitsroboter, die in der DACH-Region entwickelt werden. Sie patrouillieren autonom, überwachen großflächige Areale, erkennen Abweichungen in Echtzeit und übermitteln Daten unmittelbar an die Leitstelle. Unsere eigene, digitale Pförtnerlösung wickelt Prozesse wie Identitätsprüfung, Ausweiserstellung und Dokumentation digital und mobil ab. Das spart nicht nur Kosten, sondern schafft operative Flexibilität – ein Vorteil, den Industrieunternehmen ebenso schätzen wie öffentliche Institutionen. Mit dieser Kombination aus bewährter Sicherheitstechnik, zuverlässigen Alarmservices und innovativer Robotik schaffen wir zukunftssichere, skalierbare Sicherheitslösungen, die Prävention, Effizienz und Schutzqualität messbar steigern.

Kontakt:
Nürnberger Wach- und
Schließgesellschaft mbH
Fraunhoferstr. 10 · 90409 Nürnberg
Tel.: +49 911 51996-0
Mail: **vertrieb@nwsgmbh.de**
Web: **www.nwsgmbh.de**

Abwehrreihen gegen Cybercrime gemeinsam weiter stärken

BDSW-Fachausschuss Cybersicherheit: Aufgaben, Herausforderungen und Ziele

Von Dirk H. Bürhaus

Dirk H. Bürhaus

ist seit vielen Jahren Geschäftsführender Direktor in der KÖTTER Security Gruppe und zudem Geschäftsführer des Cybersecurity-Spezialisten G.I.P., an dem das Familienunternehmen eine Mehrheitsbeteiligung hält. Darüber hinaus ist er u. a. im Vorstand des Bundesverbandes der Sicherheitswirtschaft engagiert, langjähriges Mitglied der ASIS International (der weltweit größten Organisation für Fragen der Sicherheit in der privaten Wirtschaft) und wirkt in verschiedenen Arbeitskreisen im europäischen Dachverband des Bewachungsgewerbes CoESS mit.

Kontakt:
dirk.buerhaus@koetter.de

Cybersecurity zählt längst zu den Topthemen in Sachen Sicherheit, und die Wichtigkeit dieses Themas wird in Zukunft weiter wachsen. So verzeichnete nach Angaben des größten europäischen Thinktank zu Digitalthemen BITKOM die Mehrheit der deutschen Unternehmen, beachtliche 80 Prozent, zuletzt eine erhebliche Zunahme von Cyberattacken – und für die kommenden Monate erwarten sogar neun von zehn Unternehmen einen zusätzlichen Anstieg. Der wirtschaftliche Schaden allein durch Cybercrime summiert sich auf fast 180 Milliarden Euro, ein Plus von über 20 Prozent binnen eines Jahres.

Bereits diese Zahlen unterstreichen: Für alle Unternehmen und nicht nur für Betreiber Kritischer Infrastrukturen (KRITIS) stellt sich längst nicht mehr die Frage, ob, sondern vielmehr wann sie Ziel einer solchen Attacke werden. Und richten den kritischen Blick auf die eigene Abwehr- und Reaktionsfähigkeit. Denn auch um diese ist es nach Aussage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Deutschland nicht immer gut bestellt: immerhin verstreichen im Schnitt bis zu 353 Tage, bevor ein destruktiver Cyberangriff im Unternehmen erkannt und vor allem eingedämmt wird!

360-Grad-Sicherheit ist Trumpf

Für private Sicherheitsdienstleister, ohne die Wirtschafts- und KRITIS-Schutz undenkbar ist, ergeben sich daraus zunächst einmal große Chancen! Sie können durch eine umfassende Risikoanalyse und kundenindividuelle Sicherheitskonzepte, die alle Bausteine der Unternehmenssicherheit inklusive der Cybersecurity berücksichtigen, die eigene Leistungsstärke unter Beweis stellen. Konkret bedeutet dies, den Kunden beim Thema Cybersecurity aufzuzeigen, dass die Robustheit ihrer IT-Sicherheitsarchitektur nicht allein an Investitionen in Firewalls, Virenscanner etc. hängt. Zum Ersten erfordert umfassender Schutz weitere Verteidigungslinien, die von Netzwerksicherheit über die 24/7-Überwachung der IT-Infrastruktur des Auftraggebers bis zu Awareness-Schulungen reichen. Zum Zweiten drohen Firewalls etc. spätestens dann ad absurdum geführt zu werden, wenn beim Zugang zu Gebäuden und sensiblen Sektoren wie Rechenzentren etc. durch mangelnde personelle bzw. technische Sicherheitsmaßnahmen „Haus der offenen Tür" herrscht bzw. es Kriminellen mit Social Engineering gelingt, etwa für ein Eindringen in die Unternehmen hilfreiche Daten abzuschöpfen.

Wachsende Anforderungen, auch an Dienstleister

Die zentrale Stellung für Wirtschaft und KRITIS-Betreiber beim Areal- und Gebäudeschutz, der Informationssicherheit etc. forciert in Kombination mit den wachsenden Risiken aus dem Netz somit gleichzeitig ebenfalls die Anforderungen an alle Sicherheitsdienstleister speziell in Sachen Cybersecurity. Eine Aufgabe, der sich der Bundesverband der Sicherheitswirtschaft (BDSW) mit der Gründung und im vergangenen April erfolgten Konstituierung des neuen Arbeitskreises Cybersecurity noch gezielter widmen will. Im Rahmen der Arbeit soll zunächst ein Angebot für Mitglieder geschaffen werden, um sich besser gegen Angriffe aus dem Netz zu schützen. Auf lange Sicht soll neben dieser Stärkung des Eigenschutzes der Unternehmen auch über das Thema Cybersicherheit im Rahmen des Produktportfolios von Sicherheitsunternehmen gesprochen werden.

Verband wappnet sich für die neue Welt

Der BDSW stellt sich auf diese Weise nachhaltig und konsequent auf die Gegebenheiten und Anforderungen einer sich rasant verän-

dernden neuen Welt ein. Denn gerade auch für Sicherheitsunternehmen sind Bedrohungen im Bereich der Cybersicherheit ein Thema. Unsere Mitglieder sind sogar aufgrund ihrer Tätigkeit und der darin ausgeübten Funktionen im besonderen Maße ihren Kunden gegenüber verantwortlich, entsprechende Schutzmaßnahmen zu treffen.

Gerade deshalb erfüllt es mich mit besonderem Stolz, den neuen Arbeitskreis als Vorsitzender zu führen und meine Kompetenzen speziell auf dem Sektor der Cybersicherheit einbringen zu dürfen. Ich bedanke mich für das damit verbundene Vertrauen und freue mich auf die Zusammenarbeit mit allen Beteiligten.

Awareness und Faktor Mensch im Fokus

Die Ziele des Arbeitskreises sind prioritär, die Awareness zum Thema Cybersicherheit bei den Mitgliedsunternehmen zu steigern, praktische Umsetzungshilfen und beispielhafte Empfehlungen bereitzustellen sowie ein ganzheitliches Schulungskonzept für alle Bereiche der Unternehmen zu entwickeln – inklusive der gewerblichen Kräfte beim Kunden vor Ort.

Denn: Der Faktor Mensch spielt mit Blick auf die Vulnerabilität von Unternehmen eine ganz zentrale Rolle. Das gilt für Beschäftigte unserer Auftraggeber in gleichem Maße wie für die Mitarbeiterinnen und Mitarbeiter in unserer eigenen Branche. Deshalb wollen und müssen wir gerade als BDSW-Mitgliedsunternehmen Vorreiter sein, wenn es z.B. um umfassende und – angesichts der stetig zunehmenden Sicherheitsrisiken – kontinuierlich zu erweiternde Kompetenzen unserer eigenen Teams bei der erfolgreichen Abwehr von Phishing-Versuchen, Social Engineering und vielem mehr geht.

Hier wird der Arbeitskreis den BDSW-Mitgliedsunternehmen vielfältige Informationen und Hilfen bieten sowie stetiger Ansprechpartner sein. Themen werden langfristig sein:

– News, Schulungsunterlagen oder Veranstaltungen über aktuelle Bedrohungen wie Phishing, Malware oder Social Engineering, die anschließend in den einzelnen BDSW-Mitgliedsunternehmen weitergegeben werden können und sollen, um so speziell das Sicherheitsbewusstsein und Handeln der gewerblichen Beschäftigten zu stärken.
– Formulierung und Verbreitung klarer und fortlaufend aktualisierter Verhaltenstipps seitens des BDSW-Fachausschusses an die Mitgliedsunternehmen, wie u. a. die Zugangsberechtigungen und -verfahren ihrer eigenen Mitarbeiter und Systeme noch sicherer zu managen, verdächtige E-Mails oder andere Angriffsmethoden krimineller Angreifer zu erkennen oder sichere Datenübertragungen und Plattformbetriebe zu gestalten sind.

Nutzen Sie bitte aktiv diese Angebote! Denn jedes Sicherheitsunternehmen – ganz gleich, ob bundesweiter Player oder regionaler Anbieter – muss sich seiner ganz persönlichen Verantwortung bei der Abwehr von Cyberkriminellen bewusst sein.

STATE OF SECURITY

Sicherheitskonferenz rückte Cyberschutz in den Fokus

Cybersecurity stand auch im Fokus der von KÖTTER Security und German Business Protection (GBP) veranstalteten STATE OF SECURITY, die unter dem Titel „Digitale und physische Sicherheit im Zusammenspiel: Unternehmensschutz ganzheitlich betrachtet" Anfang Juni in Berlin stattgefunden hat. Zu den Referenten gehörten u. a. Markus Horschig (Hamburg Port Authority/Betreiber des Hamburger Hafens), Patrick Theuer (Deutsche Bahn AG), Verwaltungsrat Friedrich P. Kötter und Prof. Dr. Harald Olschok, Mitglied des KÖTTER Sicherheitsbeirates. Insgesamt waren mehr als 150 Teilnehmer bei der renommierten Sicherheitskonferenz dabei.

Der Hacker im Hoodie ist passé

Wie wehrt man sich gegen hochprofessionelle Cyberkriminelle?

Im Gespräch mit Fred-Mario Silberbach

Fred-Mario Silberbach

Leitender Kriminaldirektor beim Bundeskriminalamt (BKA)

Die Erstveröffentlichung des Interviews erfolgte in der Ausgabe 7-8/2025 der Zeitschrift GIT SICHERHEIT.

https://git-sicherheit.de/de/

Wir bedanken uns für die Abdruckgenehmigung.

Unternehmen aller Branchen sehen sich heute mit einer kriminellen Industrie konfrontiert, die hochvernetzt, arbeitsteilig und international operiert. Gleichzeitig bleibt ein Großteil der Angriffe im Verborgenen, da viele Vorfälle nicht gemeldet werden. Dabei hätte dies erhebliche Vorteile – und die Furcht vor Nachteilen ist in aller Regel unbegründet. GIT SICHERHEIT sprach darüber mit Fred-Mario Silberbach, leitender Kriminaldirektor beim Bundeskriminalamt (BKA).

Herr Silberbach, Sie haben kürzlich einen ziemlich beeindruckenden Vortrag beim BSKI, dem Bundesverband für den Schutz Kritischer Infrastrukturen, gehalten. Ich habe mitgenommen, dass die Bekämpfung der Cyberkriminalität zwar ständige und erhebliche Anstrengung erfordert – diese aber letztlich durchaus erfolgreich ist. Bevor wir tiefer einsteigen – wie besorgt bzw. wie zuversichtlich sind Sie, was das Thema betrifft?

Fred-Mario Silberbach: Die Lage ist ernst, aber nicht aussichtslos. Richtig ist, dass Cybersicherheit eine wichtige Gemeinschaftsaufgabe ist, zu der wir alle in unserem eigenen Interesse dauerhaft beitragen sollten. Dazu gehört für mich auch, dass wir die Wehrhaftigkeit unseres Rechtsstaates und unserer Gesellschaft angesichts der steigenden Bedrohungen weiter stärken müssen und uns nicht auf Erfolgen ausruhen dürfen.

Schauen wir mal auf die Zahlen: Die Charts sehen ja auf den ersten Blick aus, wie man es sich eher bei Börsenkursen wünscht – nur dass wir 2024 eben von einem Gesamtschaden von 266,6 Milliarden Euro sprechen. Wie setzen sich die Schäden im Wesentlichen zusammen?

Fred-Mario Silberbach: Diese Zahl ist das Ergebnis einer jährlich durchgeführten Studie des Digitalverbands Bitkom – und stellt einen neuen Rekordwert dar. Die zugrunde liegende Erhebung ist ein guter Indikator für die aktuelle Gefährdungslage. Für uns besonders relevant sind die Schäden durch Cyberattacken, die im vergangenen Jahr auf 178,6 Milliarden Euro angestiegen sind. Das entspricht einem Plus von 30,4 Milliarden Euro im Vergleich zu 2023 und zeigt: Cybercrime ist und bleibt eine große Bedrohung. Auch durch die zunehmende Professionalisierung der cyberkriminellen Akteure, die zur Entwicklung einer regelrechten kriminellen Industrie geführt hat.

Wirtschaftsunternehmen werden heute offenbar erheblich stärker attackiert als noch 2017. Und das zeigt der Vergleich der Zahlen zwischen „betroffen" und „vermutlich betroffen", wenn ich das richtig verstehe. Wie steht es um die Anzeigequote?

Fred-Mario Silberbach: Die Anzeigenquote ist leider sehr gering. Verschiedene Studien kommen zu dem Ergebnis, dass etwa neun von zehn Cyberdelikten nicht angezeigt werden. Wir müssen also von einem großen Dunkelfeld von rund 90 Prozent ausgehen. So vielschichtig die Ursachen dafür sein mögen – wichtig ist vor allem, dass Cyberangriffe stets auch der Polizei angezeigt werden. Das geschieht leider nicht automatisch und wir können nur Straftaten verfolgen, die uns auch bekannt geworden sind. Damit die Polizeibehörden für Unternehmen und Organisationen in Fällen von Cybercrime auch besser und schneller erreicht werden können, haben alle Landeskriminalämter und auch wir im BKA je eine Zentrale Ansprechstelle Cybercrime eingerichtet. Die Kontaktdaten und weitere Informationen zu den Aufgaben und Angeboten der Zentralen Ansprechstellen Cybercrime finden sich unter **www.polizei.de**.

Die Aufklärungsquote ist gar nicht übel – sie liegt bei Cybercrime immerhin bei fast einem Drittel. Wird das von den Betroffenen nach Ihrer Wahrnehmung unterschätzt? Und was setzen Sie dem entgegen?

Fred-Mario Silberbach: Unserer Erfahrung nach bestehen bei den Unternehmen oftmals immer noch Vorbehalte, Cybercrime-Delikte zur Anzeige zu bringen. Da spielt zum einen die Angst vor einem Reputationsverlust eine große Rolle, zum anderen jedoch auch die Befürchtung, dass wir dann

die Unternehmens-IT weitgehend beschlagnahmen. Beide Sorgen sind jedoch unbegründet: Zur Anzeige gebrachte Straftaten behandeln wir selbstverständlich vertraulich. Und wir wissen, wie wichtig die Wiederherstellung der Arbeitsfähigkeit für die Unternehmen ist. In der Regel genügt es, uns bestimmte Daten zukommen zu lassen. Hier spielt der Zeitfaktor eine wichtige Rolle – wenn wir schnell hinzugezogen werden und relevante Spuren sichern können, haben wir häufig konkrete Ermittlungsansätze. Wenn wir von einem Fall hingegen gar nichts erfahren, können wir auch keine Ermittlungen beginnen. Zudem zeigt unsere Erfahrung: Unternehmen, die bereits bei laufenden Ransomware-Angriffen die Polizei einschalten, zahlen in der Regel weniger Lösegeld. Darüber hinaus ist die Aufklärungsquote angesichts des großen Dunkelfeldes im Bereich Cybercrime sicher zu relativieren.

Nun liegt die Aufklärungsquote bei der PKS (also einem gewichtigen Teil der der Polizei bekannt gewordenen rechtwidrigen Straftaten bzw. Versuchen) aber deutlich höher, nämlich bei 58 Prozent (2024). Das dürfte hauptsächlich daran liegen, dass die Untergrundwirtschaft der Cyberkriminellen zunehmend professionalisiert und die Angriffe komplexer werden.

Fred-Mario Silberbach: Richtig ist, dass sich die Underground Economy erheblich professionalisiert hat. Das fußt auf mehrere Ebenen und relevanten Entwicklungen: erstens dem allgemeinen Megatrend der Digitalisierung. Zweitens hat die COVID-Pandemie durch die plötzliche Remote-Anbindung zahlreicher Arbeitsplätze für einen rasanten Aufwuchs an Tatgelegenheiten gesorgt und so die Entwicklungen beschleunigt. Drittens haben sich geopolitische Konflikte auf den digitalen Raum ausgeweitet. Viertens profitieren auch Kriminelle von den neuen Möglichkeiten rund um das Thema künstliche Intelligenz. Das macht die Lage und den Ausblick sehr ernst. Wir haben es heute mit einer hochprofessionellen, vernetzten kriminellen Industrie zu tun. Das stereotype Bild eines einzelnen Hackers im Hoodie ist eine romantisierte Darstellung.

Von den bekannten Akteuren haben Sie beispielsweis NoName, Sandworm und Anonymous genannt. Das sind politisch motivierte Hacker?

Fred-Mario Silberbach: Politisch motivierte cyberkrirninelle Akteure verfolgen sehr unterschiedliche Ziele und sind unterschiedlich straff organisiert. Anonymous dürfte von den genannten Gruppierungen wohl die mit dem geringsten Organisationsgrad sein. Auch die bevorzugten Modi Operandi unterscheiden sich. Aber eine politische Motivation hinter den Kampagnen kann wohl als kleinster gemeinsamer Nenner unterstellt werden. Insgesamt beobachten wir eine Zunahme von Cyberangriffen mit politischem Hintergrund, insbesondere seit dem Beginn des russischen Angriffskriegs auf die Ukraine 2022 und dem Überfall der Hamas auf Israel. Die Täterschaft der hacktivistischen Szene lässt sich daher primär in zwei Lager einordnen: pro-russisch oder anti-israelisch.

Davon sind die einfach wirtschaftlich interessierten Hacker – sprich Erpresser – abzugrenzen?

Fred-Mario Silberbach: Die Grenzen zwischen finanziell orientierten und politisch motivierten Akteuren verschwimmen zusehends. Klassischerweise sind Cyberkriminelle finanzi-

ell orientiert, sie setzen beispielsweise Ransomware ein, um Unternehmen bzw. Institutionen zu erpressen und Lösegelder zur eigenen wirtschaftlichen Bereicherung zu erlangen. Da sich die Underground Economy aber sehr spezialisiert hat und cyberkriminelle Dienstleistungen auf Darknet-Marktplätzen zum Verkauf angeboten werden, kann ein Anbieter rein finanziell motiviert sein, während sein Auftraggeber von politischen Motiven geleitet wird.

Zur Vorgehensweise dieser Cyberkriminellen: Es gibt eine richtige konzertierte Arbeitsteilung in verschiedenen Phasen des Angriffs – und das spiegelt sich in komplexen Organigrammen dieser Gruppierungen. Wie gut sind Ihre Einblicke in diese Strukturen?

Fred-Mario Silberbach: Wir beobachten in Teilen ein sehr strukturiertes und professionelles Vorgehen bis hin zu konzernartigen Organigrammen und Zuständigkeiten, das ist richtig. Öffentlich wurde das beispielsweise im Rahmen der sogenannten Conti-Leaks, aber auch abseits davon denkt man in Franchise-Systemen und wirbt um sogenannte Affiliates. Manche Dienstleistungen werden eingekauft, andere inhouse gefertigt – eben ganz wie in der Industrie.

Sie haben in den letzten Jahren sehr beachtliche Ermittlungserfolge gehabt. Sie zitieren sogar aus einem Untergrundforum, aus dem hervorgeht, dass das BKA als erfolgreiche Behörde wahrgenommen wird. Könnten Sie das eine oder andere Beispiel beschreiben, das Sie besonders wichtig finden?

Fred-Mario Silberbach: Zunächst ist eines besonders wichtig: Cybercrime ist eigentlich immer international. In keinem anderen Phänomenbereich werden Staats- und Zuständigkeitsgrenzen schneller überquert. Täter, Opfer und die sie verbindenden Infrastrukturen befinden sich häufig in anderen Ländern oder sind sogar über Kontinente verteilt. Das bedeutet vor allem: Eine gut funktionierende nationale und vor allem internationale Zusammenarbeit sind notwendige Voraussetzungen, um erfolgreich gegen die Cybercrime vorgehen zu können. Hier haben wir in den vergangenen Jahren mit unseren nationalen und internationalen Partnern viel gelernt und sehr viel vorangetrieben.

Das spiegelt sich in der Schlagzahl unserer – eigentlich immer internationalen – Ermittlungserfolge wider.

Hatten wir anfangs etwa einen großen Takedown im Jahr, sind es inzwischen schon zahlreiche. Dabei ist unsere „Operation Endgame“ sicherlich besonders interessant, weil sie auf Dauer angelegt ist und darauf abzielt, die sogenannte Kill Chain frühzeitig zu unterbrechen. Im vergangenen Jahr haben wir erstmals sechs Dropper-Familien gleichzeitig mit unseren polizeilichen Maßnahmen adressiert und die Underground Economy damit um die wichtigsten Türöffner zu den Opfern gebracht. Das hat Wirkung gezeigt – und wir haben mehrmals nachgelegt, zuletzt in diesem Jahr.

Lassen Sie uns – soweit erlaubt – einen tieferen Blick in Ihren strategischen Werkzeugkasten beim BKA werfen. Können Sie einmal überschlägig darstellen, wie Sie beim BKA vorgehen?

Fred-Mario Silberbach: Unsere Strategie ist mehrdimensional. Zum einen verfolgen wir die Straftäter selbst, versuchen also die Akteure persönlich zu identifizieren, zu lokalisieren und zu verhaften. Weil sich jedoch Straftäter auch in Ländern aufhalten, deren Strafverfolgungsbehörden nicht oder nur unzureichend mit uns kooperieren, zielen wir auch darauf ab, die technischen Infrastrukturen zu beschlagnahmen bzw. deren weitere Nutzung zu unterbinden und damit unbrauchbar zu machen. Als Drittes verfolgen wir die kriminell erlangten Finanzmittel – häufig sind das Kryptowährungen –, um den Tätern die Gelder für weitere Taten zu nehmen. Und viertens betreiben wir eine disruptive Kommunikation. Das bedeutet, dass wir der Underground Economy Hinweise geben, dass wir bereits vieles über die verschiedenen Akteure und ihr Umfeld herausgefunden haben. Das ergänzt unsere klassischen Fahndungsmaßnahmen und führt zu Misstrauen in der Szene. Dieses Vorgehen schädigt die oftmals über Jahre mühsam aufgebaute und erfolgskritische Reputation der Cyberkriminellen.

Wie sehen Sie eigentlich den Status quo, was die Vorbereitung und Prävention gegen Cyberkriminalität seitens deutscher Unternehmen betrifft?

Fred-Mario Silberbach: Der Ernst der Lage unterstreicht: Cybersicherheit können wir nur gemeinsam herstellen. Wir beobachten da einige Bewegung, aber gerade bei kleinen und mittleren Unternehmen fehlt noch immer zu häufig die unternehmerische Aufmerksamkeit für die Risiken. Für uns ist klar: Eine Vogel-Strauß-Taktik aufseiten der potenziellen Opfer erhöht das Risiko schwerwiegender Cyberangriffe erheblich. Jedes Unternehmen hat sensible Daten und eine Reputation zu verlieren, daher ist jede Branche und jede Unternehmensgröße gefährdet. Zeitgemäße, professionelle Cybersicherheitsmaßnahmen sind heute unerlässlich.

Wir haben schon darüber gesprochen, dass Sie aus guten Gründen die Zusammenarbeit mit dem BKA bzw. den ZAC, den Zentralen Ansprechstellen Cybercrime, empfehlen. Wie soll sich ein Unternehmen im Falle des Falles idealerweise verhalten?

Fred-Mario Silberbach: Es ist wichtig sich bewusst zu machen, dass wir alle Ziel von Cyberattacken werden können. Idealerweise sichert sich jedes Unternehmen so gut ab, dass kriminelle Akteure keine Sicherheitslücken ausnutzen können. Für den Fall von dennoch erfolgreichen Cyberangriffen sollte das Unternehmen einen Krisen- bzw. Notfallplan haben, den es Schritt für Schritt abarbeitet, an-

statt in Chaos zu verfallen und wichtige Maßnahmen dann zu übersehen. Darin steht dann zum Beispiel auch, dass zügig die Polizei hinzuzuziehen ist und wo die Backups liegen, um die Arbeitsfähigkeit schnellstmöglich wiederherzustellen.

Leider ist es aber nicht immer so einfach: Denn häufig befinden sich die Angreifer lange unbemerkt im System, kundschaften Informationen aus und exfiltrieren sensible Daten – ein Argument mehr für eine ordentliche Absicherung jedes Unternehmens im eigenen Interesse.

Wichtig ist, sich intensiv zu informieren – z. B. über die „Handlungsempfehlungen für die Wirtschaft“ in Fällen von Cybercrime (**www.bka.de/cybercrime**) oder auch über eine Kontaktaufnahme mit der ZAC des jeweiligen Bundeslandes oder auch des BKA, um seine Ansprechpartner bei der jeweiligen ZAC-Dienststelle kennenzulernen. Vor allem rege ich an, sich bereits im Vorfeld möglicher Cyberangriffe mit den Experten der Polizei über die in einem Ernstfall wichtigen und notwendigen Maßnahmen auszutauschen.

Hier finden Betroffene von Cyberangriffen Handlungsanleitungen und Ansprechpartner:

„Handlungsempfehlungen für die Wirtschaft“ in Fällen von Cybercrime

Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen (ZAC)

Jedes Unternehmen sollte prüfen, wo seine Verwundbarkeiten sind

Im Gespräch mit Franz Polenz

Franz Polenz

Leiter Konzernsicherheit bei Siemens Energy
(Bild: Siemens Energy)

Die Erstveröffentlichung des Interviews erfolgte unter

www.prosecurity.de

Wir bedanken uns für die Abdruckgenehmigung.

Besonders Kritische Infrastrukturen stehen zunehmend im Fokus hybrider Angriffe. Unternehmen müssen heute umfassende Sicherheitskonzepte entwickeln, um Wirtschaftsspionage, Cyberangriffe und innere Risiken effektiv abzuwehren. Ein Gespräch mit Franz Polenz, Leiter Konzernsicherheit bei Siemens Energy, über die allgemeine Bedrohung durch Spionage und Sabotage.

Herr Polenz, welchen Raum nehmen die Themen Spionage und Sabotage in Ihrer täglichen Arbeit als Sicherheitsverantwortlicher eines großen Unternehmens ein?

Franz Polenz: Der Schutz gegen Wirtschaftsspionage und Sabotage ist in der Unternehmenssicherheit zwar nur eines von vielen Themen, aber ein sehr relevantes. Die potenziellen Schäden können schon bei einem einzigen kritischen Vorfall verheerend sein. Das Thema hat deutlich an Relevanz gewonnen, was sich auch in unserer Arbeitslast widerspiegelt.

Wie hat sich die Bedrohungslage denn in den letzten Jahren entwickelt, quantitativ wie auch qualitativ?

Franz Polenz: Wie man unter anderem den öffentlich zugänglichen Informationen der deutschen Sicherheitsbehörden entnehmen kann, hat sich die Bedrohungslage insbesondere seit Beginn des Ukraine-Krieges deutlich verschärft. Wir befinden uns in Deutschland im Fokus einer sogenannten hybriden Kriegsführung durch die Russische Föderation. Das ist eine gesamtgesellschaftliche Bedrohung und somit auch eine für Unternehmen. Gerade Unternehmen im Bereich der Kritischen Infrastruktur sehen sich einer erhöhten Gefährdung durch Sabotage und Spionage ausgesetzt. Die Bedrohung ist nicht neu, aber in den letzten zwei, drei Jahren ist ein massiver Anstieg zu verzeichnen.

Und gerade im Bereich der Kritischen Infrastruktur ist ein Angriff auf ein Unternehmen letztlich ein Angriff aufs Land ...

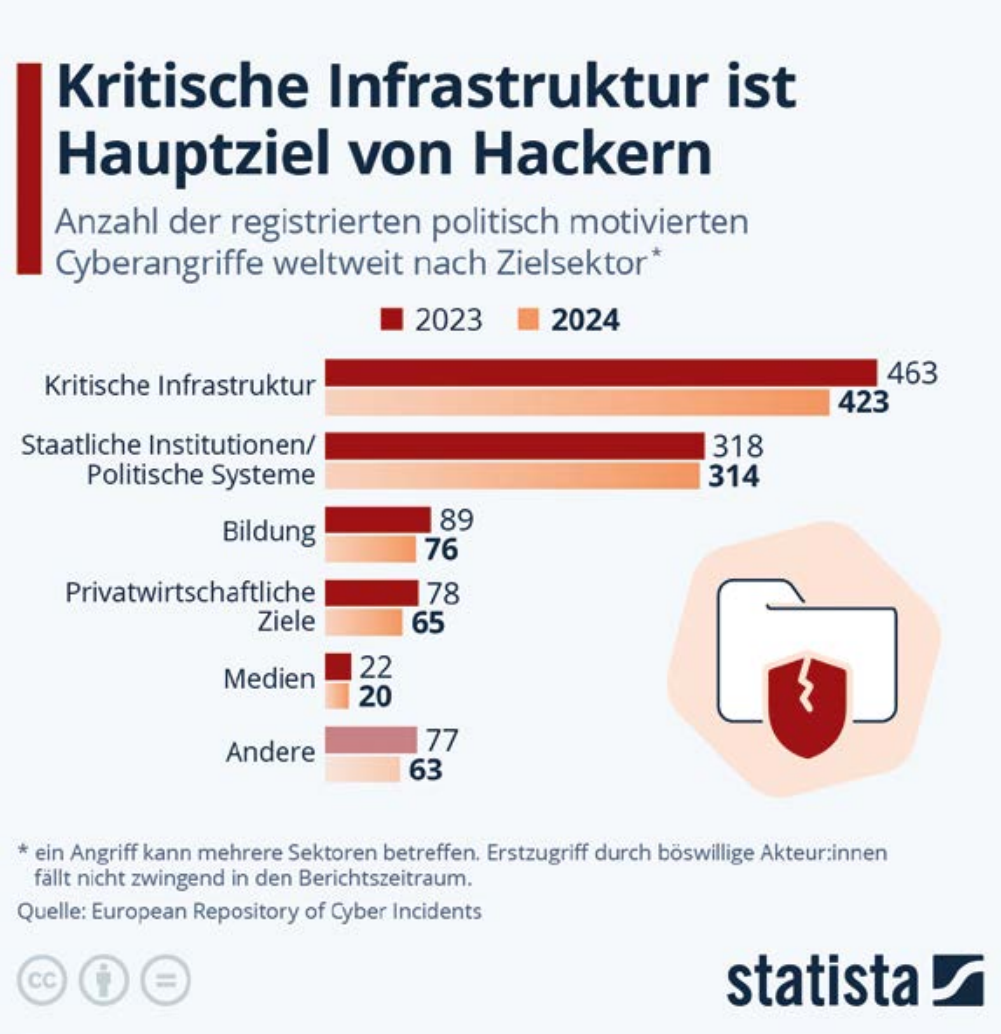
Franz Polenz: Richtig. Es greift alles ineinander. Man sollte sich auch davor hüten zu sagen, dass nur eine bestimmte, kleine Gruppe von Unternehmen betroffen ist. Heutzutage muss jedes Unternehmen prüfen, wo seine Verwundbarkeiten sind. Die Vektoren sind vielfältig, Angriffe können auf die physische Infrastruktur, durch Personen oder in Form von Cyberangriffen erfolgen. Auf ein Unternehmen selbst oder auf dessen Zulieferer. Insbesondere Cyberangriffe haben in den vergangenen Jahren massiv zugenommen. Deswegen sind die Unternehmen gehalten, eine saubere Risikoanalyse durchzuführen, um den vielfältigen Bedrohungen entgegenzuwirken.

Sprechen wir über Spionage. Geht es bei Unternehmen im Wesentlichen um Wirtschaftsspionage?

Franz Polenz: Die klassische Know-how-Ausspähung oder Konkurrenzspionage ist sicherlich ein wichtiger Punkt. Allerdings sind in den Ländern, die in den Verfassungsschutzberichten immer wieder als Akteure genannt werden, die jeweiligen staatlichen Nachrichtendienste sehr eng verknüpft mit konkreten Wirtschaftsinteressen. Es lässt sich daher oftmals nicht sauber trennen, ob es bei der Ausspähung von Know-how um rein wirtschaftliche oder um geopolitische Interessen geht. Für ein Unternehmen ist diese Frage letztlich aber auch zweitrangig. Die Gefährdung ist da, man muss versuchen, sie zu erkennen und entsprechende Methoden zur Abwehr implementieren.

Können Sie die Folgen skizzieren, die eine wie auch immer motivierte Ausspähung für ein Unternehmen haben kann?

Franz Polenz: Wenn Sie heute Know-how verlieren, kann das bedeuten, dass zu einem gewissen



Zeitpunkt Ihre Produkte im Ausland von einer fremden Firma mit Ihrer Technologie gebaut werden, die illegal erworben wurde. Für kleinere und mittelständische Unternehmen kann dies im schlimmsten Falle den wirtschaftlichen Ruin bedeuten. Für größere Unternehmen kann es bedeuten, dass man Marktvolumen verliert, Produktlinien einstellen muss und am Ende Stellen abgebaut werden müssen. Der individuelle Schaden eines Unternehmens führt in der Regel somit auch immer zu volkswirtschaftlichen Gesamtschäden.

Welche Möglichkeiten haben Unternehmen, eine Ausspähung frühzeitig zu bemerken?

Franz Polenz: Das Wichtigste sind zunächst aufmerksame Mitarbeiterinnen und Mitarbeiter. In einem Forschungs- und Entwicklungsbereich beispielsweise, der als Sonderzutrittszone definiert ist, haben die dort Beschäftigten die Aufgabe sicherzustellen, dass niemand Unbefugtes diesen Bereich betritt. Ein Unternehmen muss klar benennen können, was sind die kritischen Bereiche, wo wird Know-how produziert, wo befinden sich die sogenannten Golden Nuggets. Diese Bereiche kann man dann entsprechend schützen, durch aufmerksame Mitarbeiterinnen und Mitarbeiter, durch physikalische Barrieren und ein entsprechendes Zutrittskontrollkonzept. In der Cybersecurity kann man Applikationen wie Data Leakage Prevention einsetzen, die eine Alarmmeldung auslösen, wenn jemand zum Beispiel auffällig hohe Datenmengen von einem Laufwerk kopiert. Durch ein holistisches, abgestimmtes Sicherheitskonzept kann man Risiken also deutlich minimieren.

Welche Rolle spielt das Thema Innentäter, also eigene Beschäftigte, aber auch externe Partner und Lieferanten?

Franz Polenz: Zunächst ist wichtig, dass ein Unternehmen seinen Mitarbeitern und Geschäftspartnern vertrauen kann. Man darf das Thema Innentäter aber nicht ignorieren. Bei kritischen Bereichen muss man sich die Frage stellen, wer geeignet ist, dort zu arbeiten. Die Antwort ist

nicht immer einfach. Beim Thema Background-Checks zum Beispiel gibt es in Deutschland klare rechtliche Grenzen, die Unternehmen einhalten müssen. Was bedeutet, dass man am Ende auch hier sicherlich ein gewisses Restrisiko akzeptieren muss.

Kommen wir von der Spionage zur Sabotage. Vorfälle wie der Angriff auf Unterseekabel in der Ostsee schaffen es in die Tagesschau. Das ist aber nur die Spitze des Eisbergs. Welche Angriffe erleben Unternehmen tagtäglich?

Franz Polenz: Nicht alle Angriffe haben einen Hintergrund, der sich auf einen fremden Nachrichtendienst oder Staat beziehen. Neben normaler Kriminalität wie Diebstählen an Unternehmensstandorten sieht man mit einer gewissen Regelmäßigkeit Aktionen und strafbare Handlungen von Umweltaktivisten oder extremistischen Gruppierungen. Das kann Vandalismus beinhalten wie Farbanschläge oder Brandstiftungsdelikte gegen Firmenfahrzeuge. Dann gibt es Vorfälle ohne eigentliche Sachbeschädigung, zum Beispiel Proteste, bei denen Aktivisten sich an ein Werkstor anketten und die Zufahrt blockieren. Diese Art von Störungen ist für Unternehmen eher ein Reputationsthema, weil Aktivisten soziale Medien nutzen, um öffentlichkeitswirksam gegen ein Unternehmen zu protestieren. Eine solche Situation ist aus Sicherheitssicht zumeist relativ schnell vorbei, erfordert möglicherweise aber ein gutes Krisenkommunikationsmanagement, indem man ein entsprechendes, korrigierendes Narrativ in der Öffentlichkeit platziert.

Wir haben über die vielfältigen Bedrohungen gesprochen. Wie gut ist Deutschland auf solche Gefahren vorbereitet? Sind deutsche Unternehmen und Organisationen heute resilienter als vor fünf oder zehn Jahren?

Franz Polenz: Wir sind resilienter als vor fünf Jahren, aber noch nicht resilient genug. Wenn wir in andere Länder schauen, haben wir in Deutschland noch Nachholbedarf. In den skandinavischen Ländern beispielsweise sind die gesamte Gesellschaft und damit auch das Individuum und die Wirtschaftsunternehmen deutlich besser vorbereitet, was Zivilverteidigung angeht. Der Ukraine-Krieg war für viele ein Weckruf. Wir sind in Deutschland resilienter geworden, aber weder in der Gesamtgesellschaft noch in den Unternehmen ist die viel beschworene „Zeitenwende" im Bereich unserer Sicherheit vollumfänglich angekommen.

Welche Rolle spielen Gesetzesvorhaben wie das KRITIS-Dachgesetz und die Umsetzung der NIS2-Richtlinie für die Prävention und das Bewusstsein für Bedrohungen?

Franz Polenz: Sie senden ein Signal an die Verantwortlichen im Management, dass wir besser werden müssen in der Umsetzung von Sicherheitsanforderungen. Allerdings sind höhere Investitionen in die Sicherheit manchmal schwierig umzusetzen, weil das Management begrenzte Ressourcen hat und gegenüber den Aktionären und dem Aufsichtsrat für den Gesamterfolg des Unternehmens verantwortlich ist. Daher müssen viele wichtige Themen bei der Ressourcenzuteilung ausgewogen betrachtet werden. Bei der Umsetzung gesetzlicher Regelungen kommt es aber insbesondere auch auf die Qualität der jeweiligen Gesetze an. Wenn mit neuen gesetzlichen Regelungen im Bereich der Sicherheit nur bürokratische Meldepflichten gefordert werden, es aber keinen Zuwachs an realer Sicherheit gibt, dann bringt das relativ wenig. Wenn gesetzliche Regelungen den Unternehmen aber bei ihrer Risikoanalyse und der Umsetzung zielgerichteter Schutzmaßnahmen helfen, dann sind sie sowohl für die Awareness als auch für das faktische Schutzniveau sinnvoll.

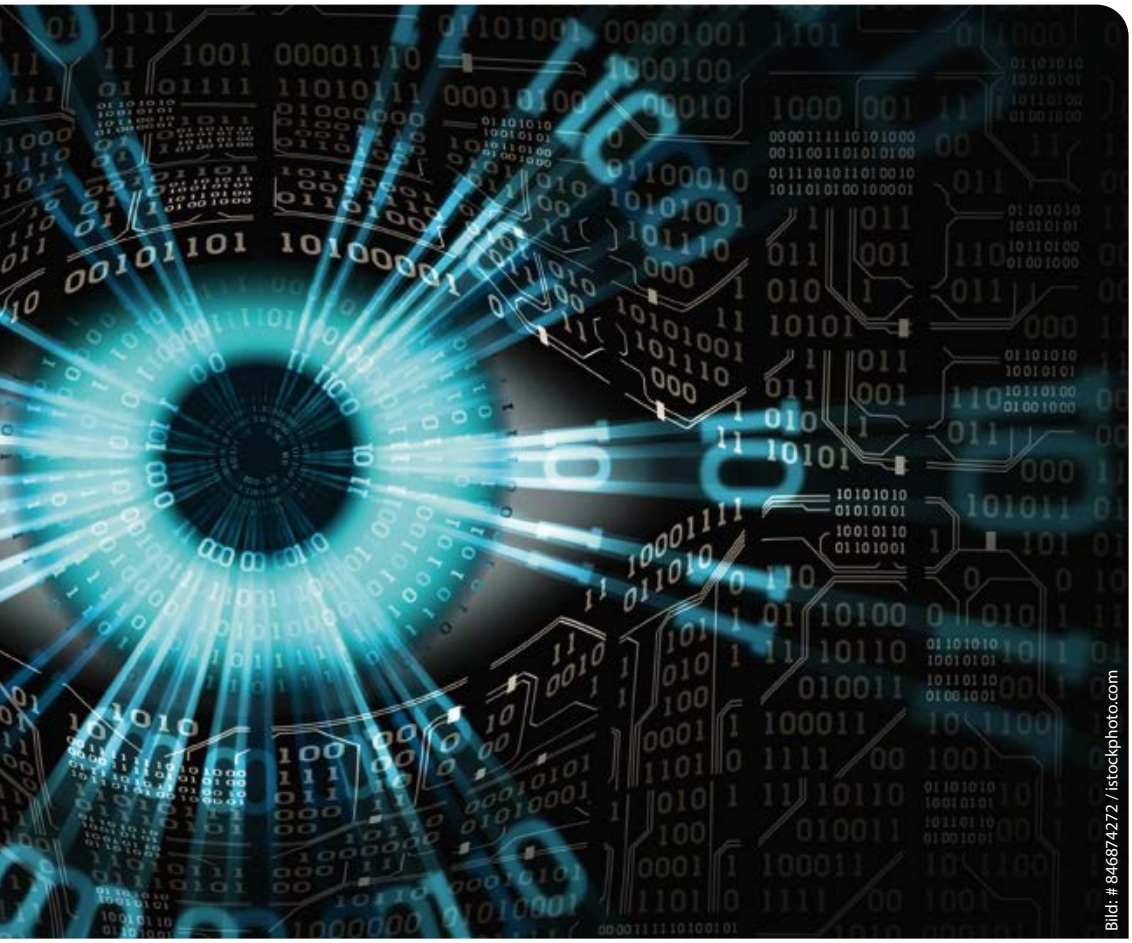


Bild: # 846874272 / istockphoto.com

Vor allem kleinere und mittlere Unternehmen haben noch Nachholbedarf beim Thema Sicherheit. Was sollte ich als Unternehmen in einer solchen Situation tun und wo finde ich Hilfe?

Franz Polenz: Zunächst einmal ist wichtig, dass ich eine methodisch saubere Risikoanalyse mache. Was mache ich, welchen Bedrohungen bin ich ausgesetzt, welche Schwachstellen habe ich, wie hoch ist das Risiko? Dann prüfe ich, wie ich dieses Risiko minimieren kann. Dafür sollte ich mir kompetente Ansprechpartner suchen. Für Spezialthemen kann das ein Beratungsunternehmen sein. Für allgemeine Sicherheitsthemen gibt es sehr gute Hilfestellungen durch die IHKs oder Verbände wie den ASW und die entsprechenden Landesverbände. Es gibt mittlerweile fast in jeder Landes- oder Bundessicherheitsbehörde eine Ansprechstelle für Wirtschaftsschutz. Von daher können auch KMUs sich mittlerweile sehr gut informieren, was Risikoanalyse und Unternehmenssicherheit betrifft.

Herr Polenz, was würden Sie sich mit Blick auf die besprochenen vielfältigen Bedrohungen von der nächsten Bundesregierung wünschen?

Franz Polenz: Wie erwähnt, arbeiten Behörden schon viel enger mit der Wirtschaft zusammen. Manchmal könnte diese Zusammenarbeit aber schneller sein. Das fängt an bei der Terminfindung für einen gemeinsamen Austausch oder bei Reaktionszeiten auf eine E-Mail-Anfrage. Es gibt auch gute Beispiele, wie etwa die Global-Player-Initiative des Bundeskriminalamtes oder die Bestrebung, eine Nationale Wirtschaftsschutzstrategie zu erstellen. Es wäre wünschenswert, dass diese Strategie am Ende einen tatsächlichen Mehrwert für Unternehmen bietet. Hier würde ich mir von der nächsten Bundesregierung wünschen, dass das Thema Wirtschaftsschutz nicht nur auf deklaratorischer Ebene betont wird, sondern dass entsprechende Ressourcen und Strukturen dahinterstehen, um die Unternehmen in Deutschland zielgerichteter zu unterstützen.

Warten wir ab, ob es so kommt. Vielen Dank für das Gespräch!

Brandmauern gegen Cybercrime

Von Stefan Pyper

Stefan Pyper

Geschäftsführer der GCT Gesellschaft für Computer-Technologie mbH, Bad Homburg

www.gct.de

Die Bedrohungslage

Die IT-Sicherheitslage in Deutschland ist und bleibt hochkritisch. Wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Bericht von 2024 feststellt, sind Angriffe durch Cyberkriminelle nicht nur häufiger, sondern auch professioneller geworden.

Ransomware-Gruppen nutzen Malware-as-a-Service-Angebote, umgehen Schutzsysteme wie EDR und setzen gezielt Zero-Day-Exploits ein – bisher unbekannte Sicherheitslücken, für die es noch keine Patches gibt. Viele IT-Infrastrukturen sind diesen Bedrohungen machtlos ausgesetzt.

Parallel existieren kriminelle Märkte: Zugangsdaten werden durch sogenannte Access Broker verkauft, Angriffe auf Cloud-Dienste führen zu Identitätsdiebstahl und DDoS-Attacken legen Unternehmen lahm. Auch kleine und mittelständische Firmen sind zunehmend betroffen.

Laut Statista wurden 2024 in Deutschland täglich etwa 250.000 neue Schadprogramm-Varianten registriert. Der wirtschaftliche Schaden belief sich auf über 266 Milliarden Euro – ein neuer Höchstwert.

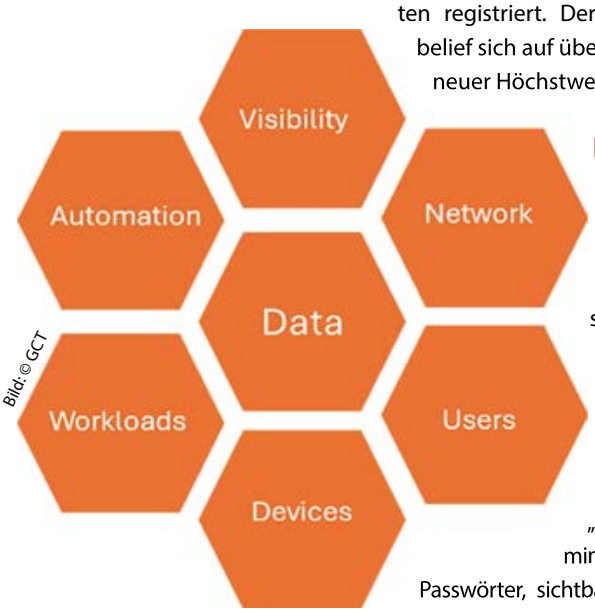


Bild: © GCT

Der Internet-Router als Schwachstelle

Oft beginnt ein erfolgreicher Angriff über einen unsicheren Router. Viele Unternehmen setzen Geräte ein, die eigentlich für den Heimgebrauch gedacht sind. Diese Kombigeräte aus Router, WLAN und „Firewall" bieten häufig nur minimale Sicherheit: schwache Passwörter, sichtbare Netzwerke und offene Ports sind ein gefundenes Fressen für Angreifer.

Besonders gefährlich: Zero-Day-Schwachstellen, die schon bei Auslieferung vorhanden, aber dem Hersteller nicht bekannt sind und daher noch nicht behoben werden konnten.

Dabei ist professioneller Schutz kein Luxus. Eine SonicWall TZ80 beispielsweise bietet ein deutlich höheres Sicherheitsniveau und bleibt dabei auch für KMU bezahlbar. In Verbindung mit einem Network Operations Center (NOC) – also einer zentralen Stelle zur Überwachung der Netzwerkinfrastruktur – lässt sich die Unternehmens-Brandmauer erheblich verbessern.

Warum eine NextGen Firewall der Stand der Technik ist

Wie beschrieben, sind die Netzwerke vieler KMUs nur mit einer einfachen Standardlösung aus dem Bereich der Heimnetz-Lösungen geschützt. Diese sind den aktuellen Cyberbedrohungen nicht gewachsen und bieten daher keinen echten Schutz. Next Generation Firewalls (NGFWs) aber leisten genau das: Sie schließen unnötige Zugänge ins lokale Netzwerk, erkennen und blockieren Bedrohungen in Echtzeit, analysieren auch den verschlüsselten Datenverkehr und verhindern gezielte Angriffe durch eine Kombination modernster Security-Schichten.

Security-Lösungen wie SonicWall Firewalls bieten zusätzlich KI-gestützten Schutz, auch vor Ransomware, sichere VPN-Zugänge für mobiles Arbeiten und eine zentrale Steuerung – einfach und übersichtlich.

KI – Fluch und Segen in der Cybersicherheit

Apropos KI: Künstliche Intelligenz ist ein zweischneidiges Schwert in der Welt der IT-Sicherheit. Auf der einen Seite nutzen Cyberkriminelle KI, um gezielte Phishing-Mails automatisch zu erstellen, Firewalls auszutricksen oder Sicherheitslücken blitzschnell zu finden. KI-basierte Phishing-Attacken sind oft so täuschend echt, dass sie selbst geübten Mitarbeitenden nicht sofort auffallen.

Bild: © BSI

Auf der anderen Seite unterstützt KI die Funktionen moderner Firewalls. Sie erkennt verdächtiges Verhalten in Echtzeit, lernt ständig dazu und blockiert solche Angriffe, bevor sie Schaden anrichten. Anders als klassische Systeme reagiert sie nicht nur auf bekannte Bedrohungen, sondern auch auf neue Muster.

Also: KI ist nicht nur ein Risiko – sie ist auch Ihre stärkste Verteidigung. Entscheidend ist, wer sie zuerst oder besser nutzt.

Doch die beste technische Lösung versagt, wenn sie falsch konfiguriert ist oder die Konfiguration nicht aktuelle Strategien der IT-Security abbildet.

Zero Trust: Vertrauen ist keine Strategie

Eine moderne Sicherheitsstrategie basiert auf dem Prinzip: Vertraue niemandem. Beim sogenannten Zero Trust wird jede Aktion überprüft – unabhängig davon, ob sie von innen oder außen kommt.

Nutzer erhalten nur Zugang zu dem, was sie wirklich benötigen. Netzwerke werden segmentiert, besonders sensible Bereiche zusätzlich durch Firewalls geschützt.

Mehr als zwei Drittel der Unternehmen in Deutschland setzen laut TechTarget bereits auf Zero-Trust-Richtlinien. SonicWall-Produkte lassen sich gezielt einsetzen, um diese Struktur sicher, skalierbar und effizient umzusetzen.

SOC: die Betriebsfeuerwehr der IT

Oft reicht ein Network Operations Center (NOC) als interne Instanz zur Überwachung der Netzwerkinfrastruktur nicht aus, bspw. bei Unternehmen, die sich an der NIS-2-Richtlinie der EU und dem daraus für den Spätherbst erwarteten Gesetz orientieren müssen. IT-Security-Expertise ist rar und muss im Falle einer Attacke auch 24/7 verfügbar sein. Hier spielt das Security Operations Center (SOC) als externe Instanz eine zentrale Rolle. Es detektiert und analysiert sicherheitsrelevante Ereignisse, koordiniert Abwehrmaßnahmen im Ernstfall und trägt zur Sicherheitsaufklärung bei.

Notfallplan: Wenn's wirklich brennt

Auch bei bester Vorbereitung kann ein Vorfall eintreten. Dann ist ein strukturierter Notfallplan entscheidend: Wer macht was, wann und wie? Ohne klare Rollen und Abläufe riskieren Unternehmen Chaos, längere Ausfallzeiten und hohe Folgeschäden. Gerade für kleine und mittlere Unternehmen gibt es praktikable Lösungen. Das BSI bietet mit der IT-Notfallkarte sowie Maßnahmenkatalogen und den „TOP 12 Maßnahmen bei Cyberangriffen" konkrete Hilfestellung – auch für Unternehmen ohne eigene IT-Abteilung.

Die Top-12-Maßnahmen bei Cyberangriffen

Das richtige Verhalten und die richtigen abgeleiteten Maßnahmen im Notfall sind der Schlüssel für die Unterbindung der Bedrohung – im akuten Fall, aber auch in Zukunft. Die folgende Liste ist eine Kurzzusammenfassung der zwölf wichtigsten Maßnahmen im Falle einer Bedrohung.

- Bewertung ob Attacke oder Defekt
- Kontinuierliche Abstimmung der Maßnahmen
- Forensische Sicherung von Logs, Datenträgern, Screenshots etc.
- Fokus auf zeitkritische Prozesse
- Trennung betroffener Systeme & Zugänge
- Stoppen von Backup-Jobs zum Schutz bestehender Backups
- Ausmaß des Angriffs feststellen
- Schwachstelle für Angriff beheben
- Information an Polizei und Behörden
- Zugänge der betroffenen Accounts geprüft
- Weitere Überwachung des Netzwerks
- Systeme und Daten wiederherstellen

Fazit

Cyberangriffe sind kein Ausnahmefall mehr, sondern Geschäftsrealität. Die Frage lautet nicht, ob ein Unternehmen angegriffen wird, sondern wann. Ein Internetrouter für das Heimnetz reicht nicht aus, um ein Unternehmen zu schützen.

Was es braucht, ist ein umfassender Ansatz: sichere Hardware, ein aktives NOC, Zero-Trust-Richtlinien, ein vorbereitetes SOC – und einen klaren Notfallplan.

Zusätzlich braucht es einen Prozess, der sicherstellt, dass die implementierte IT-Sicherheit aktuellen Anforderungen oder auch Veränderungen im Unternehmen gerecht wird. Denn IT-Sicherheit ist kein Zustand, sondern ein Prozess.

Bild: © SonicWall

DORA: fünf Gelegenheiten, um Cybersicherheit und Resilienz zu erhöhen

Von Nicholas Jackson

Nicholas Jackson

Director of Cyber Security Services bei Bitdefender

Bitdefender ist ein weltweit führender Anbieter von Cybersicherheitslösungen zur Abwehr, Erkennung und Reaktion auf Bedrohungen. Bitdefender schützt mehrere Millionen von Endverbrauchern sowie IT-Umgebungen in Unternehmen und im öffentlichen Sektor.

Weitere Informationen finden Sie unter **www.bitdefender.de**

Der Digital Operational Resilience Act (DORA), welcher am 17. Januar 2025 in Kraft getreten ist, betrifft nicht nur Anbieter von Finanzdiensten, sondern auch deren IT-Dienstleister: Dazu gehören sowohl Partner und Distributoren, aber auch indirekte IT-Dienstanbieter, wie die Anbieter von IT-Sicherheitsplattformen. Der Kreis der Unternehmen, für die sich aus dem Gesetz neue Hausaufgaben ergeben, ist also größer als vermutet. Für alle ist DORA aber eine Chance, die Resilienz ihrer IT-Infrastruktur gegen Cyberangriffe jetzt zu erhöhen.

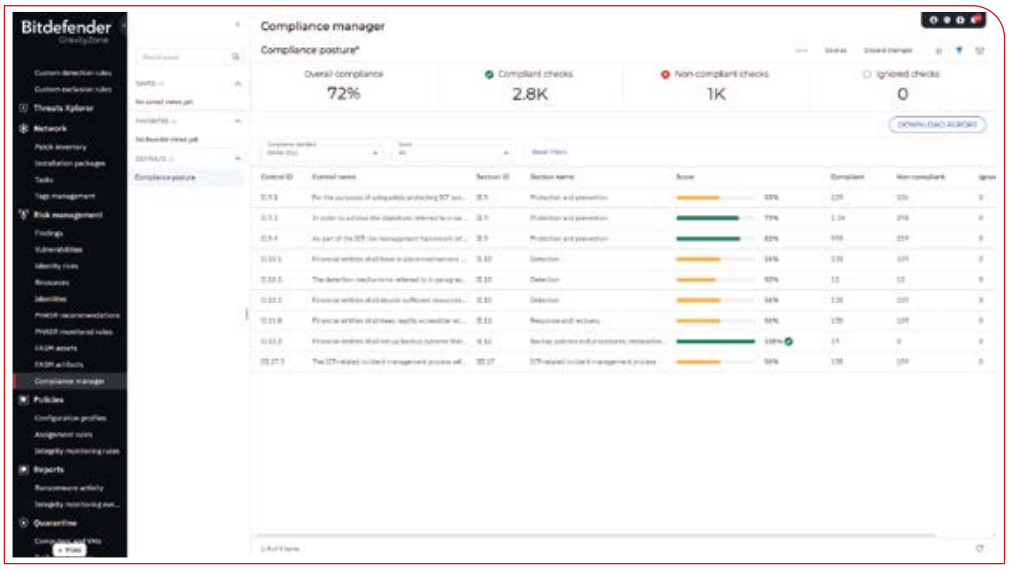
DORA zielt darauf ab, die operative Resilienz im gesamten Finanzsektor und in den EU-Mitgliedstaaten zu standardisieren, und legt deshalb eine Reihe von Best Practices für eine bessere Cyberresilienz fest. Bei Verstößen gegen die DORA-Richtlinien drohen in der EU tätigen Organisationen Geldstrafen und andere Sanktionen. Ähnlich wie bei der DSGVO sind Strafen für Unternehmen in einer Höhe von bis zu zwei Prozent des weltweiten Umsatzes möglich. Darüber hinaus können EU-Mitgliedstaaten auch individuelle Bußgelder für hochrangige Personen und Dritte beschließen. Bestrafen ist aber in der Absicht der Gesetzgeber nur die Ultima Ratio. Vor allem sind Aufsichtsbehörden daran interessiert, zu sehen, welche Schritte nicht konforme Organisationen unternehmen, um die operative Resilienz des gesamten Sektors weiter zu stärken. Alle Beteiligten sollten sich daher klarmachen, was die umfangreiche regulatorische Vorgabe konkret für in der EU tätige Finanzunternehmen und deren IT-Dienstleister bedeutet.

EU-Finanzbranche: Risiko durch eine stark vernetzte und abhängige IT

Die Finanzbranche ist stark von digitalen Technologien abhängig und beeinflusst fast alle anderen Wirtschaftsbereiche. Unterbrochene digitale Prozesse können den Fluss von Finanzmitteln für Kritische Infrastrukturen zum Erliegen bringen, sich auf Versicherungspolicen in der gesamten EU auswirken oder den freien Verkehr von Waren und Dienstleistungen zwischen Mitgliedstaaten behindern. Die Fähigkeit, fast jede Art von Transaktion unabhängig von ihrer Größe oder ihrem Umfang über Grenzen hinweg nahezu sofort durchzuführen, ist das A und O für alle wirtschaftlichen Vorgänge.

Eine der größten Ansprüche an die operative Resilienz in der Finanzbranche ergibt sich aus ihrem ausgedehnten und den Prozessen zugrunde liegenden Netzwerk. Die dafür notwendigen automatisierten Prozesse hängen von komplexen Infrastrukturen ab, die sich über lokale Rechenzentren und Cloud-Dienstleister erstrecken. Diese Abhängigkeit von Drittparteien und Technologieanbietern stellt für Finanzorganisationen ein großes Risiko dar und nimmt Drittanbieter in die Pflicht.

Wie lassen sich die sich daraus ergebenden Aufgaben einer DORA-Compliance lösen? IT-Sicherheitsanalysten im Finanzsektor und bei deren



Bilder: Bitdefender

ITK-Dienstleistern müssen fünf Punkte berücksichtigen, um die neue Richtlinie gewährleisten zu können:

1. Risikomanagement für IT und Kommunikation

Niemand kann schützen, was er nicht kennt. Daher verlangt DORA von den IT-Sicherheitsverantwortlichen und -entscheidern, dass sie ihre IT-Infrastruktur und Systeme besser verstehen und erkennen, wie sie sich selbst und ihre Kunden gefährden: Welche digitalen Assets sind vorhanden? Wie wichtig sind sie für die operative Resilienz? Welche Folgen hätte eine kompromittierte oder ausgefallene Applikation? Wie sind Systeme miteinander verbunden? Über welche Kontrollen verfügt das Unternehmen, um sie zu schützen? Diese Fragen sind grundlegend, um zu schützende Assets zu identifizieren und das tatsächliche Risiko effektiv zu bewerten. Sich an Gefahren orientierende Penetrationstests spielen eine zentrale Rolle. Sie geben den IT-Sicherheitsteams Einblicke in den möglichen Verlauf eines Sicherheitsvorfalls und zu den Maßnahmen, um Gefahren abzuwehren und zu beheben.

2. Fokus auf Drittanbieter und deren Einfluss auf das Geschäftsrisiko

Heutzutage funktionieren Geschäfte oder Prozesse selten ausschließlich mit unternehmensinternen Beteiligten. Auftragnehmer, Zulieferer und andere Dienstleister spielen eine wichtige Rolle im Geschäftsbetrieb. Ohne das zugehörige Risikomanagement ist jede externe Organisation oder Lösung ein Risiko für IT-Betrieb und IT-Sicherheit. Wird einer dieser Zugangspunkte kompromittiert, können sich Angreifer auf der Suche nach weiteren Zielen auf andere Systeme ausbreiten.

DORA ist sich dieser Abhängigkeit von Dritten bewusst und verlangt daher von Unternehmen, dass sie die Effekte ihrer Dienstleister auf das Geschäftsrisiko besser verstehen. Hierzu zählen IT- und Telekommunikationsdienstleister, Managed-Service-Anbieter, Cloud-Service-Anbieter, Verkäufer, Software-as-a-Service-Plattformen (SaaS) und andere Unternehmen, die nicht verwaltete Applikationen, Dienste und Geräte nutzen. DORA verlangt, dass Finanzorganisationen die Effekte von Drittanbietern dokumentieren und sicherstellen, dass geeignete Sicherheitsmaßnahmen getroffen wurden, um miteinander verzahnte Prozesse von Anfang bis Ende zu schützen. Die Basisdokumentation sollte in einem Informationsregister (Register of Information) abgelegt und leicht zugänglich sein: In dem Register finden sich dann Identifikationsdaten der Drittanbieter, wie etwa Standort, Kontaktdaten, Vertragsinformationen, Leistungsumfang, Risikokategorien, Regeln zum Monitoring sowie Angaben zu internen Zuständigkeitsverhältnissen.

3. Incident Management

DORA verlangt von Finanzinstituten außerdem fest strukturierte Prozesse, um IT-Sicherheitsvorfälle zu erkennen, zu bearbeiten und zu melden. Klare Klassifikationskriterien, zeitnahe Eskalationsprozesse und ein einheitliches Reporting-Framework mit strengen Zeitvorgaben sind dafür notwendig. Tabletop-Simulationen zur operativen Resilienz unterstützen diese Abläufe. Solche Manöver stellen sicher, dass alle Beteiligten die Richtlinien zur Disaster Recovery und zur Kontinuität von Geschäftsprozessen kennen und im Ernstfall sofort Maßnahmen ergreifen können.

4. Change Management

Unternehmen und ihre digitalen Umgebungen unterliegen einem ständigen Wandel. Daher ist es wichtig, dass Sicherheitsteams Einblick in IT-Modifikationen und deren Folgen für das Betriebsrisiko haben. Dies alles müssen sie erkennen, neu bewerten und die sich ergebenden Konsequenzen umsetzen sowie überwachen. Ebenso wichtig ist es, bestehende Richtlinien zu autorisieren und durchzusetzen. Derart gesichert können Angreifer diese nicht unbefugt modifizieren. Als eine logische Konsequenz bewerten Lösungen und IT-Sicherheitsverantwortliche Software-Updates, Modifikationen der Infrastruktur und die Integration von Dritten. Sicherheitsteams sollten vor und nach dem Implementieren neuer Assets deren Integration testen. Letztendlich stellt DORA sicher, dass Change-Management-Prozesse streng moderiert sind und strukturierte Genehmigungsabläufe in Kraft sind.

5. Compliance dokumentieren

Einen weiteren Schwerpunkt legt DORA auf die Rechenschaftspflicht. Wer in der Pflicht für seine sämtlichen Systeme steht, muss insbesondere für seine kritischen Systeme kontinuierliche Schwachstellentests durchführen, Risiken bewerten und – vor allem – darüber berichten. Unternehmen sollten einheitliche Vorlagen verwenden, in denen Vorgaben und Zeitpläne festgelegt sind, und diese in das bereits erwähnte Informationsregister eingeben. Die dort gesammelten Informationen von Dritten, vertragliche Vereinbarungen, bewertete Risiken, Abhängigkeiten, Vorfälle und Notfallpläne übermitteln sie bei Bedarf an externe Prüfer.

Dafür reicht es nicht aus, Informationen zu sammeln. Angesichts heute immer komplexerer IT-Infrastrukturen bedarf es der Analyse und verwertbaren Aufbereitung dieser Informationen. Erst in einer hinreichenden Form dient das Informationsregister bei Angriffen oder anderen Vorfällen als Leitfaden und liefert den Sicherheitsteams den nötigen Kontext, um schnell und einschlägig zu agieren. Die Dokumentation kann zum Beispiel auch Schritt für Schritt vorgeben, wie Wissen und Expertise im Unternehmen verbleiben, wenn Mitarbeiter dieses verlassen.

DORA als Chance für eine gestärkte Resilienz

Bei so vielen Vorgaben bleibt zu betonen: DORA ist nicht nur eine gesetzliche Pflicht. Sie bietet Finanzorganisationen und Dienstleistern eine hervorragende Möglichkeit, ihre Cyber- und operative Resilienz zu stärken sowie ihre Sicherheitsstrategien zu optimieren. Die Kriterien der neuen Vorschrift sind speziell auf die dynamischen Notwendigkeiten der Finanzbranche in der heutigen, vernetzten Geschäftswelt zugeschnitten und können mit anderen Standards oder Geschäftszielen harmonisieren.

„Nähe ist kein Zufall“ – 100 Tage im Amt

Im Gespräch mit Werner Landstorfer

Werner Landstorfer

Präsident des Bundesverbandes der Sicherheitswirtschaft (BDSW)

Seit rund 100 Tagen ist Werner Landstorfer Präsident des Bundesverbandes der Sicherheitswirtschaft. Der langjährige Landesgruppenvorsitzende aus Bayern hat sich zum Ziel gesetzt, den Kontakt zu den Mitgliedsunternehmen zu intensivieren und die politische Sichtbarkeit der Branche weiter zu stärken. Im Gespräch mit Silke Zöller, Leiterin der Kommunikation im BDSW, zieht er für den DSD Der Sicherheitsdienst eine erste Bilanz.

Herr Landstorfer, Sie kennen den Verband und die Branche seit vielen Jahren. Wie haben Sie die ersten 100 Tage im neuen Amt erlebt?

Werner Landstorfer: Die ersten Monate waren intensiv – aber im besten Sinne. Ich bin mit offenen Türen und ehrlichem Interesse empfangen worden, sowohl von unseren Mitgliedsunternehmen als auch auf politischer Ebene. Natürlich war mir vieles vertraut, aber der Blick vom Präsidentenstuhl ist noch einmal ein anderer.

Was hat Sie persönlich dazu bewogen, sich für dieses Amt zur Verfügung zu stellen?

Werner Landstorfer: Ich habe die Branche in ihrer ganzen Vielfalt schätzen gelernt. Gerade in den letzten Jahren ist deutlich geworden, wie systemrelevant Sicherheitsdienstleistungen sind. Ich möchte dazu beitragen, dass dieser Wert gesellschaftlich und politisch noch stärker anerkannt wird. Und ich glaube, dass meine Erfahrung aus der Praxis und auch der Verbandsarbeit auf Landesebene dabei hilfreich ist.

Wie unterscheiden sich Ihre Aufgaben als Präsident von denen als Landesgruppenvorsitzender?

Werner Landstorfer: Als Landesvorsitzender ist man sehr nah dran – operativ, konkret, an den Unternehmen der Region. Als Präsident trägt man zusätzlich die Verantwortung, Themen bundesweit strategisch zu platzieren, Verbindungen zu anderen Institutionen zu pflegen und politische Positionen mit Nachdruck zu vertreten. Das ist eine andere Arbeitsgrundlage, aber beides braucht vor allem Nähe zu den Mitgliedsunternehmen.

Welche politischen Themen stehen aus Ihrer Sicht aktuell ganz oben auf der Agenda der Sicherheitswirtschaft?

Werner Landstorfer: Hier gibt es mehrere Schwerpunkte: die Vergabe öffentlicher Aufträge, die faire Einbindung privater Sicherheitsdienste in öffentliche Sicherheitskonzepte, die Nachwuchsgewinnung sowie die Stärkung des Ansehens unserer Branche. Zudem wollen wir die Themen Qualifikation, Zuverlässigkeit und Professionalität unserer Mitgliedsunternehmen noch stärker in den politischen Diskurs einbringen.

Herr Landstorfer, was sind für Sie die größten Herausforderungen im Bereich Lobbyarbeit – insbesondere angesichts eines oft begrenzten Verständnisses für die Branche?

Werner Landstorfer: Die größte Hürde ist tatsächlich, komplexe Sachverhalte so zu vermitteln, dass sie in der politischen und gesellschaftlichen Diskussion verstanden und ernst genommen werden. Viele Menschen, auch die politisch zuständigen bzw. verantwortlichen Personen, wissen nicht, wie breit gefächert und mittlerweile komplex die Leistungen dieser Branche eigentlich sind. Wir

RAin Cornelia Okpara (links) und Werner Landstorfer

Werner Landstorfer (links) mit dem Bayerischen Staatsminister des Innern, für Sport und Integration, Joachim Herrmann

Das neu gewählte BDSW-Präsidium: (vl.) Gerhard Ameis, Cornelius Toussaint, Werner Landstorfer, Nora Rauch, Rasmus Finn Wackerhagen, Rainer Ehrhardt und Friedrich P. Kötter

BDSW-Hauptgeschäftsführerin RAin Cornelia Okpara und BDSW-Präsident Werner Landstorfer

müssen faktenbasiert aufklären, Missverständnisse abbauen und zeigen, wie eng unsere Arbeit mit der öffentlichen Sicherheit verwoben ist.

Sie haben bereits einige politische Gespräche geführt. Wie wird die Sicherheitswirtschaft heute in Berlin wahrgenommen?

Werner Landstorfer: Ich spüre wachsendes Interesse – nicht zuletzt wegen der aktuellen Sicherheitslage in vielen Bereichen der Gesellschaft. Gleichzeitig gibt es, wie gesagt, noch Informationsdefizite. Deshalb ist es unsere Aufgabe, diese Lücken durch konstruktive und fundierte Gespräche zu schließen.

Welche Themenfelder möchten Sie in den kommenden Monaten strategisch stärker in den Fokus rücken?

Werner Landstorfer: Neben den klassischen Kernthemen und den genannten Themen möchte ich die Digitalisierung der Branche, den Einsatz innovativer Technologien und die Förderung nachhaltiger Sicherheitslösungen voranbringen. Auch die Zusammenarbeit mit der öffentlichen Hand auf Augenhöhe ist ein Schwerpunkt, den wir weiter ausbauen wollen.

Gibt es bereits konkrete Maßnahmen oder Projekte, die Sie angestoßen haben oder anstoßen wollen?

Werner Landstorfer: Wir planen, die Sichtbarkeit der Branche und des Verbandes zu erhöhen. Wir wollen dazu neue Dialogformate aufbauen – intern beispielsweise zwischen Landesgruppen und Präsidium, aber auch einen deutlich ausgebauten Kontakt zu den einzelnen Mitgliedsunternehmen etablieren. Zudem wollen wir stärker in einen Austausch und eine Informationskooperation mit politischen Entscheidungsträgern und der Öffentlichkeit treten.

Wie möchten Sie den Dialog mit den Mitgliedsunternehmen dauerhaft gestalten?

Werner Landstorfer (links) und Ralf Brümmer, Country President von Securitas

BDSW meets CoESS: (vl.) Werner Landstorfer, Cornelius Toussaint, Catherine Piana und Alexander Frank

Werner Landstorfer: Ich möchte im Gespräch bleiben – sei es durch persönliche Besuche, Veranstaltungen oder digitale Formate. Wir starten beispielsweise eine Art offene Gesprächsrunde, in der sich die Mitglieder unkompliziert über aktuelle Themen informieren und aktiv einbringen können. Auch der Austausch in und zwischen den Landesgruppen ist mir wichtig – hier entsteht viel gute Praxis, die wir stärker sichtbar machen sollten.

Wie möchten Sie die Sicherheitswirtschaft künftig auch in der breiten Öffentlichkeit stärker präsentieren und ein positives, modernes Bild der Branche vermitteln?

Werner Landstorfer: Wir wollen zeigen, dass Sicherheitsdienstleistungen weit mehr sind als uniformierte Präsenz. Unsere Mitglieder stehen für Professionalität, hohe Qualifikation und verantwortungsvolles Handeln. Das möchten wir durch gezielte Öffentlichkeitsarbeit, Präsenz in den Medien und die Teilnahme an gesellschaftlichen Debatten sichtbar machen. Wichtig ist mir, dass wir nicht nur reagieren, wenn über Sicherheit gesprochen wird, sondern proaktiv zeigen, welchen Beitrag unsere Branche jeden Tag für ein sicheres Umfeld leistet.

Wie wollen Sie den Verband auch gegenüber jüngeren Zielgruppen – etwa neuen Mitarbeitenden oder Start-ups im Sicherheitsbereich – sichtbarer machen?

Werner Landstorfer: Wir müssen gezielt dort präsent sein, wo diese Zielgruppen sich informieren – also auch in sozialen Medien, bei Hochschulveranstaltungen oder über die Agenturen für Arbeit. Wir müssen Wege finden, um die nächste Generation für die Branche zu begeistern bzw. diese überhaupt erst in das Sichtfeld möglicher Interessenten zu rücken.

Welche Rolle spielt aus Ihrer Sicht das Thema Aus- und Weiterbildung für die Zukunftsfähigkeit der Branche?

Werner Landstorfer: Eine ganz zentrale. Die Anforderungen an Sicherheitsdienstleistungen steigen – sowohl fachlich als auch im Hinblick auf kommunikative und interkulturelle Kompetenzen. Wir müssen unsere Qualifizierungsangebote laufend anpassen und erweitern, damit unsere Mitarbeitenden den wachsenden Herausforderungen gewachsen sind.

Cybersecurity wird für viele Branchen immer wichtiger. Welche Bedeutung hat dieser Bereich für die Sicherheitswirtschaft – und wie sollte der BDSW hier agieren?

Werner Landstorfer: Cybersecurity ist längst kein Nischenthema mehr, sondern betrifft jedes Unternehmen – auch in unserer Branche. Wir sehen hier zwei Ebenen: Einerseits müssen Sicherheitsdienstleister selbst vor Cyberangriffen geschützt sein, andererseits bieten sich neue Geschäftsfelder im Bereich IT-Sicherheit und digitaler Schutzmaßnahmen. Der BDSW sollte hier Kompetenzen bündeln,

(vl.) RA Andreas Paulick, Werner Landstorfer und Ernst Steuger

Johannes Strümpfel, Vorstandsvorsitzender des VSW-Bundesverbandes (links) und Werner Landstorfer

Best Practices bereitstellen und den Austausch zwischen klassischen Sicherheitsanbietern und IT-Security-Experten fördern. Wir haben in diesem Jahr den neuen BDSW-Fachausschuss Cybersicherheit ins Leben gerufen, der sich mit diesen Aspekten befasst. Die fachlichen Kompetenzen sollen hier gebündelt werden, um gemeinsam praxisnahe Lösungen und Konzepte zu entwickeln und die Branche auch in diesem wichtigen Zukunftsfeld stark aufzustellen.

Auch große Veranstaltungen stellen besondere Anforderungen an Sicherheitskonzepte. Wo sehen Sie hier die größten Herausforderungen – und welche Rolle spielt der Verband?

Werner Landstorfer: Veranstaltungssicherheit ist komplex, weil sie viele Disziplinen vereint – von Zugangskontrollen über Crowd Management bis hin zu Notfall- und Evakuierungsplänen. Die größte Herausforderung liegt darin, flexibel auf unterschiedliche Szenarien zu reagieren und alle Akteure – Veranstalter, Behörden, private Sicherheitsdienste – optimal zu vernetzen. Der BDSW kann hier durch Leitlinien, Qualifizierungsangebote und die Vernetzung der Beteiligten einen wichtigen Beitrag leisten.

Was hat Sie in den ersten 100 Tagen positiv überrascht – und was eher gefordert?

Werner Landstorfer: Positiv überrascht hat mich, wie groß die Bereitschaft zur Zusammenarbeit innerhalb der Branche ist – und wie offen viele für neue Ideen sind. Gefordert hat mich die Vielzahl an sehr komplexen Themen, beispielsweise die Prozesse zu neuen Gesetzen wie dem Sicherheitsüberprüfungs- und Sicherheitsgewerbegesetz oder auch die Mindestlohnerhöhung, die parallel bearbeitet werden müssen.

Wenn Sie in die Zukunft blicken: Wo sehen Sie die Sicherheitswirtschaft in fünf bis zehn Jahren – und welche Rolle soll der BDSW dabei spielen?

Werner Landstorfer: Ich sehe eine Branche, die technologisch hochmodern, gesellschaftlich fest verankert und politisch als verlässlicher Partner anerkannt ist. Der BDSW wird weiterhin eine zentrale Rolle als Sprachrohr, Impulsgeber und Interessenvertreter spielen. Dafür müssen wir heute die Weichen stellen.

Herr Landstorfer, was möchten Sie den BDSW-Mitgliedern zum Abschluss dieses Gesprächs mitgeben?

Werner Landstorfer: Ich danke allen, die mir bisher ihr Vertrauen und ihre Zeit geschenkt haben. Der Verband lebt vom Engagement seiner Mitglieder. Mein Ziel ist es, ihre Interessen wirkungsvoll zu vertreten – und gemeinsam mit ihnen die Zukunft der Sicherheitswirtschaft zu gestalten. **Wir sind besser zusammen!**

Sitzung im Bundesministerium des Innern: (vl.) Holger Köster, PStS Christoph de Vries und Werner Landstorfer

Sicherheitslage 2025

Von Reinhard Rupprecht

Reinhard Rupprecht

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

Die aktuelle Lage der Inneren Sicherheit in Deutschland ist als sehr differenziert zu bewerten, sowohl hinsichtlich der vielfältigen Bedrohungsursachen als auch hinsichtlich der Betroffenheit von Personen oder Institutionen, staatlichem Bereich oder Wirtschaftsbranchen. Der nachfolgende Beitrag erläutert die Sicherheitslage anhand von Trendbeobachtungen, Kriminalitätsfeldern, Sicherheitsvorfällen und Ermittlungserfolgen.

Polizeiliche Kriminalstatistik (PKS) 2024 als Trendbasis

Die jährliche PKS misst zwar nur das Hellfeld entdeckter und angezeigter Verdachtsfälle, sodass das je nach Deliktsart unterschiedlich große Dunkelfeld unberücksichtigt bleibt. Sie ist aber ein zuverlässiger Maßstab für die im Hellfeld erfassten Kriminalitätssegmente, vor allem in der Langzeitbeobachtung. Die registrierte Gesamtkriminalität – ohne Verkehrskriminalität und PMK – schwankt langfristig leicht in einem Korridor von 6,3 Millionen Fällen im Jahr 2001, 5,6 Millionen 2022 und 5,8 Millionen 2024. Die Gesamtzahl wird sich 2025 nur wenig verändern. Die Häufigkeitszahl (HZ: Fallzahl pro hunderttausend Einwohner) betrug 2015 7.797 und 2024 6.995. Die Aufklärungsquote war 2024 mit 58 Prozent erfreulich hoch (2011: 54,7 %). Auch hier ist 2025 keine gravierende Änderung zu erwarten.

Die Gewaltkriminalität ist zwar 2024 „nur" um 1,5 Prozent auf über 217.000 Fälle angestiegen. Langfristig ist aber die Zunahme besorgniserregend (von 2021 bis 2024 ein Anstieg um 32 %). Steigerungen sind im Bereich der Gewaltkriminalität insbesondere bei nichtdeutschen Tatverdächtigen zu beobachten (2024 gegenüber dem Vorjahr um 7,5 % auf 85.000). Unter der konsequenten Migrationspolitik der Bundesregierung dürfte sich die steigende Tendenz 2025 nicht fortsetzen.

Die Straßenkriminalität hat tendenziell langfristig abgenommen (von fast 1,5 Millionen 2011 auf 1,1 Millionen 2024). Hier ist keine gravierende Änderung im Jahr 2025 zu erwarten.

Die registrierte Betrugskriminalität ist seit 2010 um ca. 25 Prozent auf 743.000 Fälle scheinbar stark zurückgegangen. Aber nicht erfasste 513.000 von Tatverdächtigen im Ausland zulasten Betroffener in Deutschland begangene Delikte zeigen eine steigende Tendenz, die 2025 anhalten dürfte.

Anschläge und Amoktaten

Die Sicherheitslage wird 2025 bedroht durch teilweise politisch oder rassistisch motivierte Angriffe und Anschläge. 2024 wurden über 15.700 Messerangriffe angezeigt, das waren 40 Prozent aller Tötungsdelikte. Da das Mitführen von Messern inzwischen gesetzlich weitgehend verboten wurde und die Polizei dieses Verbot konsequent umsetzt, ist 2025 ein Rückgang dieser Bedrohung jedenfalls im öffentlichen Raum zu erwarten. Besonders belastet wird die öffentliche Sicherheit und das Sicherheitsgefühl der Bürger durch Amokfahrten in Menschenansammlungen hinein, wie dies 2016 auf dem Weihnachtsmarkt in Berlin und am 20. Dezember 2024 auf dem Magdeburger Weihnachtsmarkt geschah. Veranstalter und Kommunen haben inzwischen darauf reagiert und durch Poller oder mobile Hindernisse Menschenansammlungen im öffentlichen Raum weitgehend geschützt (im Einzelnen Reinhard Rupprecht, Schutz öffentlicher Räume, in DSD 1 I 2025, Seite 20 ff.). Viel schwieriger vor Amokfahrten zu schützen sind Umzüge und Demonstrationszüge. So gelang es einem Amokfahrer am 13. Februar, in einen Demonstrationszug in der Münchner Innenstadt von der Rückseite her hineinzufahren. Das BKA registrierte 2024 über 84.000 politisch, ideologisch oder extremistisch motivierte Straftaten, insgesamt 3.000 extremistische Gewaltdelikte. So wurden z. B. in der Nacht zum 18. Juni 2025 in Berlin 36 Transporter an zwei Firmenstandorten in Brand gesetzt. Zu der Tat bekannte sich die linksextremistische Gruppe „Antimilitaristische Aktion". Der Verfassungsschutzbericht für das Jahr 2024 beschreibt ausführlich die Bedrohung der Sicherheitslage durch rechts- oder linksextremistischen sowie islamistischen und auslandsbezogenen Extremismus und Terrorismus. Der Bericht dürfte für das Jahr 2025 nicht günstiger ausfallen.

Bild: # 2162555454 / istockphoto.com

Erhöhte Sabotage- und Spionagegefahr

Spionage, Cyberangriffe, unzulässige ausländische Einflussnahme und Desinformation, Proliferation, Sabotage und Staatsterrorismus stellen – wie das BfV im Jahresbericht 2024 ausführt – eine ernsthafte Bedrohung für die Sicherheit Deutschlands und seiner Interessen dar. Das rechtswidrige Agieren fremder Nachrichtendienste beeinträchtigt die nationale Souveränität. Mögliche Sabotageakte können weitreichende Folgen für das öffentliche Leben haben. Cyberangriffe und Spionage verursachen jedes Jahr erhebliche betriebswirtschaftliche und volkswirtschaftliche Schäden in dreistelliger Milliardenhöhe. Als die vier Hauptakteure identifiziert das BfV die Russische Föderation, die Volksrepublik China, die Islamische Republik Iran und die Republik Türkei (Verfassungsschutzbericht 2024, Seite 301/302). Und Nordkorea infiltriert die Wirtschaft. IT-Kräfte schleichen sich unter falscher Identität und Verschleierung ihres nordkoreanischen Homeoffice nach Erkenntnissen des Sicherheitsunternehmens Mandiant verstärkt auch in deutsche Unternehmen ein (FAZ am 20. Dezember 2024). Der MAD verzeichnet deutlich verstärkte Ausspähversuche und Störmaßnahmen russischer Geheimdienste in Deutschland. dpa berichtet, die Zahl der Verdachtsfälle habe sich binnen Jahresfrist praktisch verdoppelt. Deutschland ist nach Überzeugung der Präsidentin des MAD, Martina Rosenberg, als logistische Drehscheibe für die NATO-Truppenbewegungen und als aktiver NATO-Partner fest im Blickfeld ausländischer Nachrichtendienste.

Vermehrt werden nächtliche Drohnenflüge in Norddeutschland festgestellt, allein in Niedersachsen waren es 2024 insgesamt 131. Besonders gefährdet sind dadurch Bundeswehrstandorte. Mehrfach waren in den vergangenen Monaten Schiffe der Bundesmarine Ziel mutmaßlicher Sabotageaktionen. BND, BSI und BfV informierten gemeinsam die Öffentlichkeit am 23. Mai über russische Cyberaktivitäten, die sich insbesondere gegen westliche Logistik- und Technologiefirmen richten. Sie dienten der Spionage gegen Infrastruktur-Knotenpunkte wie Flughäfen, Seehäfen, Bahnstrecken und Grenzübergänge. Wie die FAZ am 27. Juli berichtet, wollen die Wissenschaftsminister der Länder eine Nationale Plattform für Forschungssicherheit einrichten, um Forschungseinrichtungen gezielt gegen Spionage, Sabotage und ungewollten Wissenstransfer zu schützen.

Angriffe auf Kritische Infrastrukturen (KRITIS)

KRITIS bedürfen wegen ihrer herausragenden Bedeutung für die Wirtschaft, den Staat und die Grundversorgung der Bevölkerung hoher Schutzmaßnahmen, wie sie in der NIS2-Richtlinie (EU 2022/2555) und der CER-Richtlinie (EU 2022/2557) von Betreibern gefordert werden. Neben direkten Angriffen auf KRITIS haben Cyberkriminelle auch die Komplexität von Liefer- und Prozessketten als attraktive Angriffsziele erkannt. Besonders anfällig sind die Kritischen Infrastrukturen der Energieversorgung. Schon zu Beginn des russischen Angriffs auf die Ukraine verloren durch einen offenbar gezielten russischen Hackerangriff auf das Satellitennetzwerk KI-SAT die Betreiber Tausender Windräder in Deutschland die Verbindung zu ihren Anlagen.

Der Sabotageanschlag auf die Gaspipelines Nordstream 1 und 2 am 26. September 2022 verdeutlichte die Verwundbarkeit der Gasversorgung europäischer Staaten. Besonders schwer zu schützen sind auch Kabelanlagen zu Lande wie unter Wasser. Sabotageangriffe auf sie nehmen tendenziell zu. Am 26. Mai 2024 hat eine linksextremistische Gruppe Kabel in Brand gesetzt, die die Baustelle des Tesla-Werks in Grünheide in Brandenburg mit Strom versorgten. Mehrfach wurden in den letzten Jahren Datenleitungen der Deutschen Bahn mit politischer Motivation durchtrennt. Das führte zu vielen Zugausfällen. Im November 2024 wurde die Unterbrechung von zwei Datenkabeln in der Ostsee gemeldet. Am 18. Dezember 2024 wurde das Telekommunikationskabel „C-Lion 1" beschädigt, vermutlich durch das Schiff „Yi Peng 3". Über Unterwasser-Datenkabel

läuft nahezu der gesamte weltweite Internetverkehr. Europa ist über etwa 250 land- und seegestützte Leitungen mit dem Rest der Welt verbunden. Ende Dezember 2024 wurde ein Unterseekabel für die Stromverbindung zwischen Finnland und Estland zerstört, offenbar auch durch einen Tanker der russischen „Schattenflotte". Wichtige Hilfsmittel zur Überwachung maritimer Infrastrukturen sind Satellitenbilder und das automatische Identifikationssystem, das Schiffe aktivieren müssen. Die Deaktivierung des Systems kann auf potenzielle Bedrohungen hinweisen. Durch Detektion ungewöhnlicher Schiffsbewegungen können Warnsignale erkannt werden.

Auch Strommasten sind ein attraktives Anschlagsziel. Und Trinkwassersysteme sind Angriffen ausgesetzt, weil sie kritische Cybersicherheitslücken aufweisen (SECUPEDIA am 8. April 2025).

Cybercrime wird immer raffinierter

Die Bedrohungslage für Cyberkriminalität ist in Deutschland anhaltend hoch. Prägend waren 2024 und sind auch in diesem Jahr vor allem schwere Straftaten wie Ransomware-Angriffe und eine zunehmende Zahl von DDoS-(Distributed Denial of Service-)Kampagnen staatlicher Akteure gegen KRITIS und politische Institutionen. Die fortschreitende Digitalisierung nahezu aller Lebensbereiche schafft seit Jahren neue Tatgelegenheiten für Cyberkriminelle. Mobile Geräte sind der bevorzugte Angriffsvektor. „Smishing"-Bedrohungen (Phishing nach Daten über SMS) machten bereits mehr als zwei Drittel der mobilen Phishing-Angriffe aus. Fast 60 Prozent der iOS-Anwendungen und 43 Prozent der Android-Apps sind anfällig für Datenlecks mit personenbezogenen Daten. Der Trendreport 2025 von Group-IVB zeigt, dass die gefährlichen „Advanced Persistant Threats" (langfristiges Verstecken in Netzwerken) schon 2024 um 58 Prozent gestiegen waren. Betrügerische Cyberattacken nahmen 2024 um 22 Prozent zu (Protector-Newsletter am 5. Mai). Der Bereich „Ransomware as a Service" entwickelt sich rasant.

Auch die Underground Economy im Darknet sucht sich immer raffiniertere Taktiken aus (Reinhard Rupprecht in Technische Sicherheit, Ausgabe 1-2/25, Seite 32 ff.). Nach einer aktuellen Analyse von Panda Security im Juli 2025 kursieren auf Darknet-Marktplätzen ca. 15 Milliarden gestohlene Zugangsdaten. Aber immer wieder gelingt es Ermittlern auch, Darknet-Marktplätze zu schließen: so im März 2024 den illegalen „Nemesis Market" mit mehr als 150.000 Nutzerkonten und im Mai 2025 Netzwerke zum Handel von Waffen und gefälschten Waren. Zu den aktuellen Trends gehören u. a. immer glaubwürdigere Phishing-Kampagnen mithilfe von KI und Angriffe auf Cloud-Infrastrukturen (Der Sicherheitsberater am 10. Juni 2025).

KI: kriminelle Nutzung und Sicherheitstechnik

KI liegt auch 2025 weiter im Trend, sowohl ihr Missbrauch durch Kriminelle als auch ihre sicherheitstechnische Anwendung. Beispiele für Attacken mit KI bilden „Brute Force"-Angriffe, bei denen Passwörter mithilfe selbst lernender AI-gorithmen auf Basis einer Datenbank mit Kennwörtern und Daten potenzieller Opfer verknüpft werden; oder die KI-gestützte Codegenerierung, um neue Malware zu erstellen (Protector, Ausgabe 3/2025, Seite 58/59). KI-basierte Bedrohungen gehören nach der diesjährigen „Hybrid-Cloudsecurity"-Studie von Gigamon für fast die Hälfte der befragten IT-Experten zu den Top-Sicherheitsthemen, sodass sie den Einsatz der Public Cloud hinterfragen (Der Sicherheitsberater am 26. Mai). Laut einer Untersuchung von Signicat aus dem Jahr 2024 erfolgen mittlerweile über 40 Prozent aller Betrugsversuche im Finanz- und Zahlungssektor mit KI-Steuerung oder -Unterstützung. Unternehmensführer seien das Ziel von immer mehr „hyperpersonalisierten" Phishing-Mails, die von KI-Generatoren verfasst werden, warnt der britische Versicherungskonzern Beazkey. Beim Einsatz von KI ist es kaum noch möglich, eine gefälschte Stimme zu erkennen. Angreifer setzen Large Language Models ein, um Texte für Phi-


Bild: # 1781271560 / istockphoto.com

shing-Nachrichten und Webseiten mit Täuschungsabsicht zu erzeugen, lauffähige Schadcodes zu generieren oder zu verfeinern. Firmeninterne Sprachmodelle werden von Kriminellen kompromittiert und zur Exfiltration oder Manipulation von Daten genutzt (Lagebericht 2024 des BSI, Seite 41). Trainingsdaten eines KI-Modells lassen sich so manipulieren, dass das Modell falsche Muster lernt und Daten falsch klassifiziert.

Andererseits revolutioniert KI die Sicherheitstechnik: KI optimiert die Bildanalyse der Videoüberwachung, erkennt und klassifiziert Objekte, analysiert Bewegungen und Verhaltensmuster. Die Weiterentwicklung der Brandfrüherkennung aus regelbasierter Analyse und Deep Learning ermöglicht es, Rauch und Flammen selbst bei Anwendungen in offenen Flächen, hohen Lagerräumen und unter rauen Umgebungsbedingungen zu erkennen. KI unterstützt die Maschinensicherheit in vielfältiger Weise und berechnet den optimalen Wartungszeitpunkt (perspective maintenance). Und sowohl die Weiterentwicklung bestehender als auch die Entstehung neuer Risiken können mit Unterstützung intelligenter Algorithmen ziemlich zutreffend prognostiziert werden.

Eine besonders wichtige Rolle spielt KI in der IT-Sicherheit. Auf „Machine Learning" basierende Schwachstellen-Scanner erkennen Sicherheitslücken und typische Schwachstellenmuster (im Einzelnen: Reinhard Rupprecht, KI in der Sicherheitstechnik, in Technische Sicherheit, 7-8/2024, Seite 13 ff.).

Unterschiedliche Tendenzen im Diebstahlsbereich

Die Entwicklung der Diebstahlskriminalität 2024/2025 zeigt keinen eindeutigen Trend. Während die Anzahl der 2024 in der PKS registrierten Diebstähle das Niveau des Vorcoronajahres 2019 um 6 Prozent übertrifft, ist der Wohnungseinbruchdiebstahl in dieser Zeitspanne um 10 Prozent, der Diebstahl aus Dienst-, Büro- und Lagerräumen sogar um 20 Prozent zurückgegangen. Besonders alarmierend ist der sprunghafte Anstieg der Schadenssumme um 25 Prozent auf 340 Millionen Euro.

Zunehmend scheitern Wohnungseinbrüche im Versuchsstadium (2024 über 46 %), was auch auf den Einsatz von Sicherheitstechnik zurückzuführen ist. Die AQ ist mit 15,3 Prozent bedauerlich niedrig, trotz eines leichten Anstiegs gegenüber dem Vorjahr. Gravierende Veränderungen sind 2025 nicht zu erwarten.

Um den auch 2025 häufigen Baustellendiebstahl einzudämmen, haben das Bauunternehmen Otto Heil und die Syfit GmbH den „digitalen Bauhof" erfunden, meldet die FAZ am 6. Februar. Batteriebetriebene Sender werden in Baugeräten und an Betriebsmitteln verbaut. Sie senden kontinuierliche Signale an mobile Empfangsgeräte und alarmieren, wenn das Gerät unautorisiert die Baustelle verlässt.

Die Inventurverluste im Einzelhandel sind nach der am 24. Juni veröffentlichten Studie des EHI Retail Institute 2024 um 3 Prozent gestiegen. Die meisten Diebstähle werden von Kunden verübt (2024 im Wert von 2,95 Milliarden Euro), gefolgt vom Diebstahl durch Angestellte (890 Millionen Euro) und durch Personal von Lieferanten und Servicefirmen (370 Millionen Euro). Aber nach den Ergebnissen der Studie bleiben 98 Prozent der Diebstähle unentdeckt. Mit der Einführung der „Self Checkout-Kassen" sind neue Modi Operandi aufgekommen, vor allem die Täuschung durch „Umettikettierung" (Benjamin Guth, Revisor bei Globus, in der FAZ am 26. Juni 2025).

Wirtschaftskriminalität und Betrug

Die Fallzahlen im Deliktsbereich Wirtschaftskriminalität unterliegen verhältnismäßig starken Schwankungen aufgrund des Abschlusses mehrjähriger Ermittlungsverfahren. Deshalb ist es unwahrscheinlich, dass der Anstieg 2024 um über 57 Prozent auf über 61.000 Fälle 2025 anhält. Die Entwicklung der Betrugsfälle ist bundesweit nicht einheitlich. Der erneute Rückgang bei Waren- und Warenkreditbetrug um über 10 Prozent resultiert wohl aus dem Anzeigeverhalten der Geschädigten und der Einführung sicherer Zahlungsmöglichkeiten. Im Übrigen zeigt die PKS nicht das volle Ausmaß der Betrugskriminalität. Den ca. 743.000 Betrugsfällen sind weitere über 513.000 hinzuzurechnen, deren Täter im Ausland leben und agieren. Zunehmend werden Betrügereien unter Missbrauch des Internets begangen. Die Quote lag schon 2024 bei über 55 Prozent.

Reisekostenbetrug wird zunehmend mithilfe von KI begangen. Ein plausibler „Prompt" (Eingabeaufforderung) genügt, um realistisch wirkende Tank- oder Restaurantbelege zu erzeugen, die mit bloßem Auge kaum als Fälschung zu erkennen sind. Andererseits hat das Unternehmen Rydoo eine Software entwickelt, die mithilfe von KI Unregelmäßigkeiten in Spesenabrechnungen erkennt (SEDUPEDIA). Der Computerbetrug hat sich in den letzten Jahren verfünffacht.

Die Callcenter-Kriminalität nimmt ebenfalls tendenziell zu. Und KI lässt den Finanzbetrug florieren. Unsichere Produkte stellen eine ständige Gefahrenquelle für Nutzer dar. 2023 und 2024 hat die Bundesnetzagentur jeweils ca. 8.000 Geräte aus dem Verkehr gezogen, weil sie nicht den gesetzlichen Vorgaben entsprachen (heise.online am 6. Februar).

Die größte Herausforderung für die Produktsicherheit bildet aktuell der Onlinehandel. Die BAuA-Fachgruppe „Grundsatzfragen der Produktsicherheit" ist Kontaktstelle im europäischen Schnellwarnsystem Safety Gate. Produktfälschungen fügen den betroffenen Unternehmen einen hohen Schaden zu. Allein Amazon hat nach seinem aktuellen Markenschutzbericht mehr als 7 Millionen gefälschte Produkte auf seinen Onlinemarktplätzen identifiziert. Das Amt der EU für geistiges Eigentum (EUIPO)

hat in einer Studie bekannt gegeben, dass Produktpiraterie in der EU einen Schaden von bis zu 16 Milliarden Euro verursacht und europaweit etwa 200.000 Arbeitsplätze in der Bekleidungs-, Konsumgüter- und Spielzeugindustrie gefährdet (FAZ am 27. März 2024). Den Anteil der Schattenwirtschaft am BIP 2024 schätzt eine Studie des Instituts für angewandte Wirtschaftsforschung der Universität Linz auf 11,3 Prozent, also auf 480 Milliarden Euro. Seit 2021 steigt dieser Wert tendenziell an. Allein zwei Drittel entfallen auf Schwarzarbeit. Ziel eines Gesetzentwurfs des BMF ist es, durch die Auswertung größerer Datenmengen und den Datenaustausch zwischen Sozial-, Finanz- und Sicherheitsbehörden effizient gegen Schwarzarbeit vorzugehen. Die Friseur- und Kosmetikbranche soll in den Katalog von Schwarzarbeit besonders betroffener Branchen aufgenommen werden. Im Hinblick auf den Verdacht auf Schwarzarbeit bei einem Sicherheitsdienstleister bei der Gamescom 2025 erklärte die Vorsitzende der BDSW-Landesgruppe NRW, Nora Rauch, dass gesetzwidriges Verhalten von Sicherheitsunternehmen durch falsche Schwerpunktsetzung bei der Auftragsvergabe und durch mangelnde Kontrollen gefördert werde (Pressemitteilung des BDSW am 26. August 2025).

2024 hat der Zoll 27.000 Strafverfahren und 50.000 Ordnungswidrigkeitsverfahren wegen Unterschreitung des Mindestlohns eingeleitet. Verstärkt gehen die Ermittlungsbehörden und Gerichte auch gegen das Delikt der Geldwäsche vor. So hat das LG Berlin im März 2025 die Einziehung von 58 Immobilien wegen Geldwäscheverdacht angeordnet. Am 15. April teilte EUROPOL mit, dass 232 Tatverdächtige, darunter „hochrangige Zielpersonen", wegen Geldwäscheoperationen festgenommen worden seien. Und Ermittlern des BKA und des Zolls ist es gelungen, den „Krypto-Swappingdienst eXch" vom Netz zu nehmen, der damit geworben hatte, das Geldwäscheverbot nicht einzuhalten. 34 Millionen Euro wurden dabei beschlagnahmt.

Sicherheitsgefühl

Der Sicherheitslage sollte das Sicherheitsgefühl der Bürger entsprechen. Nach einer repräsentativen Erhebung im März 2025 sagten 65 Prozent der Befragten, sie fühlten sich sicher vor Kriminalität, 33 Prozent verneinten die Frage. Frauen sind im Allgemeinen ängstlicher als Männer. Nur 56 Prozent von ihnen fühlten sich sicher. Bei den Männern waren es 74 Prozent. Das Sicherheitsempfinden hängt auch stark vom Bildungsgrad ab: je niedriger der Schulabschluss, umso höher die Kriminalitätsfurcht (DIE ZEIT am 24. April 2025).


Bild: # 1979406539 / istockphoto.com

Die Sicherheitswirtschaft gewinnt an Bedeutung

Die Bundesregierung hat eine „Zeitenwende in der Inneren Sicherheit" mit „gestärkten Sicherheits-, Zivil- und Katastrophenschutzbehörden, zeitgemäßen digitalen Befugnissen, neuen Fähigkeiten und ausreichend Personal" für eine Sicherheitsoffensive angekündigt, die die europa- und verfassungsrechtlichen Spielräume ausschöpft, um ein „Höchstmaß an Sicherheit" zu gewährleisten (im Einzelnen Reinhard Rupprecht in DSD 2 I 2025, Seite 29 ff.). Die Mittel für den Zivil- und Bevölkerungsschutz, für die Nachrichtendienste und den Schutz der IT-Systeme sind von der Schuldenbremse ausgenommen. Das Ausgabenvolumen des BMI steigt nach dem Etat 2025 gegenüber dem Vorjahr um 1,83 Milliarden Euro auf 15,7 Milliarden Euro (Etat des BMI, 21/500, Einzelplan 06). Die Mittelausstattung für das BKA wird um 170 Millionen Euro erhöht. Die Bundespolizei erhält 1.000 neue Stellen und ein um 75 Millionen erhöhtes Ausgabevolumen von fast 5 Milliarden Euro. Diese Offensive wird sich wohl erst 2026 auf die Sicherheitslage auswirken.

Umso wichtiger ist es, dass die Sicherheitswirtschaft mit ihrem hohen technischen und personellen Wirkungspotenzial optimal eingesetzt wird, um die Sicherheitslage 2025 positiv zu beeinflussen. Die Zahl der Mitarbeiter ist 2024 erneut um ca. 2 Prozent angestiegen. Und die Nachfrage nach Fachkräften wird angesichts fortschreitender Digitalisierung und der vielfältigen Herausforderungen im Bereich der öffentlichen wie der privaten Sicherheit weiter steigen.

Die Sicherheitstechnik entwickelt sich als Folge der Digitalisierung, der Nutzung von KI und der innovativen Fähigkeit der Forschungsinstitute ebenso wie der Entwicklungsarbeit der Sicherheitsunternehmen im physischen wie im IT-Bereich immer rasanter.

Diese Leistungsfähigkeit und Innovationskraft können sich aber nur voll entfalten, wenn Staat und Wirtschaft, Sicherheitsbehörden und Sicherheitswirtschaft vertrauensvoll kooperieren. Die Politik muss nicht nur mit Worten, sondern mit Taten anerkennen, dass die Sicherheitswirtschaft eine Säule in der Architektur der Inneren Sicherheit darstellt.

Was der BDSW dazu beitragen kann, um die Politik entsprechend zu beeinflussen, hat Präsident Werner Landstorfer in einem Programm „Sicherheit 2030" mit zehn Impulsen definiert (**sicherheit2030@securitas.de**).

Neuer Ost-West-Konflikt? (Potenzielle) Folgen für deutsche Unternehmen

Von Prof. Dr. Stefan Goertz

Das Handelsblatt titelte Ende Juni 2025 „Der unerklärte Weltkrieg – Warum der globale Kampf zwischen Demokratie und Diktatur immer bedrohlicher wird" und stellte richtigerweise fest, dass ein „unerklärter Weltkrieg begonnen" habe, ein „Meta-Konflikt um Machtzonen und Marktzugänge, um Lieferketten und Technologieführerschaft".[1]

Spätestens seit dem Beginn des russischen Angriffskriegs gegen die Ukraine am 24. Februar 2022, sicherheitspolitisch-*realistisch* betrachtet allerdings auf hybrider Ebene bereits seit der völkerrechtswidrigen Annexion der ukrainischen Krim am 20. Februar 2014, hat ein neuer Ost-West-Konflikt begonnen. Dieser wurde vom System Putin initiiert und wird auf verschiedenen Ebenen und mit hybriden Mitteln ausgetragen, u. a. auf der militärischen (in der Ukraine), auf der wirtschaftlichen und energiewirtschaftlichen Ebene (gegen die Ukraine und die westliche Welt), mit hybriden Mitteln wie Sabotage und Mordkomplotte gegen westliche Kritische Infrastrukturen und Unternehmen. Der russischen Regierung stehen China, der Iran, Nordkorea, Belarus, Kuba, Venezuela und Nicaragua zur Seite (bis zum Sturz des Assad-Regimes auch Syrien).[2] Diese Bündnispartner Russlands stehen in einem Konflikt mit der westlichen Welt, deren Demokratien, Unternehmen und Kritischen Infrastrukturen.

Die deutschen Verfassungsschutzbehörden stellten im Mai 2025 fest, dass die Gefahren durch Spionage, Sabotage und Desinformation mit dem russischen Angriffskrieg auf die Ukraine stark gestiegen und „die Hemmschwelle für Aktionen gegen Deutschland auf russischer Seite gesunken" sei.[3]

Aktuelle Bedrohungslage durch hybride Angriffe

Nach aktuellen Angaben der drei deutschen Nachrichtendienste des Bundes – des Bundesamtes für Verfassungsschutz (BfV), des Bundesnachrichtendienstes (BND) und des Bundesamtes für Militärischen Abschirmdienst (BAMAD) – hat das Niveau der Spionage- und Sabotageaktivitäten gegen Deutschland und andere europäische Staaten dasjenige des Ost-West-Konflikts (bis 1990) zumindest erreicht, wegen der neuen technologischen Möglichkeiten wahrscheinlich bereits überschritten.[4]

Das Bundesministerium des Innern (BMI) stellt seit dem Beginn des Russland-Ukraine-Krieges fest, dass die Hauptakteure der gegen Deutschland und andere europäische Staaten gerichteten Spionage und Sabotage – mit jeweils unterschiedlichen Schwerpunkten und Zielen – Russland und China, aber auch der Iran sind.[5]

Russische Geheimdienste und deren Proxy-Akteure führen seit Jahren, signifikant erhöht seit dem Beginn des Angriffskriegs gegen die Ukraine im Februar 2022, hybride Angriffe gegen Deutschland und andere europäische Staaten aus. „Hybride Angriffe auf uns in Deutschland sind Realität, jeden Tag", erklärt Carsten Breuer, der Generalinspekteur der Bundeswehr aktuell.[6]

Hybride Kriegsführung, hybride Aktionen sind von einer Kombination regulärer und irregulärer politischer, wirtschaftlicher, medialer, geheimdienstlicher, militärischer und cybertechnischer Mittel geprägt. Dadurch verschwimmen die völkerrechtlichen Grenzen von Krieg und Frieden, äußerer und innerer Sicherheit. Ein zentrales Motiv von hybrider Kriegsführung besteht darin, eine völkerrechtliche und politische Zurechnung zu erschweren, damit die Urheberschaft hybrider Aktionen, die eigene Kriegsbeteiligung, zu verschleiern.

Prof. Dr. Stefan Goertz
Hochschule des Bundes, Fachbereich Bundespolizei, Lübeck

Dieser Beitrag stellt die persönliche Auffassung des Autors dar.

[1] Vgl. Handelsblatt (2025): Thema des Tages, 20.–22.6.2025, Nr. 116.

[2] Vgl. Handelsblatt (2025): Thema des Tages, 20.015022.6.2025, Nr. 116, S. 13.

[3] Vgl. Bundesamt für Verfassungsschutz (2025): Gefährdungen durch russische Spionage, Sabotage und Desinformation, S. 6.

[4] Vgl. https://www.tagesschau.de/inland/geheimdienste-russische-sabotage-deutschland-100.html (26.7.2025).

[5] Vgl. Bundesministerium des Innern und für Heimat (2023): Verfassungsschutzbericht 2022, S. 278-288.

[6] https://www.zdfheute.de/politik/deutschland/russland-sabotage-hybride-angriffe-100.html (26.7.2025).

Die Liste aktueller Fälle von (mutmaßlicher) Spionage und Sabotage in Deutschland und anderen europäischen Staaten ist lang: Cyberangriffe auf Parteien und den Bundestag, ein Anschlagsplan auf Armin Papperger, Vorstandsvorsitzender des Rüstungskonzerns Rheinmetall, per Luftpost verschickte Brandsätze (u. a. der Vorfall im DHL-Logistikzentrum in Leipzig im Sommer 2024), Hunderte Drohnenüberflüge zur Spionage und potenziellen Vorbereitung von Sabotageakten über Liegenschaften der Bundeswehr seit dem Beginn des russischen Angriffskriegs gegen die Ukraine, unbefugter Zutritt von mutmaßlich Proxy-Akteuren russischer Geheimdienste in militärischen Liegenschaften der Bundeswehr, die beschädigten Datenkabel in der Ostsee im Winter 2024 und Januar 2025, der BND-Spionagefall für einen russischen Geheimdienst 2022 (Verdacht auf Landesverrat durch Spionage für Russland, der Gerichtsprozess dauert an). Mehrfach waren in den vergangenen Wochen und Monaten Schiffe der Marine (Bundeswehr) Ziel von mutmaßlichen Sabotageaktionen, durchtrennte Kabelbäume, Metallspäne im Antrieb, Öl im Trinkwassersystem.[7]


Bild: # 1459802073 / istockphoto.com

Geopolitische Umbrüche – (potenzielle) Folgen für deutsche Unternehmen

Von „zerstörten Unterseekabeln fast im Monatsrhythmus, Sabotagehandlungen gegen deutsche Kriegsschiffe der Marine in deutschen Werften und auf See gestarteten Drohnen, die über deutschen KRITIS- und Industrieanlagen kreisen", berichtete Vizeadmiral der Marine der Bundeswehr, Jan Kaack, im Frühsommer 2025.

Die geopolitischen und geoökonomischen Umbrüche infolge des russischen Angriffskriegs gegen die Ukraine sowie Chinas offensive Geheimdienstaktivitäten haben neue Bedrohungen kreiert. Daher stehen – spätestens seit 2022 – vermehrt auch deutsche sowie europäische Unternehmen, KRITIS und Forschungseinrichtungen besonders im Fokus von Wirtschafts- und Wissenschaftsspionage, (potenziell) von Sabotage sowie auch strategisch motivierter ausländischer Direktinvestitionen.

Rohstoffe sind in letzter Zeit zur Verhandlungswaffe von Staaten wie China geworden. „Bei seltenen Erden aus China sind wir derzeit fast zu 100 Prozent abhängig", erklärte Stéphane Séjourné, EU-Industriekommissar, im Juni 2025. Der Bundesverband der Deutschen Industrie warnt seit Jahren davor, dass die deutsche Industrie zu sehr von Lieferungen kritischer Rohstoffe wie beispielsweise seltener Erden, aber auch Gallium und Germanium aus China, abhängig sei. Die Märkte für kritische Rohstoffe funktionierten nicht mehr, warnt der BDI. Deutsche Unternehmen stünden „staatlichen Akteuren und autokratischen Regimen gegenüber, gleichzeitig steige die globale Nachfrage nach kritischen Rohstoffen rapide.[8]

Fazit

Der russische Angriffskrieg gegen die Ukraine hat einen neuen Ost-West-Konflikt ausgelöst, in dem sich die westlichen Demokratien und Russland als „Systemrivalen" gegenüberstehen. Dieser neue Ost-West-Konflikt ist auf wirtschaftlicher und energiewirtschaftlicher Ebene auch ein Meta-Konflikt um Machtzonen und Marktzugänge, um Lieferketten und Technologieführerschaft, mit (potenziell) erheblichen Folgen für deutsche und andere europäische Unternehmen.

[7] Vgl. https://www.tagesschau.de/inland/warnung-brandsaetze-pakete-100.html; https://www.br.de/nachrichten/deutschland-welt/ostsee-wieder-datenkabel-beschaedigt,Ub0VOMY; https://www.rnd.de/politik/russische-spionage-und-sabotage-wie-putins-schattenkrieg-deutschland-trifft-UUFE3MEGPBMF5AQL7FN2Q7BNPM.html (26.7.2025).

[8] Vgl. Handelsblatt (2025): Rohstoffe als Verhandlungswaffe, Nr. 116, S. 16-17.

Cyberangriffe über den Wolken

Was passiert, wenn unsere Lieferketten digital wackeln?

Von Marc Jobelius

Verlässliche Sicherheit in der Luft. Und im digitalen Backend?

Die Luftfahrt steht für Präzision, Verlässlichkeit und höchste Sicherheitsstandards. Doch während die äußere Sicherheit von Flugzeugen durch etablierte Kontrollverfahren, Personalqualifikation und physische Schutzmaßnahmen gewährleistet wird, zeigt sich in der Tiefe eine wachsende Angriffsfläche: die digitale Infrastruktur. Die Ereignisse der letzten Monate machen deutlich, dass die zivile Luftfahrt unter digitalem Beschuss steht und zeigen, dass die Verwundbarkeit real ist und zudem wächst.

Aktuelle Vorfälle: ein Blick hinter die Firewall

1. **Angriff auf die Deutsche Flugsicherung (DFS) –** Im August 2024 wurde die Bürokommunikation der DFS durch einen Cyberangriff gestört. Zwar blieb der Flugverkehr stabil, aber der Vorfall zeigt, wie tiefgreifend die Verwundbarkeit auch jenseits operativer Systeme sein kann. Kommunikationsverlust bedeutet auch Reaktionsschwäche.

2. **Airline-Angriffe weltweit –** Mehrere internationale Airlines, darunter Hawaiian, WestJet und Qantas, meldeten Angriffe auf ihre IT-Systeme. In Einzelfällen kam es zu Datenlecks und gestörten Buchungsprozessen. Kundendaten, Flugdaten und operative Prozesse, nichts ist ohne Risiko. Einer dieser gezielten und nachhaltig ausgeführten Angriffe führte im Juli 2025 zum weitgehenden Ausfall der Systeme der größten russischen Airline Aeroflot. Und es sei den Angreifern schlicht leicht gemacht worden, durch veraltete Systeme mit Betriebssystemen Windows Server 2003 und Workstations mit Windows XP sowie zusätzlich geringem Augenmerk auf Passwörter im obersten Management.

3. **GPS-Spoofing über Osteuropa –** Navigationssysteme ziviler und militärischer Flugzeuge meldeten gefälschte Positionsdaten mit potenziell katastrophalen Folgen für Mensch und Maschine. Zudem wurde der Funkverkehr, also die technisch etablierteste Fallback-Ebene, ebenso gestört. Die Quelle solcher Angriffe bleibt oft unklar, ebenso wie die Absicht. Fest steht: Die digitale Navigation wird zur potenziellen Schwachstelle.

4. **Angriff auf Industrieunternehmen –** Im Jahr 2024 wurde ein Batteriehersteller Opfer eines Cyberangriffs, der dazu führte, dass das Unternehmen aus dem SDAX ausgeschlossen wurde. Die Attacke hatte erhebliche Auswirkungen auf die Produktion und den Geschäftsbetrieb.

5. **Angriff auf produzierende Unternehmen und Dienstleister –** Ebenfalls wurden 2024 und 2025 mehrere Hersteller durch Cyberangriffe in den Notbetrieb gezwungen. Die Produktion musste teilweise eingestellt werden, was zu Lieferverzögerungen und in England sogar zu einer Insolvenz eines alteingesessenen Logistikers führte. Und die Telekommunikation eines unserer Nachbarländer wurde kurzzeitig komplett ausgesetzt.

Was steckt dahinter? Ursachen und Muster

Cyberangriffe auf die Luftfahrt, produzierende Industrie und Dienstleister sind selten Zufall. Sie folgen einer Logik und oft einer nachhaltigen Strategie:

- **Veraltete Systeme:** Viele Unternehmen setzen auf veraltete IT-Infrastruktur, oft aus Kostengründen. Sicherheits-Updates bleiben aus, Support läuft aus, Schnittstellen sind offen.

- **Fehlende Awareness:** Cybersicherheit wird zu häufig als IT-Thema verstanden und nicht als Führungs- und Risikomanagementaufgabe. Sicherheitskultur fehlt, weil sie nicht eingefordert wird.

- **Geopolitische Interessen:** Gruppen wie APT28 (auch bekannt als Fancy Bear) agieren nach aktuellen Kenntnissen im staatlichen Auftrag. Ihre Ziele sind Störung, Ausspähung, Druckaufbau gegen Kritische Infrastrukturen.

Marc Jobelius

Geschäftsführender Gesellschafter des Beratungsunternehmens Bouché Air & Sea GmbH, Vorstand im Bundesverband für Luftsicherheit e. V. FASAG, LBA-zugelassener Ausbilder für Sicherheitspersonal

Die stille Achillesferse: Luftfracht

Während Passagierflüge oft im medialen Fokus stehen, ist die Luftfracht in besonderem Maße bedroht:

- Eng getaktete Lieferketten vertragen keine Downtime. Wenn Systeme ausfallen, stehen Warenflüsse mit Folgen für Industrie, Handel und Patientenversorgung.

- Digitale Zoll- und Trackingprozesse basieren auf Integrität. Bei einem Angriff wird nicht nur die Verfügbarkeit gestört, sondern auch die Vertrauenswürdigkeit der Daten infrage gestellt.

- Die Expresslogistik erhöht die Schlagzahl und damit auch die Angriffsfläche. Je schneller ein Prozess ist, desto weniger Fehlertoleranz ist vorhanden, auch im Cyberraum.

Besonders alarmierend ist die Möglichkeit, mittels Cyberangriffen auf produzierende Unternehmen, Sendungen und Zugänge zu manipulieren. Dies bedeutet, dass beispielsweise Sprengstoffe unbemerkt einer Sendung hinzugefügt werden könnten; man spricht von klassischer Manipulation. Wenn wiederum ein reglementierter Beauftragter (Luftfrachtspediteur) Opfer einer Korruption wird, können die Sicherheitsstatus der Sendungen arglistig verändert werden, sodass mit Sprengsätzen versehene Sendungen nicht mehr einer physischen Kontrolle wie beispielsweise Röntgen zugeführt werden. Diese Vorfälle zeigen, dass Cyberangriffe nicht nur die Produktion, den Vertrieb und den Versand beeinträchtigen können, sondern auch eine direkte Gefahr für die Menschen darstellen.

Regulatorische Entwicklungen: neue Anforderungen an die Branche

Die Europäische Union hat mit der Durchführungsverordnung (EU) 2019/1583 neue Maßnahmen in der Luftfrachtsicherheit verankert, um Schutz vor Cyberkriminalität in der gesamten sicheren Lieferkette aufzubauen. Das Luftfahrt-Bundesamt (LBA) hat auf seiner Website die neuen Richtlinien zur Anwendung von Cybersicherheitsmaßnahmen mit Verweis auf das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht. Diese Richtlinien sind gültig, von den Beteiligten der sicheren Lieferkette seit 1. Januar 2025 anzuwenden, und das LBA auditiert bereits die Umsetzung in der Fläche.

Handlungspflicht: Cybersicherheit ist keine Option

Die Frage ist nicht, ob etwas passiert. Sie lautet: wann. In einer Branche, die auf internationale Vernetzung, Echtzeitdaten und voll automatisierte Abläufe angewiesen ist, wird Cybersicherheit zur Grundvoraussetzung und nicht nur zur Kür.
Was jetzt notwendig ist:

1. Implementierung von Informationssicherheits-Managementsystemen (ISMS) für Kritische Infrastrukturen: Einführung und Pflege von ISMS nach etablierten Standards, um systematisch Informationssicherheitsrisiken zu identifizieren und folglich steuern zu können.

2. Mitarbeitersensibilisierung und Schulungen: Der Mensch bleibt das größte Risiko. Regelmäßige Schulungen für alle Mitarbeitenden sind verpflichtend durchzuführen, insbesondere für diejenigen mit Zugriff auf kritische IT-Systeme, um das Bewusstsein für Cyberrisiken zu schärfen. Es ist ganz einfach, sicherheitsbewusstes Verhalten muss gefördert und verlangt werden.

3. Regulatorische Anforderungen umsetzen: Erfüllung der Vorgaben gemäß der DVO (EU) 2019/1583, einschließlich der Erstellung eines Cybersicherheitsprogramms als Bestandteil des Luftsicherheitsprogramms.

4. Etablierung von Notfall- und Wiederherstellungsplänen: Entwicklung und regelmäßige Aktualisierung von Business Continuity- und Recovery-Plänen, um im Falle eines Cyberangriffs schnell reagieren und den Betrieb wiederherstellen zu können.

5. Technische Sicherheitsmaßnahmen: Einsatz von Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), regelmäßige Sicherheits-Updates und Patches sowie Verschlüsselung sensibler Daten.

6. Ausführung des CyberRisikoCheck nach DIN SPEC 27076 des BSI für kleine und mittelständische Unternehmen.

7. Regelmäßige Audits und Tests: Durchführung von Penetrationstests und Sicherheitsüberprüfungen, um Schwachstellen zu identifizieren und zu beheben.

8. Einführung einer lebenden Sicherheitskultur: Förderung einer Unternehmenskultur, in der Cybersicherheit als gemeinsame Verantwortung verstanden und kontinuierlich gelebt wird.

Ein gewagter Vorschlag: Bestehende Systeme nutzen und verfeinern

Ein Umdenken bei der regulatorischen Vorgabe ist eine effektive Möglichkeit. Den nationalen Luftsicherheitsbehörden wird durch die europäischen Verordnungen ein Ermessens- und Umsetzungsspielraum gewährt. Warum wehren sich das Bundesministerium für Verkehr und das LBA gegen die Anerkennung von etablierten Zertifizierungen wie bspw. die ISO 27001? Diese Option ist im Mustercyberprogramm des LBA nicht vorgesehen. Die Abwehr eines Cyberangriffs ist entscheidend, egal ob das Ziel eine Luftfrachtsendung oder die Produktion sind. Der Schutz der Systeme ist vorrangig und durch Zertifikate von unabhängigen Akkreditierungsstellen nachzuweisen. Aktuell werden zu oft für das LBA Parallelsysteme aufgebaut. Wäre es da nicht zielführend, diese Standardisierung zu akzeptieren und um Identifikation von Systemen und Daten, die für die Luftsicherheit kritisch sind, zu ergänzen?

Ausblick: Luftsicherheit 2030 nur mit digitalem Fundament

Die Gefahr sitzt nicht mehr nur am Gate oder der Frachtannahme. Cybersicherheit ist mehr als Technik. Sie ist eine Frage der Verantwortung für Passagiere, für Frachtkunden, für die Gesellschaft. Luftfahrtunternehmen, Logistiker, Dienstleister und Behörden teilen dieselbe Internetinfrastruktur. Und damit auch dieselbe Verantwortung. Und dieses digitale Backend gilt es zu schützen. Jetzt.

AWiAS Aviation Days 2025 – Fachforum für zivile Luftsicherheit in Hamburg

Von Sandra Weber

Sandra Weber

zum Zeitpunkt der Veranstaltung Schülerpraktikantin des BDLS Bundesverbandes der Luftsicherheitsunternehmen

Am 17. und 18. Juni 2025 traf sich die Luftsicherheitsbranche zu den AWiAS Aviation Days im Steigenberger Hotel Treudelberg in Hamburg. Die zweitägige Fachveranstaltung bot ein dichtes Programm mit hochkarätigen Referenten und spannenden Themen aus der zivilen Luftsicherheit. Im Mittelpunkt standen die sichere Lieferkette, Luftsicherheit, Cybersecurity sowie Zukunftsperspektiven im Aviation-Bereich. Ergänzt wurde das Programm durch praxisnahe Demonstrationen, zahlreiche Gelegenheiten zum Netzwerken und die entspannte Atmosphäre des Golfresorts – eine Kombination, die die besondere Handschrift der AWiAS Aviation Days ausmacht.

Ein besonderes Erlebnis bot in diesem Jahr auch Skillcamp, die sich bei den AWiAS Aviation Days mit ihren VR-Brillen präsentierten. Jeder Gast konnte diese innovative Technik selbst ausprobieren und hautnah erleben, wie moderne Virtual-Reality-Anwendungen die Ausbildung und Trainingsmethoden in der Luftsicherheit bereichern können.

Tag 1 – Behörden, Verbände & Innovation

Nach der Eröffnung durch Annette Wiedemann, Geschäftsführerin der AWiAS Aviation Services GmbH, die es sich auch in diesem Jahr nicht nehmen ließ, moderierend durch die gesamten AWiAS Aviation Days zu führen, machte Dr. Jürgen Vogt deutlich, wie sehr sich die Rolle von Verbänden verändert hat. Vom früher eher belächelten „Zusatz" sind sie heute zu aktiven Mitgestaltern geworden, die bei der Entwicklung neuer Vorschriften entscheidend mitwirken.

Axel Tuengerthal (Atotech Deutschland GmbH) gab einen anschaulichen Einblick in den Alltag eines „bekannten Versenders". Seit 2021 hätten die Sicherheitsauflagen massiv zugenommen – von baulichen Maßnahmen wie Fenstergittern über spezielle Arbeitskleidung bis hin zu Manipulationsschutz und verpflichtender Videoüberwachung. Für kleinere Unternehmen sei dies eine große wirtschaftliche Belastung, die in manchen Fällen sogar dazu führe, Fracht über ausländische Flughäfen abzuwickeln. Dabei stellte er auch internationale Unterschiede heraus: „Deutschland ist im Vergleich zu anderen europäischen Staaten überreguliert."

Bilder: AWiAS

Dr. Peter A. Meincke (DLR) präsentierte unter dem Titel „Flughäfen neu denken" zwei Innovationspfade für eine klimaneutrale Luftfahrt:

- EXACT – wasserstoffbetriebene Flugzeuge mit bis zu 100 % CO_2-Einsparung
- THOR – Effizienzsteigerung und Nutzeroptimierung, etwa durch gestaffeltes Boarding

Besonders eindrucksvoll waren seine Berechnungen zum Energiebedarf: Ab 2040 wird der tägliche Wasserstoffbedarf großer Flughäfen bei über 33 Tonnen liegen, bis 2050 sogar bei

mehr als 340 Tonnen. Diese Zahlen verdeutlichten, wie stark sich künftig Treibstofflogistik, Flächenbedarf und Infrastruktur verändern müssen.

Prof. Dr. Stefan Goertz nutzte aktuelle Zahlen, Daten und Fakten, um die allgegenwärtige Bedrohungslage zu verdeutlichen. Sein Fokus lag auf dem Innentäter – einer Gefahr, die aus Unzufriedenheit, ideologischer Radikalisierung oder krimineller Motivation entstehen kann. Er sensibilisierte die Anwesenden bei den AWiAS Aviation Days dafür, dass Unternehmen dieses Risiko ernst nehmen und interne Strukturen regelmäßig prüfen müssen.

Tag 2 – Cybersecurity & Praxiswissen

Der zweite Tag der AWiAS Aviation Days begann mit Anna Thurm, Referatsleiterin für „Sichere Lieferkette" beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Durch ihre Praxiserfahrung konnte sie sich besonders gut in die Herausforderungen der Unternehmen einfühlen. Ihre Botschaft war klar:

1. Jeder wird angegriffen.

2. Die Frage ist nicht, ob, sondern wann.

APT-Gruppen und Schadenssummen von 179 Millionen Euro im Jahr 2024 zeigen die Brisanz. Unternehmen seien verpflichtet, sich strategisch mit Cybersecurity zu befassen – nicht zuletzt, weil ein erfolgreicher Angriff gravierende wirtschaftliche und operative Folgen haben kann.

Philipp Köllner (AF Logistik & Speditions GmbH) sprach über den Umgang mit Behördenkontrollen, insbesondere durch das Luftfahrt-Bundesamt (LBA). Auch bei unangekündigten, teils nächtlichen Inspektionen gelte: Ruhe bewahren, Anweisungen befolgen, strukturiert reagieren. So ließen sich Konflikte vermeiden und Prozesse beschleunigen.

Christian Schneider, UN-Berater und Vertreter der Initiative Breitscheidplatz, verdeutlichte, warum fachplanerischer Zufahrtsschutz so wichtig ist. Angriffe mit Fahrzeugen seien „einfach, billig, effektiv" – und erfordern kein spezielles Know-how, um verheerend zu wirken. Für wirksamen Schutz müsse man mit qualifizierten Unternehmen wie ihm zusammenarbeiten. Der Schutz

von Flächen, Gebäuden und Zufahrten habe heute eine sicherheitsrelevante Bedeutung, die in der Planung oft unterschätzt wird.

Dr. Stefan Richter (Bundespolizei Berlin) fesselte das Publikum bei den AWiAS Aviation Days mit dem Thema „Super Recogniser". Nur ein bis zwei Prozent der Bevölkerung verfügen über diese besondere Fähigkeit, Gesichter auch unter schwierigsten Bedingungen wiederzuerkennen. Mit anschaulichen Beispielen zeigte er, wie diese Spezialisten arbeiten – präzise, fokussiert und mit einer beeindruckenden Trefferquote. Viele Teilnehmer fragten sich danach, ob sie selbst zu dieser seltenen Gruppe gehören könnten.

Nina Naske, Rechtsanwältin, spezialisiert auf Luftrecht und Luftsicherheit, beendete das Vortragsprogramm der AWiAS Aviation Days mit einer juristischen Analyse des Verhältnisses zu Behörden. Sie zeigte, wie Unternehmen ihre Rechte wahren, Entscheidungen anfechten und gleichzeitig durch partnerschaftlichen Dialog tragfähige Lösungen erzielen können – ein Balanceakt zwischen rechtlicher Klarheit und konstruktiver Zusammenarbeit.

Fazit

Die AWiAS Aviation Days 2025 boten nicht nur fundierte Fachvorträge und praxisnahe Impulse, sondern auch eine Atmosphäre, die den Austausch auf Augenhöhe fördert. Besonders bemerkenswert: Es kam zu keiner „Gruppenbildung" unter den Teilnehmern – stattdessen mischten sich die Fachleute aus unterschiedlichsten Bereichen frei und offen.

Ein Highlight war der stimmungsvolle BBQ-Abend. Inmitten der gepflegten Golfplatzkulisse mischten sich beim Duft von frisch Gegrilltem Fachgespräche mit humorvollen Anekdoten, neue Kontakte wurden geknüpft und bestehende vertieft. Dieses Zusammenspiel von Know-how, Wissensvermittlung für den Alltag und gezielten Auflockerungen macht die AWiAS Aviation Days zu einem besonderen Erlebnis. Genau so werden sie geplant – als Plattform, die Fachthemen nicht nur vermittelt, sondern erlebbar macht, und dabei den professionellen Austausch mit einem Schuss Humor und Herzlichkeit verbindet.

Bargeld in der Zukunft

Im Gespräch mit Michael Leppler

Erinnern Sie sich an den kürzlichen Stromausfall in Spanien und Portugal? Plötzlich haben digitale Zahlungen nicht mehr funktioniert, sämtliche Geldautomaten sowie POS-Terminals waren außer Gefecht gesetzt und viele Geschäfte gezwungen, auf Barzahlungen umzusteigen. Die Bargeldnachfrage stieg sprunghaft an, doch die Geldautomaten waren schnell leer und konnten nicht wieder aufgefüllt werden. Weder Online-Banking noch mobile Bezahl-Apps konnten genutzt werden, sodass digitale Überweisungen unmöglich waren. GIT SICHERHEIT sprach mit Michael Leppler, dem Head of Sales und Marketing von Prosegur Cash Services Germany, über die gesellschaftliche Bedeutung, eine Vielzahl von Zahlungsoptionen sicherzustellen, und Prosegurs weltweite Rolle bei der Sicherung physischer und digitaler Werte.

Michael Leppler

Head of Sales und Marketing von Prosegur Cash Services Germany

Die Erstveröffentlichung des Interviews erfolgte in der Ausgabe 6/2025 der Zeitschrift GIT SICHERHEIT.

www.git-sicherheit.de

Wir bedanken uns für die Abdruckgenehmigung.

Herr Leppler, als Head of Sales & Marketing von Prosegur Germany tragen Sie eine umfangreiche Verantwortung. Könnten Sie kurz Ihren beruflichen Hintergrund und Ihre aktuelle Rolle bei Prosegur erläutern?

Michael Leppler: Als gelernter Speditionskaufmann bin ich seit mittlerweile 16 Jahren in leitender Funktion bei Prosegur an Bord. In dieser habe ich den Markteintritt des Unternehmens in Deutschland im Jahr 2011, die Integration weiterer Geld- und Wertdienstleister und die damit verbundene Marktkonsolidierung begleitet.

Prosegur ist weltweit als einer der marktführenden Sicherheitsdienstleister bekannt. Welche Dienstleistungen bietet Prosegur global an und wie bedienen Sie den deutschen Markt?

Michael Leppler: Prosegur ist in 36 Ländern auf fünf Kontinenten mit sechs unterschiedlichen Geschäftsbereichen aktiv. Der Geschäftsbereich Prosegur Security etwa bietet Lösungen rund um Sicherheitstechnik und Guarding an. Die Kolleginnen und Kollegen aus der Sparte Cipher erbringen Dienstleistungen aus dem Cybersecurity-Umfeld, um nur ein paar Beispiele zu nennen. In Deutschland ist Prosegur mit dem Geschäftsbereich Cash aktiv. Wir bieten hierzulande Lösungen für alle Bereiche, in denen Bargeld und andere physische oder digitale Werte im Umlauf sind. Das umfasst die Abholung von Bargeldeinnahmen bei unseren Handelskunden, die anschließende Gutschrift auf dem Bankkonto sowie die Belieferung mit frischem Wechselgeld. Für Bankkunden befüllen wir Geldautomaten und sorgen dafür, dass SB-Geräte störungsfrei funktionieren. Mit 55 Prozent Marktanteil sind wir hiesiger Marktführer und betreiben als einziger Anbieter ein deutschlandweites Standort-Netzwerk. Wir decken das gesamte Bundesgebiet aus eigener Kraft ab, ohne den Einsatz von Subunternehmen. Insofern ist Prosegur maßgeblich dafür verantwortlich, den Zugang der deutschen Bevölkerung zu Bargeld und die Liquidität von Unternehmen zu gewährleisten. Diese Verantwortung nehmen wir sehr ernst.

Das Kerngeschäft von Prosegur Germany besteht im CIT (Cash In Transit) und einer umfassenden Verwaltung der damit verbundenen Abläufe. Der physische Geldtransport ist ein zentraler Teil davon und mit gewissen Risiken verbunden. Welche Rolle spielt Sicherheit dabei und mit welchen Maßnahmen und Produkten sorgen Sie für eine gesicherte Prozesskette?

Michael Leppler: Wo Bargeld transportiert wird, ist Risiko im Spiel. Daher sollte kein Unternehmen mit Bargeldaufkommen die eigenen Mitarbeiter selbst zur Bank schicken. Dies gebietet die gesetzliche Fürsorgepflicht, die jeder Arbeitgeber für seine Mitarbeitenden hat. Auf Geldtransport spezialisierte Unternehmen wie Prosegur minimieren durch einen Mix aus Maßnahmen und standardisierten Prozessen Risiken und erhöhen die Sicherheit für alle. Die Branche hat sich mit den Sicherheitsvorschriften der Bundesvereinigung Deutscher Geld- und Wertdienste und der DIN 77210 selbst strenge Regeln gegeben. Diese beginnen beim Recruiting: Alle Mitarbeiter im Geldtransport müssen über einen einwandfreien Leumund verfügen und gemäß § 34a GewO im Bewachungsgewerbe unterrich-

Kundengelder werden im hochgesicherten Cash Center verwahrt und aufbereitet.

tet sein. Ein Geldtransport findet immer mit mindestens zwei bewaffneten Mitarbeitern im gepanzerten und GPS-überwachten Geldtransporter statt. Für den Fußweg zwischen Fahrzeug und Kundenunternehmen werden Transportsicherungsgeräte verwendet. Die Sicherheitsvorkehrungen enden selbstverständlich nicht mit dem Transport. Auch in den Cash Centern, wo das abgeholte bzw. auszuliefernde Bargeld verwaltet und bearbeitet wird, sind strenge Maßnahmen einzuhalten. Sie reichen von baulichen Anforderungen des Gebäudes bis hin zu lückenloser Videoüberwachung.

Die deutsche Wirtschaft hat in den vergangenen fünf Jahren bedeutende Veränderungen durchlaufen, insbesondere durch die Pandemie und die verstärkte Investition in digitale Technologien. Welche Herausforderungen haben Sie in dieser Zeit erlebt und zu welchen Produktoptimierungen haben diese geführt?

Michael Leppler: Wie die gesamte Gesellschaft befand sich auch Prosegur während der Pandemie im Ausnahmezustand. Zwar waren wir als Teil der Kritischen Infrastruktur selbst nicht von behördlichen Schließungsanordnungen betroffen, wohl aber eine Vielzahl unserer Kunden. Der damit verbundene Auftragseinbruch war beispiellos. Außerdem ist der Prozess des Geldtransports eng zwischen uns Partnern abgestimmt. Kann eine Geldabholung, wie in der Pandemie gesehen, nicht erfolgen, drohen Liquiditätsengpässe aufseiten des Auftraggebers, weil Bargeld nicht zu Buchgeld umgewandelt wird. Vielen Unternehmen wurde in der Pandemie bewusst, dass sie ihre Geschäftsmodelle und -prozesse resilienter gestalten müssen. Digitalisierung ist hier ein wichtiger Faktor. Selbst ein so haptisches Tool wie Bargeld kann digitalisiert werden. Nicht erst seit der Pandemie bieten wir unseren Kunden unter dem Namen Cash Today intelligente Einzahlgeräte für ihr Bargeld an. Neben zahlreichen Vorteilen für das interne Bargeldhandling, wie dem Wegfall von manuellem Geldzählen, bringt ein smarter Safe mehr Resilienz im Vergleich zu einem herkömmlichen Tresor: Bareinnahmen sind nicht nur vor Diebstahl und Überfall bestens ver- und gesichert,

sondern können durch ihre digitale Anbindung per vorzeitiger Wertstellung bereits dem Bankkonto gutgeschrieben werden, selbst wenn das Bargeld noch nicht abgeholt wurde.

Die digitale Transformation von Geschäftsmodellen ist aktuell für sämtliche Unternehmen ein prioritärer Punkt auf der Agenda. Die Deutsche Bundesbank hat passend zu diesem Diskurs im vergangenen Jahr eine Studie zur Zukunft des Bargeldes veröffentlicht. Welche Bedeutung hat die Nutzung von Bargeld in unserer Gesellschaft mit Blick auf die Zukunft?

Michael Leppler: Bargeld ist und bleibt ein wichtiger Bestandteil im Mix der Zahlungsmittel, davon bin ich überzeugt. Jedes Zahlungsmittel hat seine Berechtigung, sei es für die einzelne Person oder auch nur für die einzelne Situation. Bei Prosegur setzen wir uns dafür ein, dass die Wahlfreiheit zwischen den Zahlungsmitteln erhalten bleibt, da sie ein Ausdruck der persönlichen Freiheit eines jeden Bürgers ist. Daher arbeiten wir als Unternehmen unaufhörlich daran, das Produkt Bargeld, das für unsere Kunden nicht Kerngeschäft ist, so attraktiv wie möglich zu gestalten. Wir als Gesellschaft müssen in diesem Zusammenhang aufpassen, eine effiziente Bargeldinfrastruktur zu erhalten. Als Verbraucher nehmen wir Einfluss, indem wir es nicht akzeptieren, sollte uns das Bezahlen mit Bargeld verweigert werden. Denn Bargeld ist das einzige gesetzliche Zahlungsmittel.

Bankinstitute streben tendenziell eine bargeldlose Wirtschaft an. In welchen Bereichen spielt gerade Münzgeld noch eine wichtige Rolle?

Michael Leppler: In der Tat ist für Kreditinstitute Bargeld, insbesondere Münzgeld, nicht mehr im Fokus. Zu diesem Umfeld kommen Vorstöße wie die Abschaffung von Ein- und Zwei-Cent-Münzen seitens des von der Bundesbank gegründeten Nationalen Bargeldforums. Bei Barzahlungen soll in der Folge auf den nächsten Fünf-Cent-Betrag auf- oder abgerundet werden, wie es in den Niederlanden oder Finnland bereits praktiziert wird. Darüber kann man diskutieren. Fakt ist: Nach wie vor sind große Mengen Münzen im Umlauf, die gerade als Wechselgeld gebraucht werden. Allein Prosegur liefert in Deutschland jährlich grob 5,3 Milliarden Münzen an seine Kunden aus. Das entspricht einem Gewicht von 25.000 Tonnen. Den Rückzug von Banken aus der Münzgeldthematik kann Prosegur abfedern.

Mithilfe eines intelligenten Einzahlgerätes Cash Today wird Bargeld digitalisiert und das hauseigene Cash Management automatisiert.

Mit welchen Projekten gestalten Sie bei Prosegur die Transaktionswelt der Zukunft?

Michael Leppler: Ein Fokus liegt auf den zuvor beschriebenen intelligenten und digital angebundenen Geräten Cash Today. Diese stehen in zwei Varianten zur Verfügung: als smarter Tresor zum sicheren Verwahren von Bargeldeinnahmen und als Bezahlautomat für Bargeld am Point of Sale. An solch einem Gerät kann die Kundschaft selbst mit Bargeld bezahlen, ohne dass das Kassenpersonal damit in Berührung kommt. Insbesondere diese Variante wollen wir weiter ausbauen und um unbare Zahlverfahren erweitern. Unser Ziel ist, eine 360°-Payment-Lösungen darzustellen. Daneben arbeitet Prosegur bereits an einem Krypto-Geschäftsbereich, der eine ganzheitliche Lösung für die Verwahrung und Verwaltung digitaler Vermögenswerte darstellen wird. Außerdem wird künstliche Intelligenz eine immer wichtigere Rolle in unseren Geschäftsprozessen erhalten. Als Marktführer haben wir den Anspruch, den Markt aktiv zu gestalten.

Bargeld im Visier – doch die eigentliche Gefahr ist Geldwäsche im digitalen Raum

Neue EU-Regeln zur Bargeldbeschränkung treffen ehrliche Bürger und kriminalisieren die Bargeldnutzung, während die Geldwäsche zunehmend digital erfolgt. Mit der Einführung neuer europaweiter Bargeldobergrenzen ab 2027 soll die Geldwäschebekämpfung verstärkt werden – doch der Fokus auf Bargeld greift viel zu kurz. „Während legale Barzahler reglementiert und kontrolliert werden, blüht die organisierte Finanzkriminalität längst im digitalen Raum", so der BDGW-Vorsitzende Michael Mewes. Der aktuelle Dark Economy Report von BioCatch liefert alarmierende Erkenntnisse: Geldwäsche findet heute in einem Ausmaß und mit einer Raffinesse im Internet statt, die durch neue Barzahlungsgrenzen in keiner Weise eingedämmt werden kann.

Ein überholter Ansatz in einer neuen Realität – mit dem neuen EU-Geldwäschepaket soll der anonyme Erwerb teurer Güter mit Bargeld erschwert werden – durch Ausweispflicht ab 3.000 Euro und ein Verbot von Barzahlungen über 10.000 Euro ab Juli 2027. Doch diese Maßnahmen treffen in erster Linie Handwerker, Gebrauchtwagenkäufer und Privatleute – also Menschen, die ihr Bargeld legal und transparent verwenden. Dagegen ignorieren die EU-Regelungen weitgehend die massiv gestiegenen Risiken im digitalen Raum.

Der Dark Economy Report[1] zeigt deutlich:

- 78 Prozent der Fachleute sehen künstliche Intelligenz als Katalysator für neue, komplexe Betrugsmuster.
- 76 Prozent benennen soziale Medien wie Telegram oder Whatsapp als Eintrittspforte für kriminelle Netzwerke.
- 73 Prozent bestätigen die Rolle des Dark Webs als Umschlagplatz für gestohlene Daten und illegale Finanztransaktionen.

Diese modernen Methoden ermöglichen Geldwäsche in Echtzeit – über digitale Wallets, Kryptowährungen, Fake-Identitäten und eine Vielzahl internationaler Konten.

Finanzkriminalität ist kein Bargeldproblem: Der BioCatch-Bericht belegt: Weltweit wurden allein 2023 rund 3,1 Billionen US-Dollar an illegalem Geld durch das Finanzsystem geschleust – kaum ein Anteil davon in bar. In nur einem Jahr entdeckten Finanzinstitute über 500.000 verdächtige Konten, die ausschließlich dem Zweck der Geldwäsche dienten. Geldwäsche ist heute ein digital vernetztes, global agierendes Geschäftsmodell – weit entfernt von der klassischen Bargeldübergabe.

Regulierung auf dem Rücken der Falschen – viele Branchen, vom Handwerk über den Automobilhandel bis zum Edelmetallhandel, kritisieren die neuen Bargeldbeschränkungen als praxisfremd und kontraproduktiv. Sie sorgen sich nicht nur um die Abwicklung alltäglicher Geschäfte, sondern auch um einen Generalverdacht gegenüber Bargeldnutzern und eine zunehmende Einschränkung finanzieller Freiheitsrechte. Sie stigmatisieren damit ohne empirische Untersuchungen auf unseriöse Art und Weise Bargeldnutzer als latent Kriminelle.

Statt immer neue Hürden für Bargeldnutzer zu schaffen, braucht es intelligente, technologische Lösungen zur Erkennung digitaler Geldwäsche-Netzwerke, grenzüberschreitende Kooperation von Finanzaufsicht, Strafverfolgung und Technologieunternehmen und Investitionen in moderne AML-Systeme, die Verhalten und Muster erkennen – nicht nur Transaktionssummen zählen.

„Wer heute noch glaubt, die Bekämpfung der Geldwäsche durch die Einschränkung von Bargeldkäufen sei effektiv, verkennt die Realität. Finanzkriminalität ist ein digitales Phänomen – sie ist unsichtbar, schnell, global und technisch hochgerüstet. Nur wer hier ansetzt, schützt das Finanzsystem wirklich", so Mewes abschließend.

[1] https://www.biocatch.com/hubfs/Dark_Economy_Research_Report_2025.pdf

Cannabis am Arbeitsplatz – neue Herausforderungen für die Sicherheit

Wie Unternehmen mit den Auswirkungen der Cannabislegalisierung umgehen müssen

Im Gespräch mit Dr. Juliane Falkenberg

Die Sicherheit am Arbeitsplatz ist ein zentrales Anliegen der Berufsgenossenschaft Rohstoffe und chemische Industrie (BG RCI). Mit der Legalisierung von Cannabis und den fortlaufenden Herausforderungen durch Alkoholmissbrauch am Arbeitsplatz stehen Unternehmen vor neuen Fragen und Anforderungen. Dr. Juliane Falkenberg, Referentin der Präventionsabteilung Gesundheit-Medizin-Psychologie bei der BG RCI, bringt ihre Expertise als Arbeitsmedizinerin und Onkologin ein, um Unternehmen bei der Prävention und dem Umgang mit Suchtmitteln und Krebs erzeugenden Gefahrstoffen zu unterstützen. In unserem Interview erläutert sie die Unterschiede in der Handhabung von Alkohol und Cannabis, die Bedeutung präventiver Maßnahmen und die rechtlichen Rahmenbedingungen, die Unternehmen beachten müssen, um die Sicherheit und Gesundheit ihrer Mitarbeiter zu gewährleisten.

Frau Dr. Falkenberg, seit dem 1. April 2024 sind der Konsum sowie der private Eigenanbau von Cannabis zum Eigenverbrauch unter bestimmten Bedingungen für Erwachsene legalisiert. Damit kommt neben Alkohol eine weitere Droge hinzu, deren Konsum eine Gefährdung am Arbeitsplatz bedeuten kann. Welche spezifischen Herausforderungen sehen Sie durch die Legalisierung von Cannabis für die Sicherheit am Arbeitsplatz?

Dr. Juliane Falkenberg: Zum um einen ist die Reaktion auf THC (Tetrahydrocannabinol), dem psychotropen Wirkstoff der Cannabispflanze, sehr individuell und hängt von vielen Faktoren wie der persönlichen Empfindlichkeit, Stimmungslage, Gesundheitszustand, Vorerfahrungen, der Konsumart, dem THC-Gehalt, der Konsumhäufigkeit sowie Misch- und Beikonsum ab. Zum anderen besteht kein linearer Abbau wie bei Alkohol. Nach dem Konsum von Alkoholika kann der erwartete stündliche Rückgang des Blutalkoholspiegels relativ verlässlich errechnet und der Beginn einer Tätigkeit mit einer Punktnüchternheit geplant werden. Dagegen findet nach dem Konsum von Cannabis im Rahmen der individuellen Verstoffwechselung eine starke Umverteilung im Körper sowie eine Wiederaufnahme in den Kreislauf statt.

Somit sind valide Berechnungen zum persönlichen TBC-Abbau derzeit nicht verlässlich möglich, auch wenn dies viele TBC-Rechner im Internet suggerieren. Entsprechend gibt es gegenwärtig keinen eindeutig wissenschaftlich belegten zeitlichen Mindestabstand zwischen Konsum und Dienstbeginn, ab dem eine Beeinträchtigung der Arbeitsleistung gänzlich ausgeschlossen werden kann. Auch der Grenzwert des § 24a Straßenverkehrsgesetz (StVG) gibt dies nicht her. Es liegen aktuell keine THC-Grenzwerte oder Empfehlungen für eine sichere Arbeitsfähigkeit von Personen vor. Aufgrund dessen wird für die Arbeitssicherheit von den Berufsgenossenschaften und Unfallkassen, wie bei Alkohol auch, eine Null-Toleranz-Politik gefordert.

Für den Arbeitsschutz spielen aber nicht nur die akute berauschende Wirkung, sondern auch die langfristige Auswirkung eine Rolle. Bei drogenbedingten Verhaltensänderungen, z. B. in Form einer zunehmenden Gleichgültigkeit, kann es zu Desinteresse und Ignoranz von Sicherheitsmaßnahmen kommen. Es könnten noch einige verhaltens- und kognitivbedingte Beispiele aufgeführt werden, die im Verlauf zu einem erhöhten Risiko für die Arbeitssicherheit führen können. Das heißt, Unternehmen müssen auch diese Anzeichen im Blick behalten.

Welche Wirkung hat der Konsum von Cannabis auf den menschlichen Organismus?

Dr. Juliane Falkenberg: Wie bereits erwähnt, ist die Reaktion abhängig von vielen Faktoren, und

Dr. Juliane Falkenberg

Referentin der Präventionsabteilung Gesundheit-Medizin-Psychologie bei der BG RCI

www.bgrci.de

Die Erstveröffentlichung des Beitrags erfolgte in den Ausgaben 3/2025 und 5/2025 der Zeitschrift GIT SICHERHEIT.

www.git-sicherheit.de

Wir bedanken uns für die Abdruckgenehmigung.

Weitere Informationen erhalten Sie in der k&b-Broschüre „Cannabis“.

es treten nicht nur die erhofften Wirkungen im gewünschten Rahmen und in der beabsichtigten Intensität auf. Cannabis kann sowohl sedierend als auch euphorisierend wirken. Der Konsum von Cannabis wirkt sich nicht nur akut aus, sondern kann auch für dauerhafte Schädigungen sorgen. Je regelmäßiger und intensiver der Cannabiskonsum, desto eher können sich körperliche und psychische Störungen entwickeln.

Bild: # 1224410530 / istockphoto.com

Zu den möglichen akuten körperlichen Nebenwirkungen bei Cannabiskonsum zählen beispielsweise Veränderungen von Blutdruck und Sehvermögen, Schwindel, Lichtempfindlichkeit, gerötete Augen, verwaschene Sprache, ein trockener Mund, gesteigerter Appetit, Müdigkeit und Herzrasen. Außerdem kann es zu einer Intensivierung der Sinneseindrücke, zu Verzerrung der optischen und akustischen Wahrnehmung bis hin zu Halluzinationen und zu einer Veränderung des Zeit- und Raumgefühls kommen. Neben einer verlangsamten Reaktionsgeschwindigkeit und gestörter Koordinationsfähigkeit sind Gleichgültigkeit, Interessenverlust und Antriebsstörungen sowie Verschlechterung der kognitiven Funktionen möglich. Aber auch Angst- und Panikzustände können auftreten.

Bei hoch dosiertem Langzeitkonsum treten häufig Persönlichkeitsveränderungen auf und das Risiko für ein vorzeitiges Eintreten einer psychischen Erkrankung steigt. Viele langfristige Veränderungen beginnen schleichend und werden selbst oft nicht wahrgenommen. Ein früher Beginn des Cannabiskonsums ist besonders kritisch, da das Gehirn bis zum 25. Lebensjahr einen Reifungsprozess vollzieht. Im Allgemeinen ist bei einem dauerhaften und regelmäßigen Cannabiskonsum eine Abnahme der geistigen und körperlichen Leistungsfähigkeit erwartbar.

Alkoholmissbrauch am Arbeitsplatz lässt sich, wie im Straßenverkehr auch, seit Jahrzehnten einfach und sicher nachweisen bzw. bestimmen. Wie stellt sich dies bei Cannabis dar?

Dr. Juliane Falkenberg: Bei Alkohol besteht bei gewöhnlichem Konsum ein gut voraussagbarer Effekt auf den Organismus. Diese eindeutige Analogie gibt es bei Cannabis nicht. Dies liegt an den bereits geschilderten Faktoren und individuellen Gegebenheiten.

Zudem sind der Nachweis und insbesondere die Interpretation von Cannabistests komplexer als bei den etablierten Alkoholtests. Cannabistests können über Urin, Blut, Stuhl, Haare und Mundsekret (sogenannte Speicheltests) erfolgen. Dabei werden je nach Test verschiedene Substanzen und ihre Abbauprodukte gemessen. Der Abbau von THC im Körper erfolgt über verschiedene Stoffwechselzwischenprodukte (Metabolite), die teilweise auch das Bewusstsein beeinflussen, bis hin zur TBC-Carbonsäure (THC-COOH), die selbst keine psychoaktive Wirkung mehr entfaltet. Die aktiven Metabolite sind im Gegensatz zur THC-Carbonsäure nur in einem vergleichsweise kurzen Zeitfenster ermittelbar. Daher ist es wichtig zu wissen, was mit dem jeweiligen Test genau gemessen wird. Zudem spielt es auch eine Rolle, ob mit der Methode nur ein positives bzw. negatives Ergebnis detektiert oder auch eine Quantifizierung, d. h. ein Messwert, generiert werden kann. Den psychoaktiven Wirkstoff verlässlich messen, können in der Regel nur Bluttests. Der Nachteil dabei ist, dass das Ergebnis nicht unmittelbar vorliegt und der Aufwand für eine Blutserumprobe hoch ist.

Grundlage vieler Tests ist die THC-Carbonsäure. Sie ist aber als Messparameter nur bedingt geeignet, da dieser Metabolit nicht mehr psychoaktiv wirksam ist und relativ lange nachgewiesen werden kann. Bei seltenem/gelegentlichem Cannabiskonsum liegt in der Regel der Messwert nach einem Tag unter der Nachweisgrenze und die Person kann somit als negativ bewertet werden. Bei häufigem/regelmäßigem Konsum kommt es zur Speicherung von THC-Carbonsäure im Fettgewebe und damit zu einer langfristigen Ausscheidung, respektive Detektierbarkeit. Dies bedeutet nicht unbedingt, dass die Person aktuell unter einem psychotropen Effekt von Cannabis steht. Somit lässt sich in solchen Fällen mit diesem Parameter nicht ableiten, ob die letzte Einnahme von Cannabis lange genug zurückliegt bzw. ob eine bewusstseinsbeeinträchtigende Wirkung mit Sicherheit ausgeschlossen werden kann.

Bild: # 1345107013 / istockphoto.com

Ließen sich die aktuellen Regelungen, die in Hinsicht auf Cannabis für den Straßenverkehr bestehen, auch für den Arbeitsschutz nutzen?

Dr. Juliane Falkenberg: Im Straßenverkehrsrecht stehen gesellschaftliche Abwägungsinteressen im Mittelpunkt. Dagegen steht im Unternehmen der betriebliche Arbeitsschutz mit der Vermeidung von Gefährdungen für alle Mitarbeitenden an erster Stelle. Im Straßenverkehrsrecht sind zu Alkohol und anderen Drogen entsprechende Regelungen verankert, dagegen bestehen im Arbeitsrecht keine festgelegten Grenzwerte. Hier müssen die Unternehmen im Rahmen der Verhältnismäßigkeit selbst tätig werden.

Unfallversicherungsträger fordern seit jeher eine Null-Toleranz-Politik in Bezug auf Alkohol und andere Drogen. Dies galt und gilt trotz der seit Langem bestehenden Regelungen zu Promillegrenzen von Blutalkohol im Straßenverkehrsrecht. Laut wissenschaftlichem Beirat, der aktuell die Bundesregierung zum Grenzwert im Straßenverkehrsgesetz beraten hat, wird bei einem Cannabisgrenzwert von 3,5 ng/ml Blutserum eine Beeinträchtigung entsprechend einer Blutalkoholkonzentration von etwa 0,2 Promille im Mittel vermutet. Dabei bestehen wegen der individuellen Auswirkungen und Verstoffwechselung von Cannabis entsprechende Schwankungsbreiten, die zu bedenken sind. Aus sicherheitstechnischer und präventiver Sicht ist die folgerichtige Konsequenz, Cannabis genauso wie Alkohol im Betrieb zu behandeln. Mit einer eindeutigen Position und einem definierten Grenzwert von null im Betrieb besteht Klarheit für die Belegschaft. Auch kann Führungskräften nicht zugemutet werden zwischen Personen, die „leicht bekifft" oder heute vielleicht doch zu sehr „zugedröhnt" sind, zu unterscheiden, um sie am Kran oder anderen sicherheitsrelevanten Bereichen arbeiten zu lassen.

Angenommen, es kommt zu einem Arbeitsunfall. Was wären die Folgen, wenn sich herausstellt, dass der Konsum von Cannabis dabei eine Rolle gespielt hat?

Dr. Juliane Falkenberg: Insbesondere kostenintensive, schwere oder gar tödliche Arbeitsunfälle werden durch die gesetzlichen Unfallversicherungsträger durchleuchtet. Ergibt sich, dass die vorsätzliche oder grob fahrlässige Verletzung der Fürsorgepflicht des Arbeitgebers zu einem Arbeitsunfall geführt hat, resultiert eine haftungsrechtliche Verantwortung für den Arbeitgeber, und der zuständige Unfallversicherungsträger kann gegebenenfalls einen Regressanspruch geltend machen. Für Beschäftigte kann ein entsprechender Konsum von Cannabis unter Umständen zum Verlust ihres Versicherungsschutzes führen und ihnen bleiben die Leistungen der Unfallversicherung bei einem Unfall versagt.

Welche rechtlichen Anforderungen müssen Unternehmen im Umgang mit Cannabis am Arbeitsplatz beachten? Ist es den Unternehmen möglich, entsprechende Verbote zu erlassen?

Dr. Juliane Falkenberg: Was einige Arbeitgeber nicht wissen ist, dass es im Arbeitsrecht kein absolutes Rauschmittelverbot gibt. Neben Alkohol haben wir nun ein weiteres Rausch- und Sucht-

mittel, das legal ist. Folglich bedeutet dies, dass jedes Unternehmen hierfür Regelungen treffen muss. Die meisten Unternehmen haben bereits schriftlich festgelegte Vereinbarungen zum Konsum von Alkohol bzw. berauschenden Mitteln. Arbeitgeber sollten analog zum Alkoholverbot auch ein Cannabisverbot am Arbeitsplatz einführen bzw. überprüfen, ob ihre Vereinbarungen auch für den Konsum von Cannabis gelten.

Die Unternehmen, die bisher keine Regelungen getroffen haben, sollten sich spätestens jetzt darum kümmern. Ein Verbot kann auf individueller Ebene arbeitsvertraglich mit den Beschäftigten vereinbart werden. Sofern ein Personal-/Betriebsrat vorhanden ist, muss eine Regelung zu berauschenden Mitteln über eine Dienst-/Betriebsvereinbarung realisiert werden, denn es

Bild: # 1327731035 / istockphoto.com

sind unbedingt Mitbestimmungsrechte zu beachten. In den Betriebs- oder Dienstvereinbarungen sollten Maßnahmen und Konsequenzen bei Konsum von berauschenden Mitteln festgehalten werden. Darüber hinaus ist es wichtig, diese Regelungen im Betrieb zu kommunizieren. Verstoßen Beschäftigte dagegen, können sie eine Abmahnung oder gar Kündigung riskieren.

Was sollten Arbeitgeber beachten, wenn Beschäftigte eine Therapie mit Cannabis erhalten? Welche Rolle spielt die individuelle Gefährdungsbeurteilung bei Mitarbeitern, die Medizinal-Cannabis konsumieren?

Dr. Juliane Falkenberg: Seit 2017 gibt es die Möglichkeit, Cannabis aus medizinischen Zwecken zu verordnen und über die gesetzliche Krankenversicherung abzurechnen. Hier ist nicht der Genuss bzw. die Rauschwirkung, sondern die Symptomlinderung bei bestimmten Diagnosen, wie zum Beispiel bei Spastiken oder Nebenwirkungen von Krebserkrankungen/-therapien das Ziel. Diese Art von Konsum unterscheidet sich auch rechtlich vom Genusskonsum. Daher sollte für eine medizinisch indizierte Cannabistherapie eine innerbetriebliche Regelung festgelegt werden, an deren Ausgestaltung Betriebsarzt/Betriebsärztin, Fachkräfte für Arbeitssicherheit, Sicherheitsbeauftragte sowie ggf. weitere Personenkreise wie Betriebsratsmitglieder und Suchtbeauftragte beteiligt sind.

Allen Vorgesetzten und Mitarbeitenden sollten die entsprechenden Regelungen bekannt sein. Die Beschäftigten müssen unterwiesen werden, dass eine Cannabistherapie zu melden ist, damit eine individuelle Gefährdungsbeurteilung erfolgen kann. Dies sollte natürlich auch für andere/medikamentöse Therapien, die möglicherweise Konzentration und Verkehrstüchtigkeit einschränken, gelten. Eine Meldung hat auch bei kurzzeitigen Therapien zu erfolgen, denn gerade die Einstellungsphase kann kritisch sein.

Die individuelle Gefährdungsbeurteilung ist die Basis einer durchdachten Arbeitssicherheitsstrategie. Gegebenenfalls sind bestimmte Tätigkeiten auszuschließen und alternative Einsatzmöglichkeiten festzulegen. Auch die regelmäßige Überprüfung dieser individuellen Gefährdungsbeurteilung und der abgeleiteten Maßnahmen sowie Kontrollen bei Auffälligkeiten sollten schriftlich festgehalten werden. Nur so kann ein sicheres Arbeiten für die Person selbst sowie für Kollegen und Kolleginnen gewährleistet werden.

Durch die Teil-Legalisierung hat sich bei der Verordnung von Medizinal-Cannabis einiges geändert. Es bedarf keines Betäubungsmittelrezeptes mehr und vielfach wird nicht mehr der Weg über die Krankenkasse gegangen, die nur bei bestimmten Diagnosen und Ausschluss anderer Behandlungsmöglichkeiten dieser Therapie zugestimmt hat. Leider wird mittlerweile viel Missbrauch unter dem Deckmantel einer indizierten Cannabistherapie und mit THC-Rezepten getrieben. Der THC-Gehalt von Cannabisprodukten aus der Apotheke wird streng kontrolliert. Bei einem anderen Bezugsweg können größere THC-Schwankungsbreiten nicht mit einer solchen Sicherheit ausgeschlossen werden. Diagnose, Therapieart, Dosierung, Anwendung, Zeitintervalle und Therapiekontrollen durch den verordnenden Arzt/die verordnende Ärztin und viele weitere Aspekte sind zu bedenken. Wegen der Komplexität der zu berücksichtigenden Einflussfaktoren sollten sich Arbeitgeber von Sicherheitsfachkräften und Betriebsarzt/Betriebsärztin, die mit den Arbeitsplatzverhältnissen vertraut sind, in jedem Einzelfall beraten lassen. Rezepte

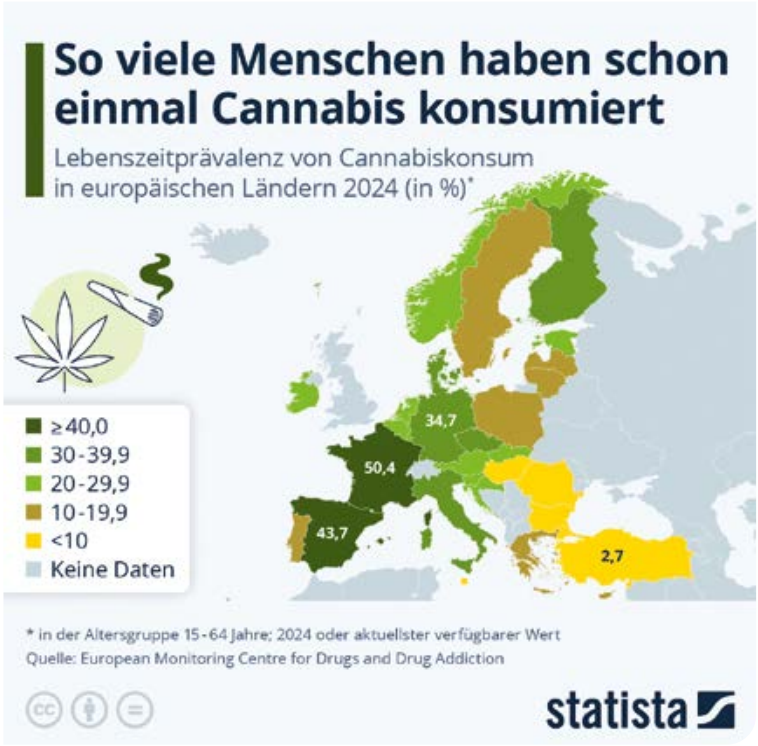
aus dem Internet ohne persönlichen ärztlichen Kontakt und Kontrolle sind in meinen Augen nicht verantwortbar und kategorisch abzulehnen. Hier wird das Medikamentenprivileg missbraucht.

Wie können Unternehmen präventiv gegen Suchterkrankungen im Allgemeinen und im Speziellen gegen Cannabisabhängigkeit vorgehen und welche Maßnahmen sind besonders effektiv?

Dr. Juliane Falkenberg: Prävention ist ein wichtiger Teil des Arbeitsschutzes, um langfristig Gesundheit und Sicherheit im Betrieb zu fördern sowie Suchterkrankungen erfolgreich zu verhindern. Cannabis ist ein weiteres Rausch- und Suchtmittel und es ist gut, dass sich aufgrund der Legalisierung gerade viele Betriebe entsprechende Fragen stellen und sich des Themas annehmen. Es sollte jedoch nicht nur um Cannabis gehen, denn auch andere Suchtmittel, insbesondere Alkohol, aber auch stoffungebundene Süchte wie beispielsweise die Spielsucht, sollten im Rahmen der aktuellen Bearbeitung des Themas überprüft und mitgedacht werden (siehe DGUV Information 206-009 „Suchtprävention in der Arbeitswelt“).

Arbeitgeber müssen mögliche suchtfördernde Gegebenheiten im Betrieb analysieren und präventiv angehen. Bewährt hat sich hierfür die Erstellung von innerbetrieblichen Regelungen in Form von Betriebs- oder Dienstvereinbarungen. Zu diesem Zweck ist es sinnvoll, verschiedene Berufsgruppen, wie Sicherheitsfachkräfte, Betriebsärzte und – sofern vorhanden – Suchtbeauftragte, Personal-/Betriebsratsvertreter und ggf. noch weitere Personenkreise an einen Tisch zu holen. Sie sollten bei der Erstellung eines Gesamtkonzeptes eingebunden werden, in dem unter anderem der Umgang mit Personen, die Hinweise auf einen Suchtmittelmissbrauch oder eine Suchterkrankung liefern, klar geregelt ist.

Zum Beispiel kann ein sogenannter Stufenplan etabliert werden (siehe z. B. Merkblatt A 003 „Suchtmittel im Betrieb“). Dieser bildet die Grundlage für eine zielführende Intervention und bietet allen Beteiligten Handlungssicherheit für den konkreten Fall. Auf diese Weise haben Führungskräfte einen Leitfaden, an dem sie sich orientieren können. Darüber hinaus müssen alle Mitarbeitenden über Suchtmittel, Suchterkrankung sowie über betriebliche Konsequenzen aufgeklärt und über richtiges Handeln im Sinne der betrieblichen Regelung unterwiesen werden. Ein offener Kommunikationsstil sollte gelebt werden.



Geeignete Mitarbeitende können speziell geschult und zu Suchtbeauftragten/Ansprechpersonen ausgebildet werden. Hilfreich sind innerbetriebliche Veröffentlichungen von Kontaktdaten von internen Ansprechpersonen sowie externer Beratungsstellen. Eine Kultur der Hilfsbereitschaft und der Angebote sollte etabliert werden. Um Gesundheit und Leistungsfähigkeit der Beschäftigten zu erhalten, ist die Umsetzung von Präventionsmaßnahmen im ureigensten Interesse eines jeden Betriebes. Außerdem geht es um mehr, denn hinter jedem Mitarbeiter, jeder Mitarbeiterin steht ein Mensch. Unternehmen können durch die genannten Maßnahmen Hilfe leisten und sofern möglich durch den Arbeitsplatz der betroffenen Person die benötigte Stabilität geben.

Neben gesetzlichen Krankenkassen, die insbesondere verhaltenspräventive Hinweise geben, finden sich bei den gesetzlichen Unfallversicherungsträgern viele Informationen zum Thema Suchtprävention und Herangehensweisen zur Etablierung einer betrieblichen Regelung. Zudem bietet beispielsweise die BG RCI auch verschiedene Seminare zum Thema „Suchtmittelprävention im Betrieb“ sowie Ausbildungsseminare zu „Betrieblichen Suchtbeauftragten“ für Beschäftigte von versicherten Mitgliedsbetrieben an. Suchtprävention ist sehr wichtig und hat nicht nur große Bedeutung für die individuelle Gesundheit, sondern auch eine enorme Auswirkung auf Familie und Gesellschaft sowie auf die betrieblichen Bedingungen.

Kritische Infrastrukturen umfassend schützen

Von Holger Köster

Holger Köster

Geschäftsführer der HERSA-Unternehmensgruppe und Vorsitzender des Fachausschusses Wirtschaftsschutz im BDSW

Manchmal braucht es keine physische Gewalt, um verheerende Schäden anzurichten, mitunter genügt dafür ein Stromausfall. Ein paar Stunden Dunkelheit, und Krankenhäuser geraten in Notbetrieb, Logistikketten brechen zusammen, Wasserwerke stoppen ihre Versorgung: Unsere moderne Gesellschaft ist verletzlicher, als wir glauben möchten.

Kritische Infrastrukturen sind das Rückgrat unseres Landes, zugleich aber auch das bevorzugte Ziel hybrider Angriffe. Umso wichtiger ist es, diese Infrastrukturen nicht nur als technische Systeme zu begreifen. KRITIS sind mehr als Stromnetze, Kläranlagen oder Rechenzentren, sie sind Teil komplexer Versorgungsstrukturen, in denen Prozesse, Menschen und Organisationen ineinandergreifen. Wer sie schützen will, muss deshalb über rein technische Maßnahmen hinausdenken und ganzheitliche, widerstandsfähige Schutzkonzepte entwickeln.

Das geplante KRITIS-Dachgesetz ist ein überfälliger Schritt in diese Richtung. Es soll den Schutz kritischer Einrichtungen auf neue gesetzliche Grundlagen stellen und neben IT- auch physische Sicherheitsmaßnahmen verbindlich einfordern. Der Fachartikel „KRITIS unter Druck: Was das neue Dachgesetz leisten muss“ in dieser Ausgabe zeichnet die Hintergründe und politischen Entwicklungen rund um das Gesetz nach und zeigt auf, was es für Betreiber, Behörden und Sicherheitsdienstleister bedeuten könnte. Dabei wird deutlich: Das Gesetz ist nicht nur ein Regulierungsvorhaben, sondern eine Chance, den Schutz kritischer Infrastrukturen auf eine neue Stufe zu heben, vor allem aber auch eine Chance für Sicherheitsdienstleister, ihre Kompetenzen strategisch einzubringen.

Denn die Sicherheit Kritischer Infrastrukturen lässt sich nicht allein durch Normen oder IT-Schutzmaßnahmen gewährleisten. Sie erfordert ein umfassenderes Verständnis von Verwundbarkeit und Schutz, das auch physische Sicherheitsmaßnahmen, organisatorische Strukturen und klare Zuständigkeiten einbezieht. Zutrittskontrollen, Reaktionspläne, personelle Ressourcen und abgestimmte Prozesse sind ebenso entscheidend wie Firewalls und Verschlüsselung. Der Schutz unserer Infrastruktur ist eine gemeinsame Aufgabe und gelingt nur im Zusammenspiel von Staat und der privaten Sicherheitswirtschaft.

Ihr
Holger Köster

Bild: Nhan Hoang / unsplash.com

KRITIS unter Druck: was das neue Dachgesetz leisten muss

Weichenstellung für mehr Resilienz Kritischer Infrastrukturen

Von Andreas Albrecht

Strom, Wasser, IT, Transport: Kritische Infrastrukturen werden zunehmend zum Ziel hybrider Angriffe. Das geplante KRITIS-Dachgesetz soll für mehr Schutz sorgen. Doch was ist genau geplant? Wer ist betroffen? Und was bedeutet das für die Sicherheitswirtschaft? Ein Überblick.

Andreas Albrecht
Freier Fachredakteur und Journalist

Wenn der Strom ausfällt, ist schnell mehr betroffen als das Licht. Ohne Energie stehen Produktionsanlagen still, Kühlketten sind unterbrochen, Krankenhäuser geraten in Notbetrieb, der Verkehr kollabiert: In Marc Elsbergs Bestseller *„Blackout – Morgen ist es zu spät"* legt ein gezielter Hackerangriff die gesamte europäische Stromversorgung lahm. Die Folgen sind katastrophal: Chaos, Verunsicherung und Kontrollverlust erfassen innerhalb weniger Tage Gesellschaft, Wirtschaft und staatliche Strukturen.

Was im Roman noch Fiktion war, wird heute immer mehr zu einem möglichen realistischen Szenario. Denn die Zahl gezielter Angriffe auf Kritische Infrastrukturen (KRITIS) nimmt stetig zu, und diese verlaufen selten eindimensional. Sabotage trifft auf Cyberattacke, Erpressung auf menschliches Versagen, digitale Schwachstellen auf physische Lücken: Immer häufiger sind es hybride Bedrohungen, die Sicherheitsverantwortliche vor immer größere Herausforderungen stellen, im Energiesektor ebenso wie in der Gesundheitsversorgung, bei Wasserwerken, im Transport oder in der Logistik.

Das KRITIS-Dachgesetz kommt – aber wann?

Der politische Wille, Kritische Infrastrukturen besser zu schützen, ist deutlich erkennbar, wie unter anderem die intensiven Bemühungen um das KRITIS-Dachgesetz zeigen, das auf einer klaren europäischen Vorgabe basiert. Konkret geht es um die Umsetzung der EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie), die im Januar 2023 in Kraft getreten ist. Sie verpflichtet die Mitgliedstaaten, verbindliche nationale Regelungen zu schaffen, die den Schutz Kritischer Infrastrukturen sektorenübergreifend verbessern, im digitalen, aber vor allem auch im physischen Bereich.

Die neue Bundesregierung hat diesen Anspruch bereits Ende Februar 2025 im Koalitionsvertrag verankert, wenn auch äußerst lakonisch. Mit einem einzigen Satz wird hier ein KRITIS-Dachgesetz angekündigt (Zeile 2698), erklärt wird nichts.

Auch ein endgültiger Gesetzestext lässt weiter auf sich warten. Nach der Verschiebung des ursprünglich für Oktober 2024 vorgesehenen Gesetzes gilt unter Branchenexperten aktuell eine Verabschiedung Ende 2025 bis Anfang 2026 als realistischer Zeitrahmen. Klar ist aber bereits jetzt: Im Zentrum des KRITIS-Dachgeset-

Bild: Dmytro Vynohradov / unsplash.com

zes wird ein ganzheitlicher Ansatz stehen, der nicht nur digitale Risiken abdecken soll, sondern auch physische Gefahren berücksichtigt. Damit wird erstmals gesetzlich verankert, dass Betreiber von KRITIS-Einrichtungen nicht nur Firewalls und Verschlüsselung brauchen, sondern auch physische Sicherheitsmaßnahmen wie Zäune, Zutrittskontrolle, Videoüberwachung oder Objektschutz.

Ein Perspektivwechsel, der tief greift. Denn von dem neuen Gesetz werden nicht nur Großkonzerne mit eigener Sicherheitsabteilung, sondern auch kleinere Betreiber betroffen sein, etwa kommunale Wasserwerke, regionale Gesundheitsdienstleister oder mittelständische Logistikunternehmen. Viele von ihnen werden dann zum ersten Mal mit sicherheitsrechtlichen Pflichten konfrontiert und wissen dies möglicherweise heute noch nicht einmal.

Herausforderung und Chance zugleich für Sicherheitsdienstleister

Für die private Sicherheitswirtschaft zeichnen sich dabei neben neuen Herausforderungen auch neue Chancen ab. Denn mit der Einführung des KRITIS-Dachgesetzes steigt nicht nur der Druck auf die Betreiber, auch Dienstleister werden verstärkt in die Verantwortung kommen. Viele kleinere Unternehmen, insbesondere im kommunalen oder mittelständischen Bereich, dürften noch nicht über das notwendige Know-how verfügen, um komplexe Risikoanalysen, Sicherheitskonzepte oder Interventionspläne eigenständig zu entwickeln und umzusetzen. Die Folge: Der Bedarf an spezialisierter externer Unterstützung dürfte deutlich steigen, sowohl technologisch als auch personell. Für Anbieter aus der Sicherheitswirtschaft könnte sich damit ein dynamisch wachsender Markt eröffnen, der nicht nur kurzfristige Schutzmaßnahmen, sondern langfristige Sicherheitsarchitekturen verlangt.

Diese Entwicklung unterstreicht auch ein gemeinsames Grundsatzpapier des Bundesverbandes Sicherheitstechnik (BHE) und des Verbands für Sicherheitstechnik (VfS), in dem von einem grundlegenden „Paradigmenwechsel in der Sicherheitsarchitektur Deutschlands“ die Rede ist und ein sektorenübergreifender technologieoffener Ansatz gefordert wird. Zugleich mahnen die Verbände an, dass Zuständigkeiten klar definiert und gesetzliche Vorgaben realistisch umsetzbar sein müssten. Andernfalls drohten Überforderung und Ineffizienz, insbesondere bei kleineren KRITIS-Betreibern.

BBK: Kontrolle mit Fragezeichen

Eine zentrale Rolle bei der Umsetzung des KRITIS-Dachgesetzes soll das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) übernehmen. Als koordinierende Stelle ist es künftig dafür verantwortlich, KRITIS-Akteure zu identifizieren, Mindestanforderungen zu definieren und die Einhaltung zu überwachen. Damit wird das BBK zur Schnittstelle zwischen staatlicher Aufsicht, Betreiberverantwortung und Fachwissen aus Wirtschaft und Verbänden.

Doch dieser koordinierende Anspruch ist ambitioniert – und nicht frei von Kritik. Die zivilgesellschaftliche Initiative Open KRITIS etwa warnt vor einem zu weit gefassten oder unklar abgegrenzten Geltungsbereich. Sie fordert transpa-

rente Kriterien für die KRITIS-Zugehörigkeit, realistische Umsetzungsfristen und eine bessere Berücksichtigung bestehender Sicherheitsstrukturen. Ziel müsse es sein, Mehrarbeit zu vermeiden und stattdessen Synergien zu nutzen.

Mehr als IT: physische Sicherheit wird zur Pflicht

Ein wesentlicher Fortschritt des geplanten Gesetzes ist die Abkehr von der bisherigen Fokussierung auf IT-Sicherheit. Künftig sollen auch physische Risiken systematisch erfasst und entsprechende Sicherheitsmaßnahmen vorgeschrieben werden – von der Zutrittskontrolle über Videoüberwachung in einzelnen Betrieben bis hin zum Perimeterschutz ganzer Liegenschaften.

Für Sicherheitsdienstleister bedeutet das: Gefragt sind keine isolierten Produkte, sondern ganzheitliche Konzepte. Wer sich als Partner der Betreiber positionieren will, muss die betrieblichen Abläufe verstehen, branchenspezifische Risiken einordnen und praxistaugliche Lösungen entwickeln.

Investitionen mit Hebelwirkung

Allerdings stellt sich angesichts des zu erwartenden Aufwands eine entscheidende Frage: Wer soll das alles bezahlen? Der Verband für Sicherheitstechnik (VfS) plädiert hier für staatliche Investitionsimpulse. Konkret fordert er ein jährliches Budget von 20 Milliarden Euro zur Unterstützung von Mittelstand und KRITIS-Betreibern.

Ob diese Mittel in dieser Größenordnung fließen werden, bleibt abzuwarten. Klar ist jedoch: Ohne zusätzliche finanzielle Mittel, wie Förderprogramme oder steuerliche Anreize, könnten viele Unternehmen bei der Umsetzung der KRITIS-Anforderungen schnell an ihre Grenzen stoßen.

Es bleibt also für alle Beteiligten in Bezug auf das kommende KRITIS-Dachgesetz noch einiges zu tun. Für Betreiber bedeutet das: Sie müssen in Schutzmaßnahmen investieren, Risiken analysieren und Betriebsabläufe strukturieren. Für Sicherheitsdienstleister gilt es, kompetent zu beraten und tragfähige Lösungen zu liefern. Und für die Politik? Sie muss aus der Ankündigung endlich eine Verbindlichkeit machen. Sonst bleibt das „Dach" weiter im Rohbau stecken.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

BKA – Bundeslagebild Wirtschaftskriminalität 2024

Die polizeilich registrierten Wirtschaftsdelikte im Jahr 2024 stiegen gegenüber dem Vorjahr um 57,6 Prozent auf insgesamt 61.358 Fälle an. Hauptgrund hierfür ist eine Zunahme von 847,6 Prozent bei Fällen von Betrug und Abrechnungsbetrug im Gesundheitswesen. Zudem gewinnt das Tatmittel Internet mehr an Relevanz. Die Gesamtschadenssumme wird auf 2,76 Milliarden Euro beziffert.
www.bka.de

FitNIS2-Navigator bietet Hilfe bei NIS2-Umsetzung

Deutschland sicher im Netz e. V. (DsiN) mit der Universität Paderborn stellt ein kostenfreies Online-Tool zur Verfügung, das KMU-Unternehmen bei der Umsetzung der EU-Richtlinie NIS2 unterstützt. Das auch vom BMWE geförderte Projekt hilft mittels eines Navigators dabei, den individuellen Handlungsbedarf zu erkennen und konkrete Maßnahmen zur IT-Sicherheit zu entwickeln.
www.fitnis2.de

EHI-Studie: Inventurdifferenzen 2025

Die Studie ermittelt für das Jahr 2024 durchschnittliche Inventurdifferenzen in Höhe von 0,64 Prozent, bewertet zu Einkaufspreisen in Relation zum Nettoumsatz. Im gesamten stationären deutschen Einzelhandel summieren sich die Inventurdifferenzen auf 4,95 Milliarden Euro. Damit sind die Inventurdifferenzen im Vergleich zum Vorjahr um rund drei Prozent gestiegen.
www.ehi.org

CyMon 2025: Befragung zur Cybersicherheit

Der Kurzbericht zu den Umfrageergebnissen der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamts für Sicherheit in der Informationstechnik (BSI). Sieben Prozent der befragten Bürger waren allein in den vergangenen zwölf Monaten von Cyberkriminalität betroffen. Am wichtigsten sind für Informationssuchende Handlungsempfehlungen für den Ernstfall.
www.bsi.bund.de

RA Dr. Berthold Stoppelkamp
zuständiges Geschäftsführungsmitglied für den Fachausschuss Wirtschaftsschutz im BDSW

Wirtschaftssicherheit ist mehr als Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

RA Dr. Berthold Stoppelkamp

Geschäftsführer des Bundesverbandes der Sicherheitswirtschaft (BDSW)

Der Berichtszeitraum von Anfang Mai bis Mitte August 2025 war innenpolitisch durch die Neuausrichtung der Migrationspolitik, die Zukunft der Sozialsysteme und die Findung eines Mindestlohns geprägt. Ein Bundestariftreuegesetz und Änderungen des Sicherheitsüberprüfungsgesetzes wurden vom Kabinett beschlossen. Sicherheitspolitisch dominierte der Krieg zwischen Israel und dem Iran, das militärische Eingreifen der USA zur Zerstörung der iranischen Atomanlagen, der Krieg in Gaza und der Ukraine sowie die personelle Stärkung der Bundeswehr durch mehr Wehrpflichtige bzw. den Ausbau der Reservistenzahlen die öffentliche Debatte. Wirtschaftspolitisch standen die US-Zollpolitik und die Vereinbarung zwischen den USA und der EU hierzu im Fokus der medialen und politischen Diskussion.

Die Welt in Unordnung

Seit der zunehmenden Infragestellung der europäischen Sicherheitsordnung nach dem Zweiten Weltkrieg durch den Angriffskrieg Russlands gegen die Ukraine und der in den letzten Jahren zunehmenden Kritik der USA an der Lastenverteilung innerhalb des NATO-Verteidigungsbündnisses gerät die etablierte und für Deutschland gewohnte Sicherheitsordnung zunehmend ins Wanken. Zudem hat sich auch durch die in den letzten Jahren festzustellende steigende illegale Migration das Unsicherheitsgefühl in der Bevölkerung vergrößert und bestimmt immer mehr den politischen Diskurs. Die notwendigen politischen Debatten zur Verteidigungsfähigkeit, zur Wehrpflicht, zur Sicherung der Sozialsysteme und zur Migrationspolitik sind Ausdruck einer Welt in Unordnung.

Resilienzsteigerung

Die deutsche Sicherheitspolitik hat sich in den letzten Jahren seit der Wiedervereinigung zu wenig auf die Verteidigungsfähigkeit und den Bevölkerungsschutz fokussiert. Die von der neuen Regierung angekündigten Maßnahmen zur Resilienzsteigerung werden diese Defizite leider nicht bereits bis 2029 ausgleichen können, um wirklich Russland konventionell abschrecken zu können. Ohne den atomaren Schutzschirm der USA bleibt Deutschland schutzlos. Deutschland hat sich in den letzten Jahren beim Thema Resilienzsteigerung primär auf den Klimaschutz, die Stärkung der Cybersicherheit und die Stärkung der Sicherheitsbehörden in Bund und Ländern fokussiert. Fast jede Partei setzt sich für eine Stärkung der Sicherheitsbehörden ein. Allein der BDSW setzt sich vernehmbar für eine verstärkte Einbeziehung der Sicherheitswirtschaft zur Resilienzsteigerung ein, wenn auch diese Bemühungen bisher nur ansatzweise mit Erfolg gekrönt waren. Primär im Bereich des Schutzes Kritischer Infrastrukturen ist bereits die vorherige Bundesregierung – allerdings veranlasst aufgrund von EU-Vorgaben – aktiv geworden. Mit der Initiative Wirtschaftsschutz, die der BDSW 2016 mitinitiiert hat, verfolgen Staat und Wirtschaft das gemeinsame Ziel, den Schutz von Unternehmen und ihrer Geschäftstätigkeit vor verschiedenen Bedrohungen zu verbessern. Dazu gehört der Schutz vor Wirtschaftsspionage, Sabotage, Datendiebstahl und anderen Formen der Kriminalität, die den wirtschaftlichen Erfolg eines Unternehmens gefährden können. Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) 2012 initiierte Allianz für Cybersicherheit verfolgt das primäre Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyberangriffen zu stärken. Beide Initiativen sind allerdings nur Teilbestandteile einer Wirtschaftssicherheitsstrategie, denn sie zielen primär allein auf den Schutz von Unternehmen ab, nicht aber auf den Erhalt der wirtschaftlichen Souveränität Deutschlands.

Prosperitätssicherung

Bei der Wirtschaftssicherheitsstrategie für Deutschland geht es demgegenüber primär darum, die Bedingungen für eine stabile und wachsende Wirtschaft zu schaffen und zu schützen, um zukünftigen Wohlstand zu sichern. Dies umfasst sowohl Maßnahmen zur Förderung des Wirtschaftswachstums als auch zur Bewältigung von Risiken und Krisen. Betrachtet man die führenden Wirtschaftsnationen USA und China, so fällt auf, dass diese im Rahmen ihrer weltweiten Rivalität um Einflusssphären Wirtschaftssicherheitsmaßnahmen einsetzen, um ihre politischen, aber insbesondere ihre wirtschaftlichen Interessen zu fördern. Als Instrumente bedient man sich Exportrestriktionen, Importrestriktionen, Investionsrestriktionen, Datenrestriktionen sowie industriepolitischer Maßnahmen, wie beispielsweise des Inflation Reduction Act in den USA. Auch die EU als Wirtschaftsraum bedient sich bereits vieler Wirtschaftssicherheitsmaßnahmen wie beispielsweise der EU-Dual-Use-Verordnung, der NIS 2 Richtlinie, der Datenschutz-Grundverordnung oder des EU Critical Raw Materials Act.

Deutschlands Zukunftsfähigkeit sichern

Die Frage ist nun, wie sich Deutschland in diesem globalen Wettbewerb der Volkswirtschaften durch eine Wirtschaftssicherheitspolitik wird behaupten können. Die Herausforderungen für Deutschland sind immens. Zwar ist Deutschland die drittgrößte Volkswirtschaft der Welt. Aber im Vergleich zu China und den USA hat Deutschland die höchste Exportquote, die in den letzten Jahren über 40 Prozent lag. Dies bedeutet für Deutschland ein erhöhtes Risiko, wenn die Wettbewerber USA und China ihre Märkte durch Regulierung abschotten bzw. den Export für deutsche Güter extrem verteuern. Auch wenn in Deutschland nach wie vor viele Unternehmen, gerade die sog. Hidden Champions, ansässig sind, die über eine weltweite Technologieführerschaft verfügen, so hat sich in den letzten Jahren die Abhängigkeit dieser Unternehmen vom Zukauf von Komponenten aus China zur Aufrechterhaltung der Technologieführerschaft erhöht. Um dem im Sinne eines De-Risking-Ansatzes zu begegnen, hat Deutschland beispielsweise mit dem IT-Sicherheitsgesetz 2.0 den Ausschluss von Huawei und ZTE bei der 5G-Technologie bis 2026 bzw. 2029 bewirkt. Allerdings hat dies zur Folge, dass sich deutsche Unternehmen in die Abhängigkeit anderer weniger Anbieter am Markt begeben müssen.

Ziele für eine neue Wirtschaftssicherheitsstrategie

Laut Koalitionsvertrag will die neue Bundesregierung die bestehende nationale Sicherheitsstrategie überarbeiten und damit auch die Wirtschaftssicherheitsstrategie. Folgende Ziele sollten nach Auffassung des Autors verfolgt werden:

1. Aufbau eines Lagezentrums, das nach einer Risikomatrix Daten aus allen Wirtschaftszweigen, aus allen staatlichen Ebenen, Sicherheitsbehörden und Zivilgesellschaft sammelt und im Sinne einer Risikoanalyse permanent auswertet.

2. Importabhängigkeiten bei kritischen Rohstoffen reduzieren und Exportabhängigkeiten beobachten bzw. minimieren.

3. Technologietrends in globalen Märkten durch den Auslandsnachrichtendienst intensiver beobachten.

4. Gezielte Förderung und Absicherung von Schlüsselindustrien.

5. Internationale Handelswege mit NATO, verbündeten Staaten und Sicherheitswirtschaft sichern.

6. Wohlstandserhaltung und Maximierung durch wirtschaftspolitische, arbeits- und sozialpolitische sowie migrationspolitische Maßnahmen.

Rolle der Sicherheitswirtschaft

Innerhalb einer die sechs aufgeführten Ziele verfolgenden Wirtschaftssicherheitsstrategie kommt der Sicherheitswirtschaft momentan primär eine rein operative Rolle zu. So kann sie Schutzmaßnahmen im physischen und Cyberbereich für Schlüsselindustrien, die KRITIS-Sektoren und die Hidden Champions garantieren. Ebenso kann die Sicherheitswirtschaft durch Seeschiffbewachung das Risko vor Piraterie auf internationalen Handelsrouten minimieren. Aber auch bei Aufbau eines Lagezentrums könnte die Sicherheitswirtschaft datenschutzkonform und anonymisiert Daten über Kriminalitätsentwicklungen übermitteln, die die Wirtschaft betreffen. Hieraus ließen sich Reaktions- und Präventionskonzepte für die Sicherheitsbehörden und die Sicherheitspolitik ableiten.

Die Sicherheitswirtschaft leistet mit ihren rund 290.000 Beschäftigten im Inland einen immer wichtigeren und unverzichtbaren Beitrag zur Sicherheit in Deutschland. Ihren Stellenwert als Sicherheitsakteur gilt es zu stärken. Nach wie vor fehlt aber eine klare gesetzliche Regelung, die sicherstellt, dass die Sicherheitswirtschaft auch in Krisen, Notfällen und Katastrophenzeiten als privilegiert und damit systemrelevant eingestuft wird und ungehindert ihren KRITIS-Schutzaufgaben nachgehen kann. Hierzu ist eine bundesweite rechtliche Verankerung der Systemrelevanz des Sicherheitsgewerbes erforderlich.

Die Sicherheitswirtschaft sollte aber zugleich auch als strategischer Sicherheitspartner seitens der Bundesregierung anerkannt und mehr in Themen der öffentlichen Sicherheit und Wirtschaftssicherheit einbezogen werden. Nur mit einer starken Sicherheitswirtschaft wird man im Zusammenwirken mit Staat und Gesellschaft in Zeiten zunehmender Bedrohungen Deutschland dauerhaft sicher halten und resilienter machen können.

KURZ BELICHTET

Risiko- und Krisenmanagement für KRITIS-Betreiber unter besonderer Berücksichtigung der Zivilen Verteidigung

Zu diesem Thema bot der BDSW seinen Mitgliedern am 13. Juni 2025 in Kooperation mit der Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung (BAKZ) im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ein Webinar an. Bei diesem wurden unter Moderation von BDSW-GF, Dr. Berthold Stoppelkamp durch ReferentInnen des BAKZ/BBK unter Federführung von Herrn Dr. Dr. Dirk Freudenberg (oben links) den rund 50 TeilnehmerInnen die aktuellen Themen Gesamtverteidigung, die Rahmenrichtlinien für die Gesamtverteidigung und Zivile Verteidigung, Zivil-Militärische Zusammenarbeit und die Rolle und Bedeutung der Sicherheitsunternehmen bzw. der Wirtschaft nahegebracht. Ebenso wurden Fragen mit besonderer Relevanz für die Sicherheitswirtschaft beantwortet.

Kontinuität im Zeichen des Wirtschaftsschutzes

Im Rahmen der Sitzung des BDSW-Fachausschusses Wirtschaftsschutz am 26. Juni 2025 wurde Holger Köster, Geschäftsführer der HERSA-Unternehmensgruppe, als Vorsitzender in seinem Amt bestätigt. Auch sein Stellvertreter Dirk H. Bürhaus, Geschäftsführender Direktor der KÖTTER Security Gruppe, wurde von den Ausschussmitgliedern erneut gewählt. Der BDSW-Fachausschuss Wirtschaftsschutz setzt sich für den Schutz unternehmensrelevanter Infrastrukturen, für Resilienz gegenüber hybriden Bedrohungen sowie für die Förderung strategischer Sicherheitskooperationen zwischen Wirtschaft und Staat ein. Er ist ein zentrales Gremium, in dem Praxis, Fachwissen und Zukunftsverantwortung aufeinandertreffen. Dabei versteht sich der Ausschuss als Brücke zwischen Sicherheitswirtschaft, staatlichen Sicherheitsbehörden und weiteren Institutionen mit dem Ziel, Synergien zu schaffen und den Wirtschaftsstandort Deutschland nachhaltig zu sichern.

(v.r.) Dirk H. Bürhaus, Holger Köster und Dr. Berthold Stoppelkamp

Bekämpfung der Cyberkriminalität

Die Bedrohungslage im Bereich Cyberkriminalität ist anhaltend hoch. Deutschland steht mehr denn je im Fokus von Cyberkriminellen. Im Jahre 2024 wurden hierzulande über 131.000 Cybercrime-Fälle erfasst. Hinzu kommen über 200.000 Auslandstaten, die aus dem Ausland oder von einem unbekannten Ort aus verübt wurden. Im Rahmen der Veranstaltungsreihe „Basecamp Nachgefragt!“ referierte BKA-Präsident Holger Münch (rechts) am 8. Juli 2025 in Berlin zu aktuellen Bedrohungen, polizeilichen Strategien und Erfolgen bei der Bekämpfung von Cyberkriminalität und stand den Teilnehmern Rede und Antwort.

Bild: © BASECAMP, Henrik Andree

EU Preparedness Union: CoESS engagiert sich in EU-Initiative zur besseren Vorsorge für Notlagen

Von Alexander Frank

Alexander Frank

Stellvertretender Generaldirektor der CoESS – Confederation of European Security Services

www.coess.eu

Europa steht an einem entscheidenden Punkt in Fragen der Sicherheit und Krisenvorsorge. Die im März 2025 vorgestellte EU-Strategie zur Preparedness Union soll daher eine neue Kultur der Bereitschaft fördern, die Bürger, Unternehmen und Mitgliedstaaten befähigt, Krisen vorzubeugen und im Ernstfall schnell sowie koordiniert zu reagieren. Für die Sicherheitswirtschaft bedeutet diese Entwicklung nicht nur neue Verantwortung, sondern auch die längst überfällige Anerkennung durch die öffentliche Hand.

Die europäische Sicherheitslage ist so ernst wie selten zuvor: terroristische Bedrohungen, physische, cyber- und hybride Angriffe auf Kritische Infrastrukturen, der russische Krieg gegen die Ukraine und zunehmend schwerwiegende Naturkatastrophen schaffen ein volatiles Bedrohungsumfeld. Diese komplexe Situation erfordert, dass Staaten jederzeit bereit sind, Bürger, Volkswirtschaften und die für Demokratie und Alltag unerlässlichen gesellschaftlichen Funktionen zu schützen. Die neuen Realitäten verlangen ein höheres Maß an Vorsorge – und damit einen

Bild: Chris Gallagher / unsplash.com

tiefgreifenden Mentalitätswandel aller Akteure in öffentlicher Sicherheit, Katastrophenschutz, Krisenmanagement und KRITIS. Bürger, Mitgliedstaaten und Unternehmen benötigen die richtigen Instrumente, um Krisen zu verhindern und im Ernstfall rasch zu reagieren.

Die EU Preparedness Union

Vor diesem Hintergrund präsentierte die Europäische Kommission im März 2025 ihre EU-Strategie für eine krisenfeste Union (Preparedness Union) – ein ehrgeiziger Rahmen zur Stärkung der Resilienz Europas. Ein Großteil der öffentlichen Aufmerksamkeit galt dem „72-Stunden-Notfallpaket" – einer Empfehlung, dass jeder Haushalt in der Lage sein sollte, sich bei einem Notfall drei Tage lang selbst zu versorgen.

Doch die Strategie enthält weit mehr als nur Haushaltsempfehlungen. Sie baut auf der umfangreichen Analyse des Niinistö-Berichts zu Vorsorge und Einsatzbereitschaft (2024) auf, der dringendes Handeln zur Stärkung der Kapazitäten Europas in mehreren Bereichen – u. a. Gesundheit, Sicherheit, Technologie, Klima und Verteidigung – forderte. Die CoESS wurde früh in den Prozess einbezogen, um sicherzustellen, dass die Stimme der Sicherheitswirtschaft Gehör findet.

Die Strategie der EU-Kommission folgt einem integrierten „All-Hazards"-Ansatz und bindet Akteure auf allen Ebenen ein – von lokalen Behörden bis zur EU – sowie Bürger, Wirtschaft, Sozialpartner und Wissenschaft. Roxana Mînzatu, Exekutiv-Vizepräsidentin der Kommission, betonte: *„Diese Strategie ist auf die Menschen und die Gesellschaft ausgerichtet und soll dafür sorgen, dass im Krisenfall alles nach Plan läuft und wir darauf vorbereitet sind, rasch und wirksam zu handeln. Dafür müssen wir die Krisenvorsorge in neuem Licht sehen, damit jeder weiß, was in Notfällen zu tun ist, und zwar unabhängig von der Art des Notfalls. Europa muss flexibel handeln und eng mit den Mitgliedstaaten zusammenarbeiten, um die Effizienz zu steigern, Zeit zu sparen und Leben zu retten. Diese Strategie ist unsere Versicherungspolice, sodass wir für die Menschen in der EU da sind, wenn sie es am dringendsten benötigen."*

Viele angekündigte Maßnahmen betreffen auch die Sicherheitswirtschaft:

- EU-weite Weiterbildungsprogramme in den Bereichen Sicherheit, Verteidigung und Krisenmanagement
- Zusammenarbeit mit Sozialpartnern zur Attraktivitätssteigerung von Berufen in der Sicherheit und im Katastrophenschutz samt Sozialpartnergipfel
- Verbesserter Informationsaustausch zwischen öffentlichen und privaten Akteuren sowie gemeinsame Übungen, koordinierte Krisenreaktion und ein EU-Notfallprotokoll für öffentlich-private Zusammenarbeit
- Einrichtung einer EU-Vorsorge-Taskforce zur Sicherung der Kontinuität kritischer Dienste


Bild: Nicolas HIPPERT / unsplash.com

Die Rolle der Sicherheitswirtschaft

Die CoESS wird im Rahmen dieser Initiativen mit den EU-Institutionen zusammenarbeiten, um die Empfehlungen der Sicherheitswirtschaft einzubringen. In Europa schützen zwei Millionen private Sicherheitskräfte Bürger, sichern Veranstaltungen, bewachen Kritische Infrastrukturen und unterstützen Strafverfolgungsbehörden und Notfalldienste rund um die Uhr. Sie sind wesentlicher Bestandteil der Sicherheits- und Krisenreaktionssysteme.

Im heutigen, sich schnell verändernden Bedrohungsumfeld sind Sicherheitsdienstleistungen längst nicht mehr auf traditionelle Bewachungsaktivitäten beschränkt. Die Branche setzt zunehmend auf moderne Technologien wie KI, Drohnen und integrierte physische und cyberbasierte Risikomanagementsysteme, um Sicherheit zu erhöhen und Resilienz im öffentlichen wie privaten Sektor zu unterstützen. Diese Fähigkeiten bilden eine entscheidende Verteidigungslinie gegen Terrorismus, organisierte Kriminalität, Sabotage, Spionage und Katastrophenlagen.

In einigen Ländern wird die Bedeutung der Sicherheitswirtschaft in der Krisenvorsorge zunehmend anerkannt. In Schweden laufen Diskussionen über die Rolle der Branche beim Schutz kritischer Dienste, sollte sich die Lage im Ostseeraum verschärfen. An anderer Stelle haben private Sicherheitskräfte in vielen Ländern Notfallmaßnahmen bei Terroranschlägen, Ausfällen kritischer Dienste oder Naturkatastrophen wie schweren Überschwemmungen oder auch der COVID-19-Pandemie unterstützt.

Allerdings ist diese Anerkennung in der EU nicht einheitlich. In vielen Mitgliedstaaten wird die Sicherheitswirtschaft in die Krisenplanung nicht miteinbezogen; Innovation wird durch regulatorische Hürden gebremst – insbesondere bei Drohnen und C-UAS.

Empfehlungen der CoESS an die EU

Bei einer jüngsten hochrangigen Veranstaltung in Brüssel mit der Europäischen Kommission und Mitgliedern des Europäischen Parlaments präsentierte die CoESS daher konkrete Empfehlungen an die EU:

- Zusammenarbeit mit der CoESS zur Stärkung der Einsatzbereitschaft von Arbeitskräften und Förderung von Karrieren in der Sicherheitsbranche
- Förderung von Sicherheitsinnovation durch intelligente Industriepolitik, die Investitionen in Technologien erleichtert, regulatorische Unsicherheiten abbaut und die Kontinuität kritischer Dienstleistungen gewährleistet
- Einbindung der Sicherheitswirtschaft in sicheren Informationsaustausch, Risikoanalysen sowie in die Gestaltung EU-weiter Notfallprotokolle und Kontinuitätspläne
- Modernisierung des Vergaberechts zur Unterstützung von Qualitätskontrolle, hochwertige Arbeitsplätze, Technologieintegration und Resilienz – insbesondere durch Nutzung von Normen wie der EN 17483 bei der Umsetzung der CER-Richtlinie

Ausblick

Die Preparedness Union wird ein zentrales Thema der Arbeit der CoESS bleiben, mit aktiver Beteiligung ihrer Ausschüsse und Mitglieder wie dem BDSW. Ziel ist, dass nationale Behörden einen gesamtgesellschaftlichen Ansatz zur Krisenvorsorge übernehmen und die Kapazitäten der Sicherheitswirtschaft zum Wohle aller bei der Vorbereitung und im Krisenfall effizient ausschöpfen.

Dies erfordert echtes Engagement, formalisierte Partnerschaften, strukturierten Informationsaustausch und gemeinsame Vorsorgemaßnahmen. Denn Vorsorge ist nicht länger optional – sie ist Europas Versicherung für die Zukunft.


Bild: Dmytro Tolokonov / unsplash.com

Arbeitsrecht in Kürze

Von Rechtsanwältin Cornelia Okpara

RAin Cornelia Okpara

Hauptgeschäftsführerin des Bundesverbandes der Sicherheitswirtschaft (BDSW)

Befristetes Arbeitsverhältnis eines Betriebsratsmitglieds – Benachteiligungsverbot

Bundesarbeitsgericht, Urteil vom 18. Juni 2025 – 7 AZR 50/24 –

Ein nach Maßgabe des Teilzeit- und Befristungsgesetzes zulässig befristetes Arbeitsverhältnis endet auch dann mit Ablauf der vereinbarten Befristung, wenn der Arbeitnehmer zwischenzeitlich in den Betriebsrat gewählt worden ist. Benachteiligt der Arbeitgeber allerdings das befristet beschäftigte Betriebsratsmitglied, indem er diesem wegen des Betriebsratsmandats keinen Folgevertrag anbietet, hat das Betriebsratsmitglied einen Anspruch auf den Abschluss des verweigerten Folgevertrags als Schadensersatz.

Die beklagte Arbeitgeberin erbringt logistische Dienstleistungen. Sie schloss mit dem Kläger Anfang des Jahres 2021 einen zunächst auf ein Jahr befristeten Arbeitsvertrag, welcher später um ein weiteres Jahr bis zum 14. Februar 2023 verlängert wurde. Im Sommer 2022 wurde der Kläger in den Betriebsrat gewählt. Von 19 Arbeitnehmern der Beklagten, die einen am 14. Februar 2023 auslaufenden befristeten Arbeitsvertrag hatten, erhielten 16 das Angebot auf Abschluss eines unbefristeten Arbeitsvertrags. Der Kläger erhielt dieses Angebot nicht. Mit seiner Klage hat er sich gegen die Wirksamkeit der Befristung gewandt und hilfsweise die Verurteilung der Beklagten zum Abschluss eines unbefristeten Arbeitsvertrags ab dem 15. Februar 2023 zu den bisherigen Bedingungen verlangt. Er hat geltend gemacht, die unterbliebene „Entfristung" seines Arbeitsverhältnisses beruhe allein auf seiner Mitgliedschaft im Betriebsrat. Zwar habe die Beklagte mit anderen Betriebsratsmitgliedern unbefristete Arbeitsverträge geschlossen, diese hätten aber anders als der Kläger nicht auf der Gewerkschaftsliste für den Betriebsrat kandidiert. Die Beklagte hat sich demgegenüber darauf berufen, sie sei mit der Arbeitsleistung und dem persönlichen Verhalten des Klägers nicht so zufrieden gewesen, dass sie das Arbeitsverhältnis habe unbefristet fortführen wollen. Die Betriebsratstätigkeit des Klägers habe bei ihrer Entscheidung keine Rolle gespielt.

Die Vorinstanzen haben die Befristung des Arbeitsvertrags als wirksam angesehen und das unterlassene Angebot eines unbefristeten Folgevertrags nicht auf das Betriebsratsamt des Klägers zurückgeführt. Die hiergegen gerichtete Revision des Klägers hatte vor dem Siebten Senat des Bundesarbeitsgerichts keinen Erfolg. Der Senat hat seine Entscheidungen vom 5. Dezember 2012 und vom 25. Juni 2014 bestätigt, wonach die Wahl eines befristet beschäftigten Arbeitnehmers in den Betriebsrat keine Unwirksamkeit der Befristung bedingt. Eine solche Annahme ist auch durch das Recht der Europäischen Union nicht zwingend vorgegeben. Das einzelne Betriebsratsmitglied ist durch die Vorschrift des § 78 Satz 2 Betriebsverfassungsgesetz (BetrVG), wonach es in der Ausübung seiner Tätigkeit nicht gestört oder behindert werden darf, hinreichend geschützt. Im vorliegenden Fall hat sich das Landesarbeitsgericht im Zusammenhang mit der Abweisung des Schadensersatzanspruchs in revisionsrechtlich nicht zu beanstandender Weise unter Würdigung des wechselseitigen Vortrags der Parteien die Überzeugung gebildet, dass die Beklagte dem Kläger den Abschluss eines unbefristeten Folgevertrags nicht wegen dessen Betriebsratstätigkeit verweigert hatte.

Kein Urlaubsverzicht durch Prozessvergleich

Bundesarbeitsgericht, Urteil vom 3. Juni 2025 – 9 AZR 104/24 –

Im bestehenden Arbeitsverhältnis kann ein Arbeitnehmer selbst durch gerichtlichen Vergleich nicht auf seinen gesetzlichen Mindesturlaub „verzichten".

Die Parteien streiten über die Abgeltung von sieben Tagen gesetzlichen Mindesturlaubs aus dem Jahr 2023. Der Kläger war bei der Beklagten vom 1. Januar 2019 bis zum 30. April 2023 als Betriebsleiter beschäftigt. Im Jahr 2023 war er von Beginn an bis zur Beendigung seines Arbeitsverhältnisses durchgehend arbeitsunfähig erkrankt und deshalb nicht in der Lage, seinen Urlaub aus diesem Jahr in Anspruch zu nehmen.

In einem gerichtlichen Vergleich vom 31. März 2023 verständigten sich die Parteien u. a. darauf, dass das zwischen ihnen bestehende Arbeitsverhältnis gegen Zahlung einer Abfindung iHv. 10.000,00 Euro durch arbeitgeberseitige Kündi-

gung zum 30. April 2023 endet. Ziffer 7 des Vergleichs lautet: „Urlaubsansprüche sind in natura gewährt." In der dem Vergleichsschluss vorausgehenden Korrespondenz zwischen den Parteien hat die Prozessbevollmächtigte des Klägers ausdrücklich darauf hingewiesen, dass auf den gesetzlichen Mindesturlaub nicht wirksam verzichtet werden könne, sich später aber unter Hinweis auf die geäußerten rechtlichen Bedenken gleichwohl mit dem Vergleich einverstanden erklärt.

Mit seiner Klage hat der Kläger von der Beklagten verlangt, die noch offenen sieben Tage gesetzlichen Mindesturlaubs aus dem Jahr 2023 mit einem Betrag iHv. 1.615,11 Euro nebst Zinsen abzugelten. Der im gerichtlichen Vergleich geregelte Verzicht auf den unabdingbaren Mindesturlaub sei unwirksam. Die Vorinstanzen haben der Klage stattgegeben. Der Neunte Senat des Bundesarbeitsgerichts hat die Revision der Beklagten – mit Ausnahme eines geringfügigen Teils der Zinsforderung – zurückgewiesen.

Der Kläger hat gemäß § 7 Abs. 4 BUrlG Anspruch auf Abgeltung seines nicht erfüllten gesetzlichen Mindesturlaubs aus dem Jahr 2023. Der Urlaubsanspruch ist nicht durch Ziffer 7 des Prozessvergleichs vom 31. März 2023 erloschen. Die Vereinbarung, Urlaubsansprüche seien in natura gewährt, ist gemäß § 134 BGB unwirksam, soweit sie einen nach § 13 Abs. 1 Satz 3 BUrlG unzulässigen Ausschluss des gesetzlichen Mindesturlaubs regelt. Weder der gesetzliche Anspruch auf bezahlten Erholungsurlaub noch ein erst künftig – mit der rechtlichen Beendigung des Arbeitsverhältnisses – entstehender Anspruch auf Abgeltung gesetzlichen Mindesturlaubs darf im Voraus ausgeschlossen oder beschränkt werden. Dies gilt selbst dann, wenn bei Abschluss eines gerichtlichen Vergleichs, der eine Beendigung des Arbeitsverhältnisses gegen Zahlung einer Abfindung regelt, bereits feststeht, dass der Arbeitnehmer den gesetzlichen Mindesturlaub wegen krankheitsbedingter Arbeitsunfähigkeit nicht mehr in Anspruch nehmen kann. Der bezahlte Mindesturlaub darf nach Art. 7 Abs. 2 der Richtlinie 2003/88/EG des Europäischen Parlaments und des Rates vom 4. November 2003 über bestimmte Aspekte der Arbeitszeitgestaltung außer bei Beendigung des Arbeitsverhältnisses nicht durch eine finanzielle Vergütung ersetzt werden. Im bestehenden Arbeitsverhältnis darf der Arbeitnehmer somit nicht gegen und erst recht nicht ohne finanziellen Ausgleich auf den gesetzlichen Mindesturlaub „verzichten".


Bild: djedzura / istockphoto.com

Der Prozessvergleich enthält keinen Tatsachenvergleich, auf den § 13 Abs. 1 Satz 3 BUrlG nicht anzuwenden wäre. Ein solcher setzt voraus, dass eine bestehende Unsicherheit über die tatsächlichen Voraussetzungen eines Anspruchs durch gegenseitiges Nachgeben ausgeräumt werden soll. Angesichts der seit Anfang des Jahres 2023 durchgehend bestehenden Arbeitsunfähigkeit des Klägers bestand vorliegend kein Raum für eine Unsicherheit über die tatsächlichen Voraussetzungen des Urlaubsanspruchs.

Der Einwand der Beklagten, dem Kläger sei es nach Treu und Glauben verwehrt, sich auf die Unwirksamkeit des Anspruchsausschlusses zu berufen, blieb erfolglos. Die Beklagte durfte nicht auf den Bestand einer offensichtlich rechtswidrigen Regelung vertrauen.

Konzepte in der Angebotswertung – welche Überprüfungsmöglichkeiten bestehen?

VK Südbayern, Beschluss vom 6. August 2024 – 3194.Z3-3_01-24-26

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.

Sachverhalt

Der Auftraggeber (AG) schreibt Sicherheitsdienstleistungen für staatliche Gemeinschaftsunterkünfte für Asylbewerber aus. Als Zuschlagskriterien werden der Preis und die Qualität benannt. Hinsichtlich der Qualitätsbewertung gibt der Auftraggeber vor: „Für die Bewertung der Qualität der vom Bieter angebotenen Leistungen soll der Bieter ein Konzept zur Durchführung der Bewachungsleistungen vorlegen. Dieses Konzept wird anhand der nachfolgend dargestellten Unterkriterien bewertet."

Der AG benennt insgesamt drei Unterkriterien mit Gewichtung. Er macht Vorgaben hinsichtlich Seitenzahl, Schriftart, Schriftgröße und Zeilenabstand und formuliert konkrete Fragen zu jedem Unterkriterium. Der AG legt dar, unter welchen Voraussetzungen wie viele Punkte für die Konzepte vergeben werden. Nach einer entsprechenden Bieterfrage wurde allen Bietern ein bearbeitbares PDF-Dokument „Ausführungen zu Zuschlagskriterien" zur Verfügung gestellt. Ein nicht berücksichtigter Bieter wendet sich nach der Vorinformation gemäß § 134 GWB und der Nichtabhilfe seiner Rüge wegen fehlerhafter Bewertungen der Konzepte an die Vergabekammer (VK).

Entscheidungsgründe

Die VK gibt dem AG auf, die Angebotswertung unter Berücksichtigung der Hinweise der VK zu wiederholen. Die VK verweist zunächst darauf, dass einzelne Angriffe aus der Rüge präkludiert sind. Diese bezogen sich auf Formulierungen in der Bewertungsmatrix, die nach Auffassung des Bieters nicht eindeutig verständlich waren. Die VK weist darauf hin, dass aus den Vergabeunterlagen erkennbare Verstöße bis zum Ablauf der Frist für die Angebotsabgabe zu rügen sind. Für diese Erkennbarkeit genügt die laienhafte rechtliche Bewertung, dass etwas nicht stimmt, wobei keine übersteigerten Erwartungen an den Bieter zu stellen sind. Bei offensichtlich ins Auge fallenden Rechtsverstößen, die einem Bieter bei der bloßen Durchsicht der Vergabeunterlagen auffallen bzw. sich ihm aufdrängen müssen, kommt eine Präklusion der Rüge in Betracht. Die Ausführungen zur Konzeptbewertung wären von einem durchschnittlichen und fachkundigen Bieter unter Anwendung der üblichen Sorgfalt bei Erstellung der Konzepte erkennbar gewesen. Bei inhaltlichen Unklarheiten im Hinblick auf Begriffsdefinitionen hätte eine entsprechende Bieterfrage oder Rüge schon bei Erstellung der Konzepte formuliert werden können und müssen.

Bild: # 131989300 / istockphoto.com

Im Übrigen ist der Nachprüfungsantrag jedoch zulässig und begründet. Die VK führt aus, dass die auf Grundlage des Formblattes „Gewichtung der Zuschlagskriterien" durchgeführte Angebotswertung einer Nachprüfung nicht standhält. Die VK stellt fest, dass die Konzeptbewertung nicht für alle Bieter einheitlich und diskriminierungsfrei erfolgt ist. Dem AG steht bei Prüfung und Bewertung der Angebote ein Beurteilungsspielraum zu. Die Nachprüfungsinstanzen können diese Entscheidung nur daraufhin kontrollieren, ob das vorgeschriebene Verfahren eingehalten, von einem zutreffend und vollständig ermittelten Sachverhalt ausgegangen wurde, keine sachwidrigen Erwägungen in die Entscheidung eingeflossen sind und allgemeingültige Bewertungsmaßstäbe beachtet wurden. Dies setzt voraus, dass die Wertung anhand der aufgestellten Zuschlagskriterien vertretbar, in sich konsistent und in diesem Sinne nachvollziehbar ist. Der Nachvollziehbarkeit komme im Rahmen des Nachprüfungsverfahrens besondere Bedeutung zu und sie sei eng mit der gesetzlich statuierten Dokumentationspflicht verbunden. Für die Nachprüfungsinstanzen muss nachverfolgbar sein, warum das ausgewählte Angebot als das wirtschaftlichste bewertet wurde. Die Gründe müssen so detailliert sein, dass ein mit dem Vergabeverfahren vertrauter Leser sie als fassbar erachtet.

Dabei ist es nicht notwendig, dass die jeweilige Nachprüfungsinstanz zu dem gleichen inhaltlichen Ergebnis kommt, da der Konzeptbewertung auch immer ein subjektives Element innewohnt.

Die VK wendet folgendes Prüfungsschema an: Auf einer 1. Stufe wird geprüft, ob der AG das von ihm selbst gewählte Bewertungsverfahren eingehalten hat. Auf der 2. Stufe wird geprüft, ob der Bewertung ein vollständig ermittelter Sachverhalt zugrunde gelegt wurde, ob also alle Angaben aus dem eingereichten Konzept berücksichtigt wurden und eine umfassende Auseinandersetzung stattfand. Auf der 3. Stufe wird beurteilt, ob die vom AG vorgenommene Bewertung nachvollziehbar ist, die vorgegebene Zielsetzung und den Erwartungshorizont berücksichtigt und den abstrakten Bewertungsmaßstab konkret ausfüllt. Im Rahmen dieses Prüfungspunktes kommt der Dokumentation tragende Bedeutung zu. Die VK prüft, welche Angaben der AG aus den Konzepten positiv und welche negativ bewertet hat, wie der AG seine Bewertung begründet hat und ob eine Subsumtion unter den abstrakten Bewertungsmaßstab vorgenommen worden ist. Auf der 4. Stufe wird beurteilt, ob ein Quervergleich mit der Bewertung anderer Bieter einer vergaberechtlichen Nachprüfung standhält, ob also die Bewertung einheitlich und diskriminierungsfrei durchgeführt wurde und Unterschiede in der Bewertung überzeugend und nachvollziehbar begründet wurden. Im konkreten Fall stellt VK Fehler bei der Ermittlung des Wertungspreises fest, da einzelne Preiskriterien nicht so berücksichtigt worden sind, wie dies zuvor angegeben wurde. Darüber hinaus ergäbe sich aus der Dokumentation nicht, dass die formellen Vorgaben zur Erstellung der Konzepte bei der Wertung berücksichtigt worden seien. Es fehle an einer Dokumentation, ob und wie sich ein Verstoß gegen die formellen Vorgaben auf die Angebotswertung auswirke. Es sei auch nicht erkennbar, dass die Einhaltung dieser Vorgaben geprüft worden sei. Der für den Zuschlag vorgesehene Bieter hatte in sein Konzept Abbildungen mit textlichen Ausführungen eingefügt, die die Vorgaben hinsichtlich Schriftart, Schriftgröße und Zeilenabstand nicht berücksichtigten.

Im Rahmen einer transparenten und gleichbehandelnden Konzeptbewertung wären auch diese formellen Vorgaben jedoch zu berücksichtigen gewesen. Bei Nichtbeachtung der Vorgaben war es möglich, mehr Informationen im Konzept unterzubringen als Wettbewerber.

Im konkreten Fall war es so, dass die mit zusätzlichen Informationen versehenen Abbildungen im Rahmen der Bewertung positiv berücksichtigt worden sind, wodurch eine Benachteiligung des nicht berücksichtigten Bieters vorlag. Die Angebotswertung war zu wiederholen.

Praxishinweise

Die Entscheidung zeigt auf, wie die Überprüfung einer Konzeptbewertung vorgenommen werden kann. Die Entscheidung des AG ist zwar nicht durch eine Entscheidung der VK zu ersetzen, sie ist dennoch voll überprüfungsfähig. Ist die Entscheidung nicht nachvollziehbar, z. B. weil selbst aufgestellte Kriterien keine Berücksichtigung gefunden haben, ist die Bewertung zu wiederholen. Der Auftraggeber muss sich zu formalen Kriterien, die er formuliert, auch Gedanken über die Wertung machen. Im vorliegenden Fall waren formale Vorgaben aufgestellt worden, es lag jedoch keine Festlegung dazu vor, wie mit Abweichungen von diesen Vorgaben umgegangen werden soll. Die Entscheidung macht auch deutlich, dass der Bieter gehalten ist, die Wertungsvorgaben bereits vor Abgabe der Angebote kritisch zu prüfen. Diese Unklarheiten sind vor Abgabe der Angebote zu rügen, zu einem späteren Zeitpunkt, u. a. wenn die Wertung nicht im Sinne des Bieters ausgefallen ist, sind Beanstandungen nicht mehr zulässig.

Cornelia Okpara zur Hauptgeschäftsführerin des BDSW berufen


Cornelia Okpara

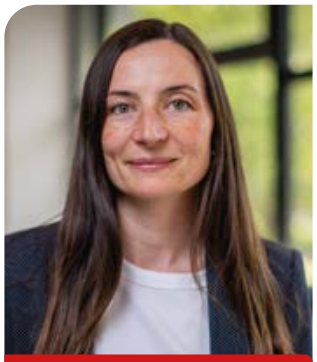
Das neue BDSW-Präsidium setzt auf Erfahrung, Kontinuität sowie Sachorientierung und beruft Cornelia Okpara zur neuen Hauptgeschäftsführerin. Nachdem sie zum zweiten Mal innerhalb weniger Jahre die kommissarische Geschäftsführung für den Verband übernommen hatte, hat das im Mai neu gewählte Präsidium in seiner ersten Sitzung beschlossen, Okpara dauerhaft mit der Hauptgeschäftsführung zu betrauen. „Mit dieser Entscheidung setzt der Verband ein klares Zeichen für Kontinuität, fachliche Kompetenz und eine konzentrierte Sacharbeit", so BDSW-Präsident Werner Landstorfer.

Cornelia Okpara ist seit 31 Jahren für den BDSW tätig und hat in dieser Zeit die Verbandsarbeit in der Sicherheitswirtschaft maßgeblich mitgestaltet. Seit 2013 war sie stellvertretende Hauptgeschäftsführerin und 2022 sowie seit Mitte 2024 kommissarische Hauptgeschäftsführerin des Verbandes. Die Volljuristin ist Expertin für Tarifpolitik und betreut seit vielen Jahren federführend die Landesgruppen Bremen, Hamburg, Niedersachsen und Nordrhein-Westfalen sowie mehrere Fachausschüsse des Verbandes.

„Die Entscheidung für Cornelia Okpara basiert auf ihrer langjährigen Erfahrung, ihrem großen juristischen Sachverstand und ihrer ausgewiesenen Führungsstärke", so BDSW-Präsident Werner Landstorfer. Sie sei eine hochgeschätzte Persönlichkeit innerhalb und außerhalb des Verbandes und stehe für Verlässlichkeit, Sachlichkeit und den Ausgleich unterschiedlicher Interessen.

Mit der Berufung von Cornelia Okpara will der BDSW die anstehenden Herausforderungen in der Sicherheitswirtschaft mit Klarheit und strategischem Fokus angehen. „Nach einer Phase der Unruhe setzen wir jetzt auf Stabilität und inhaltliche Arbeit – Frau Okpara ist dafür die ideale Besetzung", so Landstorfer abschließend.

Funktionserweiterung von Silke Zöller in der BDGW als Leiterin der Kommunikations- und Öffentlichkeitsarbeit


Silke Zöller

Der Vorstand der BDGW hat in seiner letzten Sitzung am 24. Juni 2025 beschlossen, die Funktion der Pressesprecherin zur Leiterin der Kommunikations- und Öffentlichkeitsarbeit auszubauen. Mit dieser Entscheidung würdigt der Vorstand die langjährige, engagierte und erfolgreiche Arbeit von Silke Zöller, die bisher als Pressesprecherin für die BDGW tätig war.

Die BDGW unterstreicht mit dieser Entscheidung die strategische Bedeutung einer wirkungsvollen und professionellen Kommunikations- und Öffentlichkeitsarbeit nach innen und außen.

Ziel ist es, die Position der Bargeldversorgung in der öffentlichen Wahrnehmung weiter zu stärken und Bargeld auch künftig als sicheres, verlässliches und attraktives Zahlungsmittel zu positionieren. Angesichts der derzeitigen Entwicklungen – darunter zunehmender politischer und gesellschaftlicher Druck zur Einschränkung von Bargeldzahlungen, eine wachsende Zahl an Geschäftsstellenaufgaben im Bankensektor, sowie infrastrukturelle Herausforderungen bei der flächendeckenden Bargeldverfügbarkeit – ist eine strategisch ausgerichtete Kommunikation von zentraler Bedeutung.

Die BDGW wird sich daher weiterhin mit Nachdruck dafür einsetzen, den hohen Stellenwert des Bargelds für breite Bevölkerungsschichten sichtbar zu machen, faktenbasiert über dessen Vorteile aufzuklären und die Bedeutung einer verlässlichen Bargeldlogistik als Teil der öffentlichen Daseinsvorsorge zu betonen.

BDSW-Landesgruppe Bayern wählt und erweitert Vorstand

Die Mitgliederversammlung BDSW-Landesgruppe Bayern hat ihren Vorstand neu gewählt und erweitert. Der wiedergewählte Vorsitzende, Werner Landstorfer, wird zukünftig von fünf Stellvertretern unterstützt. Ebenfalls wiedergewählt wurden die bisherigen Stellvertreter Gerhard Ameis, Vorsitzender der Geschäftsführung der Nürnberger Wach- und Schließgesellschaft mbH, Andreas Schade, Geschäftsführer der Munich Security Services GmbH, Rüdiger Schulz, Geschäftsführer der WISAG Sicherheit & Service Bayern GmbH & Co. KG sowie Klaus Winkler, Prokurist der VSU Vereinigte Sicherheitsunternehmen GmbH. Neu in den Vorstand gewählt wurde Lars Homann, Geschäftsführender Direktor der KÖTTER SE & Co. KG Security, München.

Werner Landstorfer, seit Mai Präsident des Bundesverbandes, ist bereits seit 2016 Mitglied im Landesgruppenvorstand und wurde 2022 zum Vorsitzenden gewählt. „Ich freue mich, erneut als Landesgruppenvorsitzender die Interessen der bayerischen Sicherheitsunternehmen vertreten zu dürfen, und bedanke mich für das mir und der Arbeit des gesamten Landesgruppenvorstandes entgegengebrachte Vertrauen", so Landstorfer im Nachgang der Versammlung.

Sicherheitspartnerschaft zwischen der Polizeidirektion Hannover und der BDSW-Landesgruppe Niedersachsen

Die teilnehmenden Sicherheitsunternehmen der BDSW-Landesgruppe Niedersachsen, die in der Sicherheitspartnerschaft zwischen der Polizeidirektion Hannover und der BDSW-Landesgruppe Niedersachsen engagiert sind, haben ihre Absicht zum Jahresanfang 2025 bekräftigt, diese Kooperation aktiv zu unterstützen. Diese bewährte Zusammenarbeit besteht bereits seit 2007 und verfolgt das Ziel, die Sicherheitslage in der Region Hannover nachhaltig zu stärken.

Dabei geht es vor allem um die Verhütung von Straftaten sowie um den Schutz der öffentlichen Sicherheit und Ordnung im öffentlichen Raum. Das Hauptziel dieser Partnerschaft ist es, die Sicherheit der Bürgerinnen und Bürger in Hannover zu erhöhen, Kriminalität wirksam vorzubeugen und Gefahren frühzeitig zu erkennen. Ein wichtiger Aspekt ist dabei, das Risiko für Straftäter zu erhöhen, also es für sie schwieriger zu machen, Straftaten unbemerkt zu begehen. Zudem soll der Informationsaustausch zwischen Polizei und Sicherheitsunternehmen verbessert werden, um sicherheitsrelevante Umstände schneller zu erkennen und zu melden.

Die BDSW-Landesgruppe Niedersachsen ist sich ihrer Verantwortung bewusst, zur Sicherheit in der Region beizutragen. Das Motto der Vereinbarung lautet „Beobachten, Erkennen, Melden". Sicherheitskräfte der beteiligten Mitgliedsunternehmen sammeln im Rahmen ihrer Arbeit vielfältige Informationen, die für die Polizei von Bedeutung sein können – sei es im Zusammenhang mit Straftaten, Ordnungswidrigkeiten oder Gefahren für die öffentliche Sicherheit.

Der BDSW ist bereit, bei der Erstellung eines umfassenden Sicherheitslagebildes mitzuwirken. Dabei stellen die beteiligten Sicherheitsunternehmen ihre Erkenntnisse der Polizei zur Verfügung und informieren sie über besondere Feststellungen. Im Gegenzug erstellt die Polizeidirektion Hannover ebenfalls ein Sicherheitslagebild und teilt es mit dem BDSW, soweit dies notwendig ist, um die Interessen der Unternehmen, der Polizei oder das öffentliche Interesse zu wahren.

Insgesamt zeigt diese Partnerschaft, wie wichtig die Zusammenarbeit zwischen Polizei und Sicherheitswirtschaft ist, um die Sicherheit in Hannover nachhaltig zu stärken.

Rheinland-Pfalz/Saarland – Landesgruppenvorstand im Amt bestätigt

Die Mitglieder der BDSW-Landesgruppe Rheinland-Pfalz/Saarland haben sowohl den Vorsitzenden Tobias Stamper, Geschäftsführer der Securitas Sicherheitsdienste GmbH, als auch Nora Rauch, Geschäftsführerin der VSU Brandschutz Mainz GmbH, und Hans Jürgen Rössner, Referent der Geschäftsführung der Pond Security Service GmbH, als stellvertretende Vorsitzende im Amt bestätigt.

Stamper, Rauch und Rössner haben 2021 den Vorsitz der gemeinsamen Landesgruppe für die Bundesländer Rheinland-Pfalz und Saarland übernommen.

BDSW-Landesgruppenvorstand Sachsen-Anhalt wiedergewählt

Der Vorsitzende der BDSW-Landesgruppe Sachsen-Anhalt, Rüdiger Haase, sowie sein Stellvertreter Hagen Henschel wurden von den Mitgliedern wiedergewählt. Neu im Landesgruppenvorstand ist Stellvertreter Daniel Balke. „Ich bedanke mich für das Vertrauen der Landesgruppenmitglieder und die Bestätigung, die Arbeit gemeinsam mit Hagen Henschel und nun Daniel Balke im Sinne der Unternehmen weiterführen zu können“, so Haase.

BDSW-Landesgruppe Schleswig-Holstein wählt Niels Blunck zum neuen Vorsitzenden

Die Mitgliedsunternehmen der BDSW-Landesgruppe Schleswig-Holstein haben am 12. Juni in Lübeck Niels Blunck, Geschäftsführer der Hauschildt & Blunck Wach- und Objektschutz GmbH & Co. KG, zu ihrem neuen Vorsitzenden gewählt. Blunck folgt damit auf den langjährigen Vorsitzenden Lutz Kleinfeldt. Unterstützt wird der neue Vorsitzende von den stellvertretenden Vorsitzenden Kanut Seddig, Andreas Segler, und Björn Wackerhagen.

Im Rahmen der Mitgliederversammlung ernannten die Mitgliedsunternehmen den bisherigen Vorsitzenden Lutz Kleinfeldt zum Ehrenvorsitzenden der Landesgruppe. Kleinfeldt ist Geschäftsführer der Lübecker Wachunternehmen Dr. Kurt Kleinfeldt GmbH und war seit 2010 Vorsitzender der Landesgruppe Schleswig-Holstein sowie von 2013 bis 2025 BDSW-Vizepräsident und von 1993 bis 2001 Rechnungsprüfer des BDSW.

„Ich freue mich, dass mir die Kollegen der Landesgruppe das Vertrauen ausgesprochen haben, nun den Vorsitz zu übernehmen, und bedanke mich herzlich bei Lutz Kleinfeldt für die Arbeit und das Engagement der letzten 15 Jahre“, bedankte sich Blunck im Nachgang der Wahl.

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 6172 948050
Mail: dsa@bdsw.de

Redaktion:
Cornelia Okpara (Chefredakteurin), Andrea Faulstich-Goebel, Martin Hildebrandt, Andreas Paulick, Dr. Berthold Stoppelkamp, Silke Zöller, Tanja Staubach (Redaktionsassistenz)

Anzeigenbetreuung:
Tanja Staubach · Tel.: +49 6172 948052 · 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 2831 97639-0
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 01.01.2025

77. Jahrgang 2025 | Auflage: 10.000 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 weiteres 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: 10,50 Euro einschl. ges. MwSt.
Auslandsbezug: 49,90 Euro einschl. ges. MwSt.

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

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 47906 Kempen
Tel.: +49 2152 9588-0, Fax: 9588-44

ZIEMANN SICHERHEIT GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0
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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Altennotruf

Hier könnte Ihr Firmeneintrag stehen!

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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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

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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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

Ausbildung

Krisenmanagement

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

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-Str. 36, 65189 Wiesbaden
Tel.: +49 61118141-0, Fax: 18141-99
Mail: sicherheit@samsic.de, Web: 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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

STI SECURITY TRAINING INTERNATIONAL GmbH
Steinmühlenweg 5, 65439 Flörsheim am Main/Wicker
Tel.: +49 6145 599910, Fax: 5999169
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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

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

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.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

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

Body-Cam

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

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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

Hier könnte Ihr Firmeneintrag stehen!

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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Empfangskontrolle

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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
Industriering Ost 66, 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 Wertdienste

Prosegur Cash Services Germany GmbH
Kokkolastr. 5, 40882 Ratingen
Tel.: +49 2102 1248-0
Mail: welcome@prosegur.com
Web: www.prosegur.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 CASHSERVICE GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0
Mail: info@ziemann-gruppe.de
Web: www.ziemann-gruppe.de

Einlagerung von Werten

Prosegur Cash Services Germany GmbH
Kokkolastr. 5, 40882 Ratingen
Tel.: +49 2102 1248-0
Mail: welcome@prosegur.com
Web: www.prosegur.de

Full Cash Management Outsourcing

Prosegur Cash Services Germany GmbH
Kokkolastr. 5, 40882 Ratingen
Tel.: +49 2102 1248-0
Mail: welcome@prosegur.com
Web: www.prosegur.de

Geldautomaten-Management

Prosegur Cash Services Germany GmbH
Kokkolastr. 5, 40882 Ratingen
Tel.: +49 2102 1248-0
Mail: welcome@prosegur.com
Web: www.prosegur.de

Geldbearbeitung

Prosegur Cash Services Germany GmbH
Kokkolastr. 5, 40882 Ratingen
Tel.: +49 2102 1248-0
Mail: welcome@prosegur.com
Web: www.prosegur.de

ZIEMANN CASHSERVICE GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0
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

Prosegur Cash Services Germany GmbH
Kokkolastr. 5, 40882 Ratingen
Tel.: +49 2102 1248-0
Mail: welcome@prosegur.com
Web: www.prosegur.de

ZIEMANN CASHSERVICE GmbH
Gewerbestr. 19–23, 79227 Schallstadt
Tel.: +49 7664 9720-0
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
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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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
Industriering Ost 66, 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
Industriering Ost 66, 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

Luftsicherheitsdienste

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
Steinmühlenweg 5, 65439 Flörsheim am Main/Wicker
Tel.: +49 6145 599910, Fax: 5999169
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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

WAB Wach- und Alarmbereitschaft GmbH,
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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

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

LivEye GmbH
Europa-Allee 56b, 54343 Föhren
Tel.: +49 6502 4034722
Mail: info@liveye.com
Web: www.liveye.de

Turmwächter GmbH
Am Lenkwerk 9, 33609 Bielefeld
Tel.: +49 521 75981040
Mail: info@turmwaechter-deutschland.de
Web: https://www.turmwächter.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

Museumsdienste

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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.de

WAB Wach- und Alarmbereitschaft GmbH,
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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
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

SAMSIC Sicherheitsdienste GmbH
Abraham-Lincoln-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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
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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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

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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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

Post- und Empfangsdienste

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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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
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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: 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
Industriering Ost 66, 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

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.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
Industriering Ost 66, 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

WA Sicherheitsdienste GmbH
Bommichring 35, 63864 Glattbach
Tel.: +49 6021 58045-0, Fax: 58045-20
Mail: info@wa-sicherheitsdienst.de
Web: www.wa-sicherheitsdienst.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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
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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

WAB Wach- und Alarmbereitschaft GmbH
Carl-Zeiss-Str. 40, 47445 Moers
Tel.: +49 2841 9588-0, Fax: 9588-44
Industriering Ost 66, 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
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.gbp-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-Str. 36, 65189 Wiesbaden
Tel.: +49 611 18141-0, Fax: 18141-99
Mail: sicherheit@samsic.de
Web: www.samsic.de

Kontinuität und Aufbruch

Von Rechtsanwältin Cornelia Okpara

RAin Cornelia Okpara

Hauptgeschäftsführerin des Bundesverbandes der Sicherheitswirtschaft (BDSW)

100 Tage mit dem neuen Präsidium – das ist zunächst eine kurze Zeitspanne, aber zugleich eine prägende Phase, mit neuen Perspektiven, Aufgaben und Einstellungen.

Nach vielen Jahren als stellvertretende Hauptgeschäftsführerin und mehreren Phasen in kommissarischer Verantwortung habe ich viele Erfahrungen im Verband und mit den ehrenamtlichen Vertretern gesammelt – und doch verändert sich der Blickwinkel, wenn man eine solche Rolle endgültig übernimmt –, besonders in einer Zeit des Umbruchs.

Diese ersten Monate mit dem neuen Präsidenten, Herrn Werner Landstorfer, und dem neu besetzten Präsidium haben mir gezeigt, wie stark unser Verband verwurzelt ist.

Gleichzeitig ist deutlich geworden, dass unsere Stärke nicht nur in dieser Verwurzelung liegt, sondern vor allem in der Fähigkeit, uns gemeinsam weiterzuentwickeln. Der Verband lebt vom Miteinander zwischen Geschäftsstelle, Präsidium und Mitgliedern – und genau in diesem Zusammenspiel entstehen Nähe, Vertrauen und neue Impulse. Dieses Vertrauen ist keine Selbstverständlichkeit, sondern das Ergebnis vieler Gespräche, sorgfältiger Abstimmungen und der Bereitschaft, gemeinsam Verantwortung zu tragen.

Nähe entsteht nicht von selbst, sie wächst durch Dialog, durch gegenseitiges Vertrauen und durch das Bewusstsein, dass wir als Branche nur geschlossen und mit klarer Stimme erfolgreich sein können. Austausch macht den Verband lebendig und sorgt dafür, dass wir nicht nur aktuelle Herausforderungen meistern, sondern auch frühzeitig aufkommende Entwicklungen im Blick behalten. Unsere Mitglieder sind nah an der Praxis, sie wissen, wo der Schuh drückt, und sie geben uns wertvolle Impulse, die wir aufgreifen und in unsere Arbeit einfließen lassen können.

Gleichzeitig stehen wir vor großen Herausforderungen. Die Anforderungen an Sicherheitsdienstleistungen steigen kontinuierlich – inhaltlich, organisatorisch und technisch. Fachkräftesicherung, Qualifikation, Digitalisierung und Nachhaltigkeit sind keine Schlagworte, sondern Handlungsfelder, die wir konsequent weiterentwickeln müssen. Dazu kommt der Anspruch, unsere Rolle in Politik und Gesellschaft noch deutlicher sichtbar zu machen. Denn nur wenn wir verstanden werden, wenn unsere Leistungen und Standards richtig eingeordnet werden, können wir die Wertschätzung erreichen, die unsere Branche verdient. Sichtbarkeit bedeutet nicht nur Präsenz, sondern auch die Fähigkeit, unsere Arbeit verständlich und nachvollziehbar zu vermitteln – nach innen wie nach außen.

In den vergangenen 100 Tagen habe ich gespürt, dass wir die Kraft haben, diese Aufgaben gemeinsam zu schultern. Kontinuität und Aufbruch schließen sich nicht aus – sie ergänzen sich. Auf der Basis unserer langjährigen Erfahrung und mit der Offenheit für Neues können wir die Sicherheitswirtschaft zukunftsfest gestalten. Es ist diese Balance zwischen Bewährtem und Innovation, die uns handlungsfähig macht. Bewährtes gibt Halt, Neues eröffnet Chancen. Wer beides zusammendenkt, legt den Grundstein für nachhaltigen Erfolg.

Mein persönliches Fazit nach dieser Wegmarke lautet daher: Wir sind ein Verband mit starker Substanz und klarer Perspektive. Die nächsten Monate und Jahre werden anspruchsvoll, aber sie bieten zugleich große Chancen. Entscheidend ist, dass wir sie gemeinsam nutzen – mit Geschlossenheit und mit dem festen Willen, die Sicherheitswirtschaft als unverzichtbaren Partner für unsere Gesellschaft weiter zu stärken. Diesen Weg möchte der Verband gehen – Schritt für Schritt, im offenen Austausch, getragen von der Überzeugung, dass wir zusammen mehr erreichen als allein.

SAVE THE DATE

15. Luftsicherheitstage

des BDLS Bundesverband der Luftsicherheitsunternehmen und dem Bundespolizeipräsidium

18. - 19. März 2026

im Holiday Inn Berlin Airport Conference Centre
in Schönefeld bei Berlin

Merken Sie sich den Termin bereits heute 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 **Svenja Wallocha** unter **Tel. +49 6172 948063** oder **E-Mail wallocha@bdls.aero** zur Verfügung.

BUNDESVERBAND DER LUFTSICHERHEITS-UNTERNEHMEN BDLS

BUNDESPOLIZEI

www.luftsicherheitstage.de

VBG
Ihre gesetzliche
Unfallversicherung

7. VBG-Forum Sicherungsdienstleistungen

7. Oktober 2025
Oktogon / Zeche Zollverein / Essen

JETZT ANMELDEN!

Foto: Interartes GmbH

vbg.de/veranstaltungen

Diesjähriges Schwerpunktthema:

Gewaltprävention

in Kooperation

BDSW
BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT