BLUE SWAN BULLETIN

Der KRITIS und Supply Chain Newsletter

Oktober 2025 | MIT FREUNDLICHER EMPFEHLUNG VON BLUE RISK IQ | AUSGABE 4 | www.blueriskiq.de

Energiewende in Deutschland – Wie die Geothermie neuen Schwung in den Energiemix bringt

KRITIS: Energiewirtschaft

Fachbeitrag von Stefan Vito Hiller, Senior Security Advisor

Die deutsche Energiewirtschaft steht vor einem grundlegenden Umbruch. Der Ausstieg aus fossilen Energien ist beschlossen, der Ausbau erneuerbarer Energien nimmt Fahrt auf – doch die zentrale Frage bleibt: Wie sichert Deutschland eine stabile, klimafreundliche Energieversorgung, die gleichzeitig die Anforderungen an die Funktionsfähigkeit und Resilienz der kritischen Infrastrukturen (KRITIS) erfüllt? Denn Versorgungssicherheit, Schutz wichtiger Anlagen und Verfügbarkeit rund um die Uhr sind essenziell, um gesellschaftliche und wirtschaftliche Funktionen aufrechtzuerhalten. Inmitten von Photovoltaik, Windkraft und Wasserstoff rückt eine oft unterschätzte Energiequelle in den Fokus: die Geothermie. Als grundlastfähige, erneuerbare Energieform könnte sie zu einem stabilisierenden Element im deutschen Energiemix werden – wenn ihre Potenziale richtig genutzt und abgesichert werden.

Deutschland verfolgt mit seiner Energiewende das Ziel, bis spätestens 2045 treibhausgasneutral zu sein. Kohle- und Gaskraftwerke sollen sukzessive abgeschaltet werden, während Wind- und Solarkraft weiter ausgebaut werden. Diese wetterabhängigen Energieformen liefern jedoch nicht immer dann Strom, wenn er gebraucht wird.

Gleichzeitig steigt der Strombedarf kontinuierlich – durch Wärmepumpen, Elektromobilität und die Dekarbonisierung

IMPRESSUM

Herausgeber
BLUE RISK IQ ist ein spezialisierter Geschäftsbereich von WSD permanent security GmbH
Neißestraße 1, 14513 Teltow

E-MAIL letstalk@blueriskiq.de
TELEFON 03328 - 432 444

#blue-risk-iq

der Industrie. Ohne grundlastfähige Energiequellen oder zuverlässige Speicher drohen Versorgungslücken und Netzinstabilität.

Wärme aus der Tiefe – stabil und lokal

Geothermie nutzt die Wärme des Erdinneren zur Strom- und Wärmeerzeugung. Sie ist rund um die Uhr verfügbar und wetterunabhängig. In geeigneten Regionen lassen sich **Temperaturen über 100 °C** in mehreren Kilometern Tiefe erschließen – ideal für kombinierte Strom- und Wärmenutzung.

Vorteile der Geothermie

- Klimaneutral und emissionsarm;
- Geringer Flächenverbrauch;
- Ideal für Wärmenetze und kommunale Nutzung;
- Unabhängig von Importen oder Preisschwankungen.

Nachteile der Geothermie

- Hohe Investitionskosten und Erkundungsrisiken;
- Aufwendige Genehmigungsverfahren;
- Begrenzte geologische Eignung in manchen Regionen.

Der Ausstieg aus fossilen Energien – Chancen & Risiken

Der geplante Kohleausstieg bis spätestens 2038 (teilweise bereits 2030) sowie die Abkehr von Erdgas stellen Deutschland vor eine enorme Aufgabe. Fossile Kraftwerke liefern derzeit noch den Großteil der gesicherten Leistung – also Strom, der jederzeit abrufbar ist.

Ein zu schneller Ausstieg ohne tragfähige Alternativen birgt erhebliche Risiken:

- Dunkelflauten mit Stromengpässen;
- Netzschwankungen ohne stabile Grundlast;
- Abhängigkeit von Stromimporten; (z. B. Atomstrom aus Frankreich);
- Strukturwandelprobleme in Kohleregionen.

Geothermie kann hier einen Teil der Lösung darstellen – nicht allein, aber als stabile Säule in einem vernetzten, vielfältigen Energiesystem.

Geothermie in Deutschland – Regionen mit Potenzial

Deutschland verfügt über mehrere geologisch geeignete Regionen für die Nutzung von Tiefengeothermie.

Gerade in urbanen Räumen ermöglichen geothermische Wärmenetze unabhängige, langfristige Versorgungslösungen mit hoher regionaler Wertschöpfung.

Rechtlicher Rahmen: Das Bundesberggesetz (§ BBergG)

Die Nutzung von Tiefengeothermie unterliegt in Deutschland dem Bundesberggesetz (BBergG). Es regelt u. a.:

- Erlaubnis zur Suche geothermischer Ressourcen;
- Anforderungen an Sicherheit, Umweltschutz und Rückbau;
- Rolle der Bergbehörden und Aufsicht;
- Meldepflichten und Dokumentation im Betriebsplanverfahren.

Das **BBergG** schafft einen verbindlichen rechtlichen Rahmen, der Investitionssicherheit bietet und Sicherheits- sowie Umweltstandards garantiert.

Die Rolle des Sicherheitsbeauftragten

Tiefengeothermische Projekte sind technisch komplex und sicherheitsrelevant. Entsprechend den Vorgaben des **BBergG und der KRITIS-Anforderungen** müssen Betreiber umfassende Maßnahmen zur Gefahrenabwehr, Zutrittskontrolle und Anlagensicherung umsetzen – sowohl in Planungs- und Bauphase als auch im Betrieb.

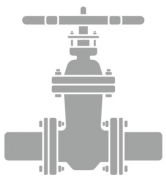
Hier kommt unsere Erfahrung zum Tragen: Wir sind spezialisiert darauf, die besonderen Anforderungen technischer Infrastrukturen und die komplexen regulatorischen Rahmenbedingungen im Energiesektor flexibel und kompetent zu erfüllen.

Mit verlässlichen Sicherheitskonzepten gewährleisten wir nicht nur den Schutz der Anlagen, sondern stärken auch das Vertrauen in die Technologie – bei Behörden, Investoren und der Öffentlichkeit. Dank unserer lokalen Präsenz können wir jederzeit schnell und direkt vor Ort reagieren, Betreiber bestmöglich unterstützen und dabei auf unsere umfassenden Erfahrungen im internationalen Bergbausektor zurückgreifen.

Fazit

Die Zeit ist reif, das heiße Potenzial unter unseren Füßen zu heben – mit technischem Know-how, Verantwortungsbewusstsein und einem klaren Fokus auf Sicherheit. Nur durch die sichere und zuverlässige Integration von Geothermie in die kritischen Infrastrukturen Deutschlands lässt sich eine stabile und nachhaltige Energieversorgung gewährleisten, die den Anforderungen von Gesellschaft, Wirtschaft und Umwelt gerecht wird.

Als spezialisierter Sicherheitsdienstleister begleiten wir diesen Prozess vor Ort, sorgen für den Schutz der Anlagen und unterstützen Betreiber dabei, die strengen Vorgaben des Bundesberggesetzes und der KRITIS-Richtlinien einzuhalten. So leisten wir einen wichtigen Beitrag, damit die Energiewende nicht nur innovativ, sondern auch sicher gelingt.



Unsere Spezialisten von Blue Risk IQ bereiten Sie mit praxisbewährten Lösungen verlässlich auf den Ernstfall vor.

www.blueriskiq.de

BLUERISKIQ

Verkehr & Logistik

Air Cargo Conference 2025

– Innovation, geopolitischer Realismus und Sicherheit mitten im Stadion

Eintracht Frankfurt statt Konferenzsaal: Die diesjährige Air Cargo Conference 2025 überraschte mit einer eindrucksvollen Location – dem Business-Bereich des Deutsche Bank Parks. Zum 10-jährigen Jubiläum trafen sich Luftfracht-, Supply-Chain- und Sicherheitsexperten auf dem Rasen der Realität: AI-Mindset, Resilienzstrategien und geopolitische Risiken standen im Fokus der Diskussionen.

Die Inhalte waren hochaktuell: Von den neuen transatlantischen Ausrichtungen der USA über die Auswirkungen des EU-Freihandelsabkommens bis hin zur Frage, wie logistikgetriebene Resilienz künftig organisiert werden muss.

Geopolitische Risiken und militärische Perspektiven

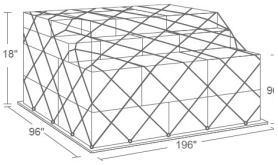
Ein besonderer Akzent kam von General Lungershausen, der in seinem Beitrag zur Bundeswehr-Logistik betonte, dass die „starke Abhängigkeit und Unterstützung durch Logistik-Dienstleister in der Zukunft" unumgänglich ist. Der Appell war deutlich: Resiliente Logistik ist sicherheitspolitisch relevant – und erfordert strategische Partnerschaften zwischen Staat, Wirtschaft und Technologieanbietern.

„Open-heart surgery" am FRA Airport

Auch auf infrastruktureller Ebene wurde deutlich, wie anspruchsvoll die Zukunft der Luftfracht gestaltet wird: Stefan Dürr von Lufthansa Cargo präsentierte unter dem Titel *„Open-heart surgery",* wie das zentrale Frachtzentrum in Frankfurt bei laufendem Betrieb modernisiert wird – ein komplexes Zusammenspiel aus Bau, IT, Automatisierung und Prozessneugestaltung. Die Metapher war treffend: Eingriffe am offenen Herzen dulden keine Fehler – ebenso wenig wie logistische Knotenpunkte im 24/7-Betrieb.

Virtuelle Einblicke in den Sicherheitsbereich – ohne Kontrolle

Mithilfe einer VR-Brille konnten die Teilnehmer erstmals realitätsnahe Einblicke in die luftseitigen Abläufe des Flughafens Frankfurt erhalten – ohne physische Zugangskontrolle.
Das immersive Erlebnis ermöglichte einen Zugang zu sicherheitsrelevanten Prozessen, der sonst nur wenigen Fachleuten vorbehalten ist – und zeigte eindrucksvoll, wie Technologie Transparenz schaffen kann, ohne Sicherheit zu kompromittieren.



Wo Blue Risk IQ ansetzt – und warum das für unsere Kunden relevant ist

Die Air Cargo Conference hat erneut verdeutlicht, dass die Luftfracht- und Logistikbranche mehr ist als nur „Transport" – sie ist ein integraler Bestandteil der kritischen Infrastruktur (KRITIS). Sicherheit, Resilienz und vorausschauendes Risikomanagement beginnen nicht am Flughafen, sondern deutlich früher: in den vorgelagerten, oft global verzweigten Prozessen, die Lieferketten überhaupt erst ermöglichen.

Wir unterstützen Unternehmen dabei, ihre sicherheitsrelevanten Prozesse systematisch zu analysieren, zu bewerten und widerstandsfähig zu gestalten.

Wir schaffen Orientierung im komplexen Zusammenspiel von Infrastruktur, Risiko und Verantwortung – damit Ihre Lieferkette nicht nur effizient, sondern auch krisenfest und compliant bleibt.

Resilienz ist eine Expedition - Klimaforschung trifft Infrastrukturdenken

Im Rahmen unserer Arbeit bei Blue Risk IQ beschäftigen wir uns intensiv mit der Resilienz, Sicherheit und Zukunftsfähigkeit kritischer Infrastrukturen in Deutschland. Unser Besuch am **Alfred-Wegener-Institut, Helmholtz-Zentrum für Polar- und Meeresforschung (AWI) in Bremerhaven** war deshalb weit mehr als ein Blick in die Welt der Wissenschaft – er war ein direkter Erkenntnisgewinn für unsere tägliche Arbeit.

Die Forschungsarbeit des AWI in den Polarregionen liefert zentrale Daten für das Verständnis des globalen Klimawandels. In den Laboren des Instituts konnten wir sehen, wie Eisbohrkerne aus bis zu drei Kilometern Tiefe untersucht werden – ein Fenster in die Klimageschichte der Erde. Diese Informationen sind nicht nur für die Wissenschaft entscheidend, sondern haben auch direkte Relevanz für unsere Risikobewertungen im Kontext von Naturkatastrophen und systemischen Bedrohungen, wie sie im Rahmen des KRITIS-Dachgesetzes adressiert werden.

Resilienz lernen von den Extremen

Besonders wertvoll für uns war der Einblick in die Vorbereitung und Durchführung polarer Expeditionen. Die Herausforderungen in der Arktis und Antarktis sind extrem – und erfordern entsprechend durchdachte Logistik, Sicherheitsstrategien und Notfallmanagement.

Ein prägendes Learning dabei war die Erkenntnis, welche zentrale Rolle Treibstoff auf dem **Forschungsschiff Polarstern** spielt – nicht nur für den Antrieb, sondern für das Überleben an Bord.

Treibstoff bedeutet dort:

- Heizenergie zum Schutz vor eisigen Außentemperaturen;
- die Möglichkeit, aus Eis Trinkwasser zu gewinnen;
- die Sicherstellung von Kommunikation und Navigation; und
- letztlich die Aufrechterhaltung des gesamten Bordbetriebs.

Diese enge Verflechtung von lebensnotwendigen Funktionen mit einer einzigen Ressource zeigt eindrucksvoll, wie kritisch Interdependenzen auf kompaktem Raum sind – genau wie in urbanen Infrastrukturen oder Versorgungssystemen. Was auf dem Schiff Realität ist, gilt im Prinzip auch für unsere vernetzte Welt an Land.

Auch die weiteren Sicherheitsmaßnahmen der Polarstern zeigen dieses Denken in Redundanzen und Szenarien: Die isolierte Mensa fungiert im Ernstfall als Schutzraum bei Heizungsausfall. Und die zwei Rettungsboote auf beiden Schiffsseiten sind jeweils so ausgelegt, dass sie die gesamte Besatzung eigenständig aufnehmen können – ein klares Beispiel für 100-prozentige Evakuierungsfähigkeit durch doppelte Absicherung. Dazu ist nicht nur Platz für einen, sondern für zwei Helikopter.

An Einrichtungen wie der *Neumayer-Station III* in der Antarktis wird dieses Prinzip ebenso gelebt. Ohne systematische Vorsorge, Redundanz und Risikomanagement wären solche Missionen nicht möglich. Die ständige Auseinandersetzung mit möglichen Szenarien und deren Folgen gehört zum Alltag der Menschen am AWI – genau wie in unserer Arbeit.

Parallelen zum KRITIS-Dachgesetz

Die gewonnenen Eindrücke lassen sich direkt auf unsere Arbeit übertragen. Die Menschen am AWI beschäftigen sich täglich mit der Frage: **Was könnte passieren – und wie bereiten wir uns darauf vor?** Genau der gleiche Denkansatz steht auch hinter unserer Methodik in der Bewertung, Planung und Absicherung kritischer Infrastrukturen.

Das neue KRITIS-Dachgesetz hebt die Bedeutung von Resilienz, Redundanz und funktionaler Absicherung auf eine neue regulatorische Ebene. Unsere Erkenntnisse aus dem AWI zeigen, dass diese Prinzipien nicht nur theoretisch sinnvoll, sondern praktisch unerlässlich sind – insbesondere im Kontext des Klimawandels und seiner Auswirkungen auf Versorgungs- und Sicherheitsstrukturen.

Fazit: Resilienz entsteht durch Vordenken.

Urlaubszeit ist Spionagezeit – Warum Führungskräfte und ihre Familien im Urlaub zur leichten Beute werden

Palmen, Pool – und perfekte Tarnung für Spione

Während Führungskräfte und Wissensträger deutscher Unternehmen mit ihren Familien in der Ferne entspannen, nutzen professionelle Akteure gezielt diese Gelegenheit zur Informationsgewinnung. Moderne Ausspähversuche beschränken sich längst nicht mehr auf Geschäftsreisen oder Bürokommunikation – sie verlagern sich zunehmend in den privaten Raum, insbesondere während Urlaubsreisen.

Denn im Urlaubsmodus lassen viele unbewusst Vorsicht und Sicherheitsroutinen fallen: Gespräche finden ungefiltert statt, Geräte sind ungeschützt, Aufmerksamkeit ist gering. Und häufig geraten auch Familienangehörige, insbesondere Kinder und Jugendliche, ins Visier – meist ohne es zu bemerken.

Warum Urlaub im Ausland besondere Risiken birgt

- Reduzierte Wachsamkeit, da es keine IT-Sicherheitsvorgaben und keinen Schutz durch Unternehmensstrukturen gibt;
- Private Gespräche am Pool, im Restaurant oder an der Hotelbar – vertrauliche Informationen lassen sich leicht mitlauschen;
- Kinder teilen oft in sozialen Netzwerken Standortdaten, Bilder und Reisepläne;
- Hotel-WLAN, AirBnB-Router oder Kreuzfahrtnetze sind oft unzureichend gesichert oder kompromittiert und gelten als unsicher.

Potenziell gefährliche Urlaubsziele – wenn Erholung zur Schwachstelle wird

Was viele nicht bedenken: Manche Urlaubsregionen gelten längst als hochriskant – insbesondere für deutsche Führungskräfte und Wissensträger. In beliebten Zielen wie Südostasien, der Arabischen Halbinsel oder Teilen Nordafrikas operieren staatlich gesteuerte Nachrichtendienste oder wirtschaftlich motivierte Gruppen gezielt dort, wo mit einer hohen Dichte an ***„lohnenden Zielen“*** gerechnet werden kann.

Zugleich verhalten sich Reisende außerhalb ihrer gewohnten Umgebung oft weniger kontrolliert. Intransparentere Sicherheitsstandards, schwer überprüfbare Abläufe in Hotels oder unklare rechtliche Rahmenbedingungen fördern gezielte Zugriffe auf digitale und persönliche Informationen – häufig ohne jeden Verdacht.

Deutschland bleibt im Fokus globaler Spionageaktiven

Die deutsche Industrie ist seit Jahren ein bevorzugtes Ziel staatlich gelenkter Spionage. Dabei geht es nicht nur um Technologiediebstahl, sondern auch um strategische Informationsgewinnung, das Aushebeln von Wettbewerbsvorteilen und gezielte Schwächung des Wirtschaftsstandorts Deutschland. Führungskräfte – und zunehmend auch ihre Familien – geraten dadurch in den Mittelpunkt und werden Zielobjekte.

Der oftmals unterschätzte Risikofaktor: Familie

Angriffe erfolgen immer seltener direkt. Stattdessen nutzen Angreifer gezielt das private Umfeld, um an Informationen zu gelangen. Kinder und Jugendliche sind besonders anfällig – nicht aus Nachlässigkeit, sondern weil ihnen schlicht das Risikobewusstsein fehlt. Beispiele:

- **Zufällige Begegnungen:** Small Talk am Pool mit vermeintlich harmlosen Bekanntschaften kann sensible Informationen wie Wohnort, Beruf, Reisedaten oder Familiennamen preisgeben;
- **Unreflektierte Social-Media-Nutzung:** Fotos mit Standortangaben oder Hashtags wie **#Thailand2025** offenbaren Aufenthaltsorte und Abwesenheitszeiten;
- **Geteilte IT-Infrastruktur:** Kinder nutzen offene WLANs – oft auf denselben Geräten, mit denen manchmal auch Führungskräfte auch beruflich arbeiten.

Was wie eine Szene aus einem Spionagefilm klingt, ist in der Realität längst technischer Alltag: Abhörtechnik in **Smart-TVs, Lampen, Steckdosen oder scheinbar harmlosen Ladegeräten** ist weder futuristisch noch selten.
Moderne Miniaturisierung erlaubt es, Mikrofone, Kameras oder sogar Mobilfunkmodule in Alltagsgegenständen unterzubringen – vollkommen unauffällig für den normalen Nutzer.

Gerade in Hotelzimmern, die regelmäßig wechselnde Gäste beherbergen, sind solche Geräte ideale Träger für gezielte Überwachung.
Die Manipulation ist meist nicht sichtbar, und viele Geräte haben ohnehin eine Dauerverbindung ins Netz – was eine Übertragung im Hintergrund erleichtert. Misstrauen Sie der technischen Umgebung – besonders in Regionen mit erhöhtem Spionagerisiko.

Unsichtbare Risiken im Hotelzimmer – Wie Spionagetechnik heute aussieht

Kompromittierte WLAN-Router durch Manipulation keine Seltenheit

Achtung Wecker: Nutzung als Dauer-aufnahmegerät möglich

Fernzugriff auf Kamera oder Mikrofon vom Smart-TV kann nicht ausgeschlossen werden

Ladegeräte oder USB-Ports können mit Keyloggern oder WLAN-Modulen ausgestattet sein

Was macht das besonders kritisch in Hotels oder privat angemietete Villen oder Apartments?

Falls Sie fremde Geräte nutzen, können diese bereits kompromittiert sein. Niemand weiß genau, ob:

1. **Die Firmware manipuliert wurde.**
2. **Die Kamera über eine Cloud mit Dritten verbunden ist.**
3. **Netzwerkdaten vom Hotel-Router mitleiten.**

Insbesondere in Regionen mit niedrigen Datenschutzstandards kann Technik gezielt so manipuliert sein, dass sie bei bestimmten Gästeprofilen (z. B. Führungskräfte, Geschäftsreisende, Diplomaten) aktiviert wird.

Empfohlene Maßnahmen – Vor, während und nach der Reise

- Keine geschäftlichen Daten auf privaten Geräten speichern;
- Familienangehörige für Risiken und Verhaltensregeln sensibilisieren;
- Keine Angaben zu Firma, Job, Wohnort oder Reisedaten;
- Keine vertraulichen Gespräche in öffentlichen Bereichen;
- Keine fremden USB-Sticks oder Ladegeräte nutzen;
- Vorsicht bei auffällig interessierten neuen Kontakten;
- Alle genutzten Geräte professionell prüfen lassen – auch private;
- Familienmitglieder gezielt befragen ob es ungewöhnliche Begegnungen gab.

Warnsignale nach dem Urlaub – Woran Sie erkennen, dass etwas nicht stimmt

- Unerklärliche Aktivitäten oder Datenabflüsse im Firmennetzwerk;
- Anmeldungen von ungewöhnlichen Orten oder zu ungewöhnlichen Zeiten;
- Verlangsamte oder fehlerhafte Gerätefunktionen;
- Hinweise, dass Wettbewerber über intern bekannte Informationen verfügen.

Wie sie sich schützen können

- Kamera physisch abkleben (wenn vorhanden).
- Smart-TV nicht mit eigenem Gerät koppeln (z. B. Handy-Screen oder WLAN-Sharing vermeiden).
- TV bei Nichtnutzung ausschalten – am besten über Steckdose, nicht nur per Fernbedienung.
- Keine persönlichen Accounts (Netflix, YouTube) auf fremden Geräten einloggen.
- Fernbedienung mit Mikrofon? – Batterie entfernen oder ausschalten.

Fazit:
Sicherheit endet nicht am Flughafengate

Führungskräfte stellen ein attraktives Ziel für staatlich oder wirtschaftlich motivierte Spionage dar – nicht nur im beruflichen Umfeld, sondern gerade auch in vermeintlich sicheren Momenten wie dem Urlaub. Abseits des geschäftlichen Alltags fehlen häufig grundlegende Schutzmechanismen, was Angriffsflächen schafft. Besonders kritisch: Das persönliche Umfeld wird zur potenziellen Schwachstelle. Familienangehörige und Freunde sind in der Regel weder sensibilisiert noch geschult im Umgang mit Sicherheitsrisiken und werden so unbewusst zum Einfallstor für potenzielle Angreifer.

Ein weiterer Trugschluss besteht im Vertrauen auf die Sicherheitsstandards großer Hotelketten. Schon vor der Corona-Pandemie war das Sicherheitsniveau in der Hotellerie trotz moderner Infrastruktur kein Garant für tatsächlichen Schutz – es gab ausreichend dokumentierte Fälle, in denen Wirtschaftsspione gezielt Schwachstellen in Hotels ausnutzten.

Seit der Pandemie hat sich die Lage weiter verschärft: Viele Hotels mussten ihr Sicherheitskonzept von Grund auf neu aufbauen, doch Ressourcenmangel, Personalfluktuation und ein dramatischer Know-how-Verlust machen diesen Wiederaufbau bislang unzureichend.

Insbesondere qualifiziertes Fachpersonal hat die Branche in der Krise verlassen, und das heute tätige Personal ist in vielen Fällen nicht ausreichend geschult, um sicherheitsrelevante Vorgänge zu erkennen oder adäquat zu reagieren.

Empfangs- und Servicemitarbeitende verfügen selten über das nötige Wissen, um etwa potenzielle Ausspähversuche zu identifizieren oder Risiken im IT- und Kommunikationsbereich zu minimieren. Gleichzeitig haben sich kriminelle Akteure technisch wie organisatorisch weiterentwickelt – sie nutzen gezielt diese Lücken in einem ohnehin angespannten System.

Vor diesem Hintergrund sollten sicherheitsbewusste Führungskräfte nicht davon ausgehen, dass Hotels standardmäßig ausreichenden Schutz bieten.
Persönliche Vorsorge und ein erhöhtes Risikobewusstsein sind heute notwendiger denn je – insbesondere im Ausland. Wer als Wissensträger unterwegs ist, trägt auch selbst die Verantwortung für seine Sicherheit.