SICHERHEIT.
DAS FACHMAGAZIN.

SICHERHEIT AUF DEN PUNKT GEBRACHT.

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.

SICHERHEIT. DAS FACHMAGAZIN.

bietet kleinen und mittelständischen Unternehmen, Behörden und Organisationen bedeutendes und praxisnahes Wissen. Mit konkreten Schritt-für-Schritt-Anleitungen, individuell anpassbaren Musterdokumenten und Formularen, praktischen Handlungsempfehlungen sowie innovativen Tools und Werkzeugen verspricht Ihnen SICHERHEIT. Das Fachmagazin. einen einzigartigen Mehrwert.

DOWNLOADS

Alle Ausgaben von SICHERHEIT. Das Fachmagazin. enthalten nützliche und wissenswerte Downloads. Diese finden Sie auf unserer Homepage unterhalb der jeweiligen Ausgabe.

SECURITY-SERVICE-CENTER

Mit unserem Security-Service-Center bieten wir Ihnen einen attraktiven Mehrwert. Sollten Sie zu einzelnen Artikeln nähere Informationen benötigen, Rückfragen haben oder ggf. auf der Suche nach kompetenter Fachexpertise sein, stehen Ihnen unsere Experten jederzeit gerne zur Verfügung.

Telefon: +49 (0) 30 / 700 36 96 5
E-Mail: redaktion@sicherheit-das-fachmagazin.de

KOSTENFREI & UNVERBINDLICH

Warum ist SICHERHEIT. Das Fachmagazin. für Sie kostenfrei erhältlich?

Sicherheit hat in vielen Unternehmen, Behörden und Organisationen einen eher nebensächlichen Stellenwert, kaum personelle Ressourcen und/oder entsprechendes Budget. Durch das kostenfreie Angebot gelingt es uns, aktuelle (Sicherheits-) Themen, Trends und Entwicklungen mit unseren Zielgruppen zu teilen, unabhängig davon, ob das nötige Budget für ein Abonnement aufgebracht werden kann.

Wie finanziert sich SICHERHEIT. Das Fachmagazin.?

Das Magazin finanziert sich durch erkennbare Werbeanzeigen, Kompetenzpartner und sog. Affiliate-Links im Rahmen des Amazon Partnerprogramms. Unabhängig davon gilt bei der redaktionellen Arbeit jedoch stets der Grundsatz einer neutralen und seriösen Informationsvermittlung: „Werbung bleibt Werbung, Artikel bleibt Artikel!“

Erfahren Sie mehr unter www.sicherheit-das-fachmagazin.de/transparenzhinweis

GENDERHINWEIS: *Aus Gründen der besseren Lesbarkeit wird bei SICHERHEIT. Das Fachmagazin. auf eine geschlechtsneutrale Differenzierung (z. B. Mitarbeiterinnen/Mitarbeiter) verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.*

UNSERE THEMEN

- Wirtschaftsschutz
- Sicherheitsvorkehrungen
- Reisesicherheit im Ausland
- Krisen- und Notfallmanagement
- Security Awareness-Kampagnen

E-PAPER

SICHERHEIT. Das Fachmagazin. als ePaper bringt Ihnen alle Vorzüge eines gedruckten Magazins auf Ihren Bildschirm. Zu Hause oder unterwegs, im Büro oder im Urlaub – auf Ihrem PC, Tablet und Smartphone.

Ihre Vorteile:

› Ressourcenschonend durch nachhaltige Einsparungen beim Verbrauch von Papier, Treibstoff und CO2

› Komfortable Web-Ansicht mit besonderen Bedienfunktionen oder als Download im PDF-Format

©Syda Productions/Fotolia

SICHERHEITSVERANTWORTLICHE: TIPPS FÜR EINE BESSERE WAHRNEHMUNG

Sicherheit ist im Unternehmen auf viele Schultern verteilt. Dennoch sollte der Sicherheitsverantwortliche im Unternehmen den Überblick behalten und alle Themen offen mit den Akteuren besprechen. Welches persönliche Rüstzeug Sie benötigen, damit Sie in Ihrer Funktion besser wahrgenommen werden, erläutern wir Ihnen im Folgenden näher.

Mit der Verantwortung für (Unternehmens-) Sicherheit stehen Sie nicht alleine da. Der Unternehmer hat eine Fürsorge- und Sorgfaltspflicht und ggf. weitere gesetzliche, versicherungsseitige oder gar vertraglich basierende Verpflichtungen. Des Weiteren ist er natürlich auch an einem reibungslosen betrieblichen Ablauf ohne sicherheitsrelevante Zwischenfälle interessiert. Aber auch die Führungskräfte müssen als gutes Vorbild vorangehen. Berührungspunkte wird es dabei immer mit den Bereichen Brandschutz, Arbeitssicherheit, Datenschutz, Compliance, IT-Sicherheit und dem Betriebsrat geben.

Es ist nicht immer die reine Kraft der Argumente, die den größten Erfolg bringt. Entscheidend ist, die Angesprochenen zu erreichen und mitzunehmen. Dazu haben wir Ihnen ein paar Tipps zusammengestellt, die Ihnen dabei helfen sollen, positiv in Ihrer Funktion wahrgenommen zu werden.

1. Benutzen Sie Ihren gesunden Menschenverstand

Sie müssen nicht immer um die Ecke denken, Ihr gesunder Menschenverstand reicht manchmal aus, um einem Problem auf die Schliche zu kommen.

2. Zeigen Sie Fingerspitzengefühl

Niemand lässt sich gerne belehren! Diplomatisches Geschick ist gefragt. Erläutern Sie immer die Vorzüge von Sicherheitsmaßnahmen und setzen Sie diese in einen praktischen Kontext.

3. Gehen Sie dosiert vor

Weisen Sie gerade zu Beginn Ihrer Tätigkeit nicht auf alle Sicherheitslücken gleichzeitig hin und suchen Sie nicht gezielt nach Fehlern. Denken Sie stets daran: „Elefanten isst man scheibchenweise!“

4. Ändern Sie Ihren Blickwinkel

Betrachten Sie Ihre Aufgaben oder die Interaktion mit Mitarbeitern, Führungspersonen etc. einmal als Außenstehender. Somit können Sie erahnen, wie Sie auf Andere wirken.

5. Kommunikation heißt Ihr Schlüsselwort

Der Ton macht die Musik. Ein offenes Ohr fördert das Miteinander und die Solidarität mit Ihrem Job.

6. Heben Sie Positives hervor

Sprechen Sie insbesondere über solche Dinge, die gut laufen. Tagtägliche Kritik und Negativbeispiele fördern keine Motivation.

7. Erkennen Sie die Grenzen Ihrer Funktion

In vielen Fällen sind Sie nur in beratender Funktion tätig und keinem Mitarbeiter direkt weisungsbefugt. Sprechen Sie Dinge ggf. zu einem späteren Zeitpunkt noch einmal an oder informieren Sie bei vermehrten Verstößen den Vorgesetzten.

> IHRE FUNKTION STELLT EINE ANSPRUCHSVOLLE UND MEIST (UNGELIEBTE) HERAUSFORDERUNG DAR, MIT DER SIE WACHSEN UND SICH AUCH PERSÖNLICH WEITERENTWICKELN KÖNNEN.

©Myst/Fotolia

WIRTSCHAFTSSCHUTZ: SICHERHEIT IST NICHT ALLES, ABER OHNE SICHERHEIT IST ALLES NICHTS!

Dieser Slogan greift den Kern des Wirtschaftsschutzes auf, denn alle unternehmerischen Werte wie beispielsweise Produkte, Maschinen, Mitarbeiter, Gebäude, Dokumente, Entwicklungs-Know-how und Innovationen sind nur dann etwas wert, wenn sie effektiv vor Ausspähung, Abwanderung oder Sabotage geschützt werden. Im Kern geht es bei Wirtschaftsschutzmaßnahmen um die Aufrechterhaltung der künftigen Wettbewerbsfähigkeit ihres Unternehmens.

Die internationale Spitzenstellung und die immensen Forschungs- und Entwicklungstätigkeiten deutscher Unternehmen wecken nicht nur bei Konkurrenten Begehrlichkeiten, sondern auch bei fremden Staaten, die ihrer heimischen Wirtschaft Kosten für Forschungs- und Entwicklungsarbeiten ersparen wollen und nach schnellem Markterfolg streben. Globalisierung und zunehmende Digitalisierung bergen nicht nur Chancen, sondern auch erhebliche Risiken für Unternehmen. Wirtschaftsschutz eint dabei informationstechnische Maßnahmen mit baulichen/technischen, personellen, prozessualen und organisatorischen Aspekten.

WER TRÄGT DIE VERANTWORTUNG FÜR DEN WIRTSCHAFTSSCHUTZ IM UNTERNEHMEN?

Grundsätzlich unterliegen die Unternehmenssicherheit und der Know-how-Schutz der Eigenverantwortung deutscher Unternehmen. Somit sollte der Wirtschaftsschutz zur Chefsache erklärt werden. Da die Risiken aber vom klassischen Wirtschaftsschutz bis hin zu hoch professionalisierten Spionageangriffen und Sabotageakten aus dem politisch motivierten Milieu reichen, ist das Bundesamt für Verfassungsschutz (BfV) gemeinsam mit den Verfassungsschutzbehörden der Länder ein guter „Dienstleister“ zum Thema Spionageabwehr und Wirtschaftsschutz. Hierzu kooperiert das BfV mit zahlreichen nationalen und internationalen (Sicherheits-) Behörden und Verbänden als Informations- und Dialogplattform. Auch das europäische Parlament hat die Notwendigkeit zum Schutz von Geschäftsgeheimnissen erkannt und hierzu eine entsprechende Verordnung verabschiedet, die wir Ihnen auf Seite 12 näher vorstellen. Die oberste Leitungsebene in ihrem Unternehmen muss bei dem Thema Wirtschaftsschutz und dem damit verbundenen Aufbau eines Sicherheitsmanagementsystems nicht nur aufgrund der rechtlichen Verpflichtungen wie z. B. Fürsorgepflicht, Organisationshaftung etc. „mit ins Boot geholt werden“, ausreichende finanzielle und personelle Ressourcen zur Verfügung stellen und das System letztlich auch freigeben. Sie muss maßgeblich bei der Einordnung der unternehmerischen Werte sowie der daraus resultierenden Maßnahmen mitwirken.

BEISPIELE FÜR KNOW-HOW-ABFLUSS:

- Ausspähung ihrer Mitarbeiter in den sozialen Netzwerken.
- Vermeintliche Forschungsangebote oder Headhunter-Akquisition.
- Gezielte Sabotageangriffe auf ihre Entwicklungsstandorte.
- Diebstahl oder Erschleichung von vertraulichen Dokumenten.

WIRTSCHAFTSSPIONAGE VERSUS INDUSTRIE- UND KONKURRENZSPIONAGE

Der Begriff „Wirtschaftsschutz“ definiert den Schutz der deutschen Wirtschaft vor Spionageaktivitäten (Wirtschaftsspionage), die durch ausländische Geheimdienste gelenkt oder unterstützt werden. Dies ist neben der Ausspähung von politischen und militärischen Aufklärungsthemen ein Bereich, der aufgrund der zunehmenden Globalisierung und der damit einhergehenden Verteilung der wirtschaftlichen Konstellationen in den vergangenen Jahren an besonderem Interesse gewonnen hat. Die Industrie- und Konkurrenzspionage hingegen meint das Ausspionieren von Wettbewerbern oder sonstigen Kriminellen, also die illegale Beschaffung von Know-how oder Produkten durch konkurrierende Unternehmen oder im Auftrag von konkurrierenden Unternehmen. Ziel ist die Erlangung von Geschäftsvorteilen durch die Hinderung des Konkurrenten in seinen Geschäftsaussichten, die Verringerung von Marktanteilen und das illegal beschaffte Wissen für eigene Innovationen zu nutzen. Der Schutz vor Informationsabfluss und Produktdiebstahl liegt somit in ihren Händen. Daher sollten sie ein passgenaues und nachhaltig erarbeitetes Sicherheitsmanagementsystem etablieren, um ihr unternehmerisches Know-how, physisches Eigentum und/oder die Unversehrtheit von Leib und Leben ihrer Mitarbeiter und Kollegen zu schützen. Wie genau ihr Schutzsystem letztlich aussieht, hängt neben der individuellen Gefährdungs- und Bedrohungslage sowie der Risikotoleranz auch maßgeblich von der Unternehmensgröße ab. Einen weiteren Einfluss haben die unternehmensstrategische Ausrichtung, ihre Interessengruppen und ihr sicherheitsrelevantes Umfeld. ›››

IM AKTUELLEN VERFASSUNGSSCHUTZBERICHT KÖNNEN SIE SICH ÜBER DIE METHODEN UND VORGEHENSWEISEN AUFGEDECKTER SPIONAGE- UND SABOTAGE-AKTIVITÄTEN INFORMIEREN UND DIESE INFORMATIONEN AUF IHRE UNTERNEHMERISCHEN TÄTIGKEITEN BEZIEHEN.

©peshkov/Fotolia

IN FÜNF SCHRITTEN ZUM WIRTSCHAFTSSCHUTZ

Der Aufbau des Wirtschaftsschutzes als Sicherheitsmanagementsystem erfolgt grundsätzlich in 5 Schritten, die sich in weitere Unterschritte aufteilen, welche wiederum aus den unterschiedlichen Einflüssen und Ergebnissen resultieren.

1

VERANTWORTLICHE PERSON BENENNEN

Um ein Sicherheitsmanagementsystem nachhaltig und übergreifend implementieren zu können, ist es essentiell, eine Person zu benennen, die dieses Thema im Unternehmen voranbringt.

2

NUTZUNGBEREICHE BESTIMMEN

Definieren Sie den Anwendungsbereich des Sicherheitsmanagementsystems, z. B. in relevanten Bereichen wie Produktion, Forschung, Entwicklung, Vertrieb oder ggf. nach Standorten, Gebäuden etc. Hierbei sollten Sie u. a. auch die unternehmerischen Werte berücksichtigen, welche zur Aufrechterhaltung der allgemeinen bzw. spezifischen Geschäftstätigkeit dienen. Diese sollten Sie gemeinsam und bereichsübergreifend mit der obersten Leitungsebene eruieren.

3

SICHERHEITSTHEMEN PRIORISIEREN

Definieren Sie bereichsübergreifend die jeweiligen Themengebiete, die einen direkten Einfluss auf ihr Unternehmen haben. Themen wie Objekt-/Standortsicherheit, Know-how-Schutz, Bewerberprüfung, Integritätsprüfung, Lauschabwehr, Kontinuität der Gebäudedienste, Einsatz von Sicherheitsdienstleistern oder Reisesicherheit können in unterschiedlicher Ausprägung für Sie von Relevanz sein.

4

REGELUNGSBEDARF ABLEITEN

Der erforderliche Regelungsbedarf und die weiteren Maßnahmen resultieren aus der Sicherheitsstrategie. Der Regelungsbedarf umfasst immer bauliche/technische, personelle, prozessuale und organisatorische sowie informationstechnische Maßnahmen.

5

MASSNAHMEN IMPLEMENTIEREN

Mit den Analyseerkenntnissen stellen Sie eine Organisationsstruktur und Regelprozesse auf, mit denen Sie ihre Sicherheitsrisiken regelmäßig identifizieren, bewerten und behandeln können. Die Umsetzung der vorab definierten und besprochenen Maßnahmen funktioniert jedoch nur, wenn Sie alle internen und externen Mitarbeiter sowie betroffene Dritte auch entsprechend informieren und sie somit auf die Reise in eine „sicherere Zukunft“ mitnehmen.

Wie Sie ein Sicherheitsmanagementsystem aufbauen und implementieren werden wir Ihnen in den folgenden Ausgaben von SICHERHEIT. Das Fachmagazin. ausführlicher erläutern.

WIE VERMARKTET MAN „SICHERHEIT“ FÜR EINE BESSERE SICHERHEITSKULTUR?

Bei sicherheitsrelevanten Vorfällen steckt in den allermeisten Fällen der „Faktor Mensch“ als Ursache dahinter. Manche Menschen kreieren (vermeintlich) sichere Systeme und Andere bringen sie mit ihrer kreativen Unbedarftheit zu Fall. Ein umfassendes Sicherheitsbewusstsein kann ihre interne Sicherheitsorganisation bei dem nachhaltigen Aufbau einer Sicherheitskultur im Unternehmen unterstützen. Doch wie erreichen Sie ihre Mitarbeiter und welche Erfolgsfaktoren gibt es?

Der „Faktor Mensch“ ist derjenige, der die Tür offen lässt, das Passwort zu einfach gestaltet, seinen Ausweis einem Dritten überlässt, seinen Laptop verliert, Informationen allzu bereitwillig mit Anderen teilt, Unterlagen offen liegen lässt und noch vieles Weitere mehr. Security Awareness ist mehr als nur die Sensibilisierung ihrer Mitarbeiter gegenüber potentiellen Gefahren und Risiken. Security Awareness hat vielmehr die Aufgabe, Menschen zu verstehen, sie zu erreichen und letztlich auch zu überzeugen. Vielleicht sogar, unbedarfte Verhaltensweisen nachhaltig zu ändern.

WAHRNEHMUNG VON SICHERHEIT IM UNTERNEHMEN

Eines sollten Sie in jedem Fall beachten, wenn Sie an den Aufbau einer Security Awareness-Kampagne denken: für ihre Mitarbeiter ist der Umgang mit Sicherheit ein eher passiver und teilweise sogar lästiger Akt. Aktive Sicherungsaufgaben nehmen nur „Sicherheitsverantwortliche“ wahr. Den „Aha-Moment“ erleben Sie bei ihren Mitarbeitern in den meisten Fällen, wenn es um direkte Verbindungen zum Privatleben geht („Bei mir wurde auch schon mal eingebrochen.“) oder wenn ihre Mitarbeiter selbst einer gewissen Unsicherheit gegenüberstehen („Letztens hatte ich auch so eine komische E-Mail im Postfach.“). Die Sicherheit im Unternehmen stellt zum Einen eine Kontrollinstanz dar und ist zum Anderen aber interner Dienstleister. Sicherheitsverantwortliche werden als Wissende, als Insider erlebt und entsprechend misstrauisch wird ihnen teilweise begegnet. Zumal sich die Tätigkeiten umgesetzter Sicherheitsmaßnahmen nur schwer betriebswirtschaftlich bemessen lassen. Sicherheit darf aber nicht nur als Kostenfaktor gesehen werden, sondern als wesentliches Element, das zur Schaffung der vor allem betriebswirtschaftlichen Unternehmensziele beiträgt.

SCHAFFUNG EINER SICHERHEITSKULTUR

Sicherheitsmaßnahmen, das Überzeugen ihrer Mitarbeiter von diesen Maßnahmen und das gemeinsame Schutzziel müssen individuell konfiguriert werden, denn nur so erreichen Sie eine gute Sicherheitskultur im Unternehmen. Durch die Einbeziehung ihrer Mitarbeiter in das ›››

„Warum" wird die vorherrschende Mitarbeiterperspektive auf die gesamte Unternehmensperspektive erweitert.

Security Awareness thematisiert u. a. paradoxe Handlungen und zeigt neue Risiken auf. Das Ziel sollte aber immer sein, ein gemeinschaftliches Interesse zu entwickeln, sich und das unternehmerische Umfeld nachhaltig zu schützen. Dies erreichen Sie allerdings nur, wenn Ihre Security Awareness-Kampagne in die Unternehmenskultur eingebunden wird.

DIE FOLGENDEN 8 FAKTOREN FÜHREN NACHWEISLICH ZU MEHR SICHERHEITSBEWUSSTSEIN:

- Das Wissen um die aktive Gestaltung der eigenen Unternehmenskultur.
- Der Erhalt und die Pflege der Alltagskultur.
- Die Förderung der gemeinschaftlichen Entwicklung, aber auch des Einzelnen.
- Die Berücksichtigung der Kommunikationshistorie des gewählten Mediums.
- Die Förderung der Verantwortung und die Loyalität gegenüber der Gemeinschaft und den Unternehmenszielen unter Berücksichtigung von Bildungsgrad, Status und Verfassung der Mitarbeiter.
- Ein hoher Grad der Vernetzung aller Kanäle und Tools.
- Ein intensiver Austausch und ein „Gehört-werden".
- Die Erzeugung eines Wiedererkennungswertes durch unternehmensaffine Faktoren.

HERANGEHENSWEISE AN EINE SECURITY AWARENESS-KAMPAGNE

Der Kreativität in der Vermittlung der Inhalte sind grundsätzlich keine Grenzen gesetzt, natürlich immer unter Berücksichtigung der Unternehmenskultur und Ihrer psychologischen Grundlagen. Setzen Sie unterschiedliche Maßnahmen und Herangehensweisen ein, um eine „neue" erweiterte Sicherheitskultur zu schaffen. Dies erreichen Sie durch innovatives Marketing, die Nutzung unterschiedlichster Tools und Kanäle und ein selbstbewusstes Auftreten. Als Erstes stellt sich die Frage der Herangehensweise an solch eine Kampagne.

BEACHTEN SIE DIE CHECKLISTE RECHTS >>>

Besprechen Sie Ihre Ideen im Vorfeld mit der Führungsebene, dem Betriebsrat und allen anderen Sicherheitsabteilungen im Unternehmen, wie z. B. IT, Datenschutz, Compliance und Co. Nicht zuletzt, um Ressourcen zu definieren und gemeinsame Lösungen/Kampagnen aufzusetzen. Ggf. erhalten Sie auch Unterstützung von der Marketingabteilung.

Sollte es Ihnen schwerfallen, das Thema Sicherheit kreativ an den Mitarbeiter zu bringen, können Sie sich auch externer Hilfe bedienen. Bei der Suche eines Anbieters für Security Awareness zeigt sich allerdings deutlich, wie sich mit Unsicherheit im Unternehmen Kapital schlagen lässt. IT-Beratungsunternehmen, Rechtsanwaltskanzleien, Wirtschaftsprüfer und Kommunikationsagenturen haben dieses Beratungsfeld für sich entdeckt. Finden Sie für sich heraus, welches Unternehmen zu Ihnen passt und vor allem Sicherheit als ganzheitlichen Ansatz versteht.

NUTZEN SIE FÜR IHRE SECURITY AWARENESS-KAMPAGNE UNSERE KOSTENFREIEN POSTER, FALTKARTEN UND COMIC-BILDER.
››› WWW.SICHERHEIT-DAS-FACHMAGAZIN.DE ‹‹‹

INNOVATIVES MARKETING DURCH KREATIVE IDEEN

Stellen Sie sich beim Aufbau einer Security Awareness-Kampagne folgende Fragen:

Generell:

- ☐ Wo stehen wir?
- ☐ Wo wollen wir hin?

Maßnahmenbezogen:

- ☐ Wie können wir das generelle Ziel erreichen?
- ☐ Was könnte man an der bisherigen Herangehensweise ändern?
- ☐ Was wäre, wenn man das ändern würde?
- ☐ Warum ist die gewählte Maßnahme erfolgsversprechend?
- ☐ Wie kann die Maßnahme umgesetzt werden?

UMSETZUNG (BEISPIELE)

Integriertes Lernen (blended learning) via

- ☐ Individualisierte Mitarbeiterschulungen intern oder durch externe Trainer
- ☐ Kurzbriefings zu Schichtbeginn
- ☐ Vorträge auf Unternehmensveranstaltungen (Betriebsversammlung)
- ☐ Führungskräfteschulung als Multiplikator
- ☐ E-Learning

Integrierte und systematische Kommunikation über alle Kanäle

- ☐ Schaffen Sie eine Rubrik „Sicherheit" im Intranet oder integrieren Sie Ihre Sicherheitsthemen in Newslettern, der Mitarbeiterzeitung o.ä.
- ☐ Stellen Sie dort sich als Person, Ihre Aufgaben, Tätigkeiten und Ihren Zuständigkeitsbereich vor
- ☐ Entwerfen und verteilen Sie Faltblätter mit unternehmensspezifischen Sicherheitsinformationen
- ☐ Entwickeln Sie eine Art „Welcome Kit" mit allen sicherheitsrelevanten Basisinformationen für neue Mitarbeiter und verteilen Sie diese an die Personalabteilung
- ☐ Setzen Sie auf kreative Security Awareness-Poster an besonders stark frequentierten Orten, wie z. B. Fahrstuhl, Zentraldrucker, Pausenraum, Kantine etc.
- ☐ Produzieren Sie kleine (Sicherheits-) Videos/Audios mit Mitarbeitern aus ihrem Unternehmen (sog. „story telling")
- ☐ Erstellen Sie ein Sicherheitsquiz oder -rätsel (sog. „game based developments")
- ☐ Kleine „give aways" können große Wirkung erzielen, wie z. B. Webcam-Abdeckung, PC-Sichtschutzfolie, PC-Bildschirmschoner etc.


©weerapat1003/Fotolia

„CEO-FRAUD“: SICHERHEITSBEHÖRDEN WARNEN EINDRINGLICH VOR NEUER BETRUGSMASCHE

Was würde ihre Finanzabteilung tun, wenn sie eine E-Mail oder eine Anweisung einer (vermeintlichen) Person aus der Führungsebene erhält, in der sie dazu aufgefordert wird, einen größeren Geldbetrag zu überweisen? Genau dieses Phänomen beschreibt CEO-Fraud. Beugen Sie dieser Betrugsmasche mit entsprechenden Maßnahmen vor.

Die ersten Fälle dieser Art von Internetkriminalität traten 2013 auf. Man geht mittlerweile von hunderten betroffenen und geschädigten Unternehmen allein im deutschsprachigen Raum aus. Genauere Zahlen sind nicht bekannt, da viele Unternehmen den Gang an die Öffentlichkeit scheuen. Weltweit belaufen sich die Schäden in Milliardenhöhe.

VORSICHT VOR ÜBERWEISUNGSAUFTRÄGEN DES CHEFS

Bei der Betrugsmasche des CEO-Fraud geben sich die Betrüger als vermeintliches Mitglied der Unternehmensführung, Führungskraft oder Handelspartner aus und fordern im Vorfeld ausgeforschte Mitarbeiter dazu auf, größere Geldsummen von einem Unternehmenskonto aus vermeintlich berechtigten Gründen auf ein ausländisches Konto (meist mit den Transferzielen Hongkong, China oder Osteuropa) zu überweisen.

> „VORSICHT VOR ÜBERWEISUNGSAUFTRÄGEN DES „CHEFS“

Der vermeintliche Überweisungsauftrag kann mittels E-Mail, bei der der Absender manipuliert ist, gefälschter Briefpost mit Behördenstempel, Hoheitszeichen oder Freigabeunterschriften von Vorstandsmitgliedern erfolgen.

Zur Betrugsvorbereitung setzen die Betrüger auf Social Engineering. Sie sammeln im Vorfeld Insiderinformationen zu unternehmerischen Prozessen und Vorgängen und kundschaften Mitarbeiter, z. B. mit Hilfe von Profilen in sozialen Netzwerken, aus. Sämtliche öffentlichen Angaben zu Personen und zum Unternehmen wie Handelsregisterauszüge, Wirtschafts- und Medienberichte, Werbebroschüren oder die unternehmenseigene Website, auf der Telefonnummern, Organigramme und dergleichen zu finden sind, werden in Erfahrung gebracht. Besonders interessant sind hierbei E-Mail-Adressen des Unternehmens, Investments und Geschäftspartner. Die betroffenen Mitarbeiter arbeiten meist in der Buchhaltung oder dem Rechnungswesen.

DAS VORGEHEN DER TÄTER

Die erhaltenen E-Mails weisen Hinweise zu geänderten Bankverbindungen, angeblichen Unternehmensübernahmen oder dergleichen aus. Die Täter schmeicheln mit netten Worten im Hinblick auf die Vertrauenswürdigkeit oder Verlässlichkeit der Person und bauen mit einem Geheimhaltungshinweis und dem nötigen Zeitdruck Stress auf. So wirkt die Überweisungsaufforderung dann auch entsprechend wichtig. Rückfragen sind nur über E-Mail erwünscht oder unter einer Telefonnummer, bei der eine vermeintliche Anwaltskanzlei in Form der Betrüger erreichbar ist. Es ist nachvollziehbar, wenn Mitarbeiter in einer solchen Situation nervös werden. Hinzu kommen hierarchische Strukturen, in denen die Mitarbeiter die Entscheidungen von Vorgesetzten nicht hinterfragen.

SO KÖNNEN SIE SICH SCHÜTZEN

Auf bekanntgewordene Betrugsmaschen kann man sich vorbereiten, indem man frühzeitig mit den entsprechenden Abteilungen Kontakt aufnimmt und gemeinsam eruiert, ob derartige Betrugsphänomene dort bereits bekannt sind und wie mit Überweisungsaufträgen verfahren wird. Gerade patriarchalisch-autoritär geführte Unternehmen, in denen Zweifel und Widerspruch unerwünscht sind, sind am häufigsten von Überweisungsbetrügereien betroffen.

Die örtlichen Polizeidienststellen und die Landeskriminalämter stehen Ihnen diesbezüglich mit weiteren Informationen zur Seite. Die Sicherheitsbehörden gehen auch gezielt auf Unternehmen zu, bei denen bekannt ist, dass gefälschte E-Mail-Adressen im Umlauf sind. Davon betroffen sind keinesfalls nur Konzerne, sondern auch Werkstätten, Autohäuser, Maschinenbauer, Handwerksbetriebe, Sportvereine, soziale Einrichtungen und dergleichen.

SINNGEMÄSS BEDEUTET CEO-FRAUD „GESCHÄFTSFÜHRER-BETRUG". CEO-FRAUD IST EINE BETRUGSMASCHE, BEI DER FIRMEN UNTER VERWENDUNG FALSCHER IDENTITÄTEN ZUR ÜBERWEISUNG VON GELDBETRÄGEN MANIPULIERT WERDEN.

CEO-Fraud ist als Betrugsmasche der organisierten Kriminalität nicht von der Hand zu weisen. Jedes Unternehmen sollte sich darauf vorbereiten.

EINIGE GENERELLE SCHUTZVORRICHTUNGEN SOLLTEN SIE ERRICHTEN:

1. Weisen Sie alle Mitarbeiter an, grundsätzlich sensibel bei der Preisgabe von unternehmerischen Informationen zu sein.

2. Unternehmensbezogene E-Mail-Adressen sollten für die private Registrierung bei Onlinediensten nicht verwendet werden.

3. Informieren Sie die betroffenen Mitarbeiter über die Betrugsmasche und ziehen Sie gemeinsam Rückschlüsse auf die unternehmerischen Prozesse. Appellieren Sie an ein besonnenes Vorgehen: Würde der Geschäftsführer diejenige Person wirklich per E-Mail bitten, größere Summen ins Ausland zu überweisen?

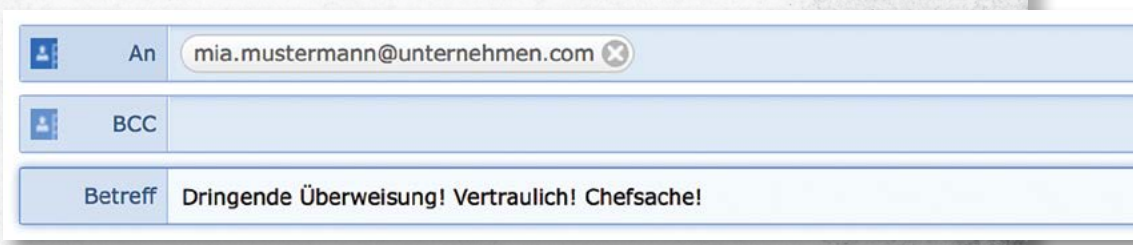
4. Führen Sie Verhaltensregeln und Kontrollmechanismen ein.

5. Derartige Überweisungsanweisungen sollten persönlich über einheitliche und bekannte Wege und Telefonnummern verifiziert werden oder zumindest mit der Abteilungsleitung abgestimmt sein.

6. Die Schreibweisen von E-Mail-Adressen müssen stets überprüft werden (vertauschte Buchstaben, ein Punkt statt ein Bindestrich, 0 statt O etc.). Fachkundige Personen können auch die Absenderadresse prüfen. Wenden Sie sich hierzu an die IT-Abteilung.

7. Informieren Sie Mitarbeiter, die Überweisungen tätigen können, an wen sie sich bei Verdachtsmomenten vertrauensvoll wenden können (interne Ansprechpartner, Bankberater, Polizei etc.).

8. Überprüfen Sie das routinierte Vorgehen der Mitarbeiter, indem Sie zu Testzwecken selbst einmal fingierte E-Mails versenden.



EU-RICHTLINIE ZUM SCHUTZ VON GESCHÄFTS-GEHEIMNISSEN: EMPFEHLUNGEN ZUR UMSETZUNG

Am 05.07.2016 wurde die „Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung" in Kraft gesetzt. Wie Sie sich als Unternehmen auf die Umsetzung dieser Richtlinie vorbereiten können, lesen Sie im Folgenden.

Der Anwendungsbereich der VO (EU) Nr. 2016/943 erfasst Vorschriften für den Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb, rechtwidriger Nutzung und rechtswidriger Offenlegung. Der europäische Gesetzgeber hat hierzu den Begriff des „Geschäftsgeheimnisses" definiert.

GEHEIMHALTUNGSSCHUTZMASSNAHMEN SIND NOTWENDIG

An den „Geheimhaltungswillen des Geheimnisträgers" wurden bisher keine hohen Anforderungen gestellt. Dies ändert sich mit der neuen Richtlinie, denn die EU fordert angemessene Geheimhaltungsschutzmaßnahmen. Demzufolge sind unternehmensinterne Informationen nicht mehr als Geschäftsgeheimnis geschützt, wenn die Angemessenheit der Maßnahmen nicht nachgewiesen werden kann. Um der drohenden Rechtsunsicherheit vorzubeugen und sich optimal vorzubereiten, empfehlen wir Ihnen die folgenden Maßnahmen:

- Unterteilen Sie ihre Geschäftsgeheimnisse in unterschiedliche Geheimhaltungsstufen.
- Kennzeichnen Sie ihre Daten explizit als intern/vertraulich/geheim/streng geheim.
- Überprüfen Sie alle Vertragswerke (auch Arbeitsverträge) und passen Sie diese an die neuen Regelungen an.
- Erfassen Sie alle Mitarbeiter, die Kenntnis von Geschäftsgeheimnissen haben.
- Überprüfen Sie in diesem Zusammenhang Berechtigungskonzepte (IT-Systeme, Zutrittsberechtigungen etc.).
- Schulen Sie ihre Geheimnisträger im Umgang mit sensiblen Daten.

Somit können Sie mit einfachen Maßnahmen die Erfolgsaussichten eines hypothetischen Gerichtsverfahrens wegen Geheimnisverrats erheblich steigern. Führen Sie das Prinzip der Datensparsamkeit auch in ihrem Unternehmen ein, um den neuen Regularien gerecht zu werden und ihr Know-how bestmöglich zu schützen. Auch hier kann Sie die Einführung eines Sicherheitsmanagementsystems unterstützen.

DEFINITION „GESCHÄFTSGEHEIMNIS" GEMÄSS EU-VERORDNUNG

Geschäftsgeheimnisse sind in dem Sinne geheim, als dass sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich sind. Sie sind von kommerziellem Wert, weil sie geheim sind und sie sind Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person, die die rechtmäßige Kontrolle über die Informationen besitzt.

KRISEN- UND NOTFALLMANAGEMENT: WARUM JEDES UNTERNEHMEN EIN SOLCHES SYSTEM VORHALTEN SOLLTE

Kleinere Störungen wie kurzfristige Stromausfälle, defekte Geräte oder Lieferverzögerungen gehören zum betrieblichen Alltag. Länger andauernde Störungen, Notfälle und Krisen, die den Betrieb massiv beeinträchtigen und somit erheblichen Schaden anrichten können, ereignen sich hingegen seltener. Lassen Sie sich nicht von unerwarteten Ereignissen überraschen. Bereiten Sie sich mit einem umfassend und nachhaltig geplanten Krisen- und Notfallmanagement (KNM) darauf vor.

Vor Unglücksfällen ist niemand gefeit: Das gilt für große Konzerne ebenso wie für kleine und mittelständische Unternehmen. Mögliche Auslöser können beispielsweise Unwetter, Hochwasser, Stromausfälle, kriminelle Eingriffe, technische Defekte oder menschliches Versagen sein. Die Ursache liegt nicht immer im betrieblichen Geschehen begründet. Schäden beziehen sich dabei nicht immer nur auf technische Anlagen und die Funktionsfähigkeit des Unternehmens, sondern ggf. auch auf Menschenleben. Ein holpriges Krisenmanagement und eine unglaubwürdige Krisenkommunikation können in solchen Fällen nachhaltige Imageschäden zur Folge haben. Die Bewusstseinsbildung sowie die Sensibilisierung im Umgang mit Risiken von bisher undenkbarer Art und Ausmaß bilden den Grundstein jeder durchdachten Krisenvorsorge.

RECHTLICHE GRUNDLAGEN ZUM VORHALTEN EINES KRISEN- UND NOTFALLMANAGEMENTS

Viele Unternehmen haben den Mehrwert eines koordinierten und strukturiert aufgebauten KNM noch nicht erkannt, da es keinerlei umfassende rechtliche Grundlagen zur Vorhaltung eines solchen Systems gibt. Lediglich für Betreiber kritischer Infrastrukturen und einige wenige andere Bereiche ist dies vorgeschrieben. Eine Notwendigkeit leitet sich aber dennoch aus der Fürsorge- und Sorgfaltspflicht gegenüber Mitarbeitern und Dritten sowie der grundsätzlichen Verantwortung gegenüber der Umwelt oder aufgrund der Unternehmerpflichten ab. Es sollten daher geeignete Vorsorgemaßnahmen implementiert werden, die vor Gefahren schützen. Konkret bezieht sich das auf die folgenden Themen. ›››

ANWEISUNGSPFLICHTEN

- Notfall-/Krisenplan
- Telefonlisten
- Unterweisung der Mitarbeiter

AUSWAHLPFLICHTEN

- fachkundige Personen benennen
- Entscheidungsträger definieren

KONTROLLPFLICHTEN

- Einhaltung von Vorschriften und Anweisungen

In jedem Unternehmen hängen beispielsweise Flucht- und Rettungswegpläne sowie Hinweisschilder zur Sammelstelle (ehem. Sammelplatz) aus, was auf gesetzlichen Bestimmungen beruht. Dies zielt auf die operative Schadensbekämpfung ab. Wenn ein Gebäude aber beispielsweise geräumt werden muss, sollte dies nicht ad hoc geschehen, sondern mit einer hinterlegten Bewältigungsstrategie – dem KNM. Das bedeutet: schnelle Entscheidungen müssen getroffen werden, eine zügige Alarmierung muss – mittels strukturierter Kommunikation an alle Betroffenen – erfolgen und klare Anweisungen müssen erteilt werden. Wenn eine Führung fehlt, gibt es Kopflosigkeit und Autoritätsgehabe. Oftmals reagieren Betroffene erst dann auf einen gravierenden Ereignisfall, wenn dieser schon in vollem Gange ist. Doch das ist meist schon zu spät. Mit der richtigen Vorbereitung auf das „Unerwartete" könnte so mancher Ereignisfall souveräner und durchdachter bewältigt werden, um schnellstmöglich in den Normalbetrieb zurückzukehren oder das Schadensausmaß zumindest in Teilen zu minimieren.

Dies gelingt allerdings nur, wenn Sie sich mit „typischen Ausfallszenarien" und Hypothesen möglicher Erscheinungsformen im Unternehmen auseinandersetzen. Die Horizonterweiterung hilft bei der Frage: Was werden wir tun, wie können wir reagieren? Können wir den Verlauf lenken? Welche Ressourcen sind verfügbar? Wo sind unsere Stärken und Schwächen? Denn grundlegende Abläufe für Notfälle, Krisen und Katastrophen sind planbar.

WOMIT BEFASST SICH DAS KRISEN-UND NOTFALLMANAGEMENT KONKRET?

Ein adäquates Krisen- und Notfallmanagement kann potentielle Gefahren zwar nicht vollständig eliminieren, doch es ermöglicht die souveräne Handlungsfähigkeit und eine beschleunigte Wiederaufnahme essentieller (Geschäfts-) Prozesse und somit der Wertschöpfung des Unternehmens.

FRAGEN, DIE SICH IHR MANAGEMENT NACH EINEM KRISENFALL STELLEN MUSS

Wenn Sie sich mit der Führungsebene diesbezüglich austauschen, sollten Sie darauf achten, dem Wort „Krise" den negativen Beigeschmack zu nehmen. Krise bedeutet eine beschleunigte Veränderung und somit das Herauskommen aus der Komfortzone „Zeit". Das Managen von Krisen kann aber zugleich das Managen von Chancen sein, wenn man gut vorbereitet ist. Viele Führungspersonen sind der Annahme, dass derartige Notfall- oder Krisensituationen, welche die Existenz bedrohen, zu abstrakt sind. Doch so überzogen und unwahrscheinlich einige Szenarien auch sein mögen, die Erfahrung der Praxis zeigt, dass niemand vor Notfall- und Krisenlagen gefeit ist und sich das Management folgenden Fragestellungen gegenübersieht:

- Was bedeutet der Infrastrukturausfall für unser Unternehmen?
- Welche Kunden/Geschäftspartner sind betroffen?
- Sind die Kunden-, Unternehmens- und Forschungsdaten gesichert?
- Wurden Mitarbeiter geschädigt?
- Wer informiert die Angehörigen?
- Gibt es Ausweicharbeitsplätze?
- Hätten wir mehr tun sollen?
- Wer ist schuld?

Die Kette an Fragen ist im Ereignisfall immens. Ein professionell aufgebautes Krisen- und Notfallmanagement bereitet einen Großteil der Fragen bereits im Vorfeld auf und erleichtert die Handlungsfähigkeit in kritischen Situationen. Ein Krisen- und Notfallmanagementsystem dient dazu, Schaden zu verhindern bzw. dessen Ausmaß zu minimieren und somit den Fortbestand des Unternehmens zu sichern sowie die Reputation zu wahren. Im Wesentlichen zielt das Krisen- und Notfallmanagement darauf ab, das Ereignis einzugrenzen, einen definierten Notbetrieb zu starten und eine angemessene Krisenreaktion zu ermöglichen, um dadurch eine Ausweitung des Schadens zu verhindern, insbesondere im Hinblick auf:

- das Leben und die Gesundheit von Menschen
- Sachwerte und Finanzen

- die betriebliche Kontinuität
- rechtliche Haftungen
- die eigene Reputation

Ein Krisen- und Notfallmanagementsystem basiert stets auf den individuellen unternehmensspezifischen Anforderungen sowie den finanziellen, personellen und technischen Möglichkeiten.

©Martina Berg/Fotolia

DER AUFBAU EINES KRISEN- UND NOTFALLMANAGEMENTS

Die Implementierung eines zweckmäßigen und nachhaltigen Krisen- und Notfallmanagementsystems bedarf einer professionellen und intensiven Vorbereitung und Organisation. Hierzu zählen u. a. folgende Maßnahmen:

- ☐ ausführliche Analyse der kritischen Prozesse des Unternehmens
- ☐ Erstellung von Maßnahmenkatalogen für einzelne Szenarien je nach Risikoabwägung
- ☐ Definieren von Ablaufplänen und Meldeketten
- ☐ Aufbau eines Krisenstabs inkl. Stellvertreterregelung
- ☐ Erstellung von Krisenkommunikationsplänen
- ☐ zielgruppenspezifische Schulungs- und Sensibilisierungsmaßnahmen
- ☐ regelmäßige Übungen unter realistischen Bedingungen

Die Auseinandersetzung und somit ganzheitliche Betrachtung der Risiken, die schwer zu beeinflussen sind oder ein großes Schadenspotential besitzen, ist der Weg zur Bewältigung einer Krise, welche auf diese Weise beherrschbarer wird.

Das System muss kontinuierlich optimiert werden, um auf veränderte Rahmenbedingungen zu reagieren und aus Praxiserfahrungen zu lernen. Das regelmäßige Üben unterschiedlichster Gefahrensituationen mit unterschiedlichen Beteiligten, Mitarbeitersensibilisierungen und Führungskräfteschulungen sowie die stetige Erweiterung und Überprüfung des Krisen- und Notfallmanagementsystems sind dazu ein wesentlicher Bestandteil. Nur so steht einer „planmäßigen“ Bewältigung eines Ereignisses durch eine erfolgreiche Umsetzung aller Beteiligten nichts mehr im Wege.

Darstellung der unterschiedlichen Einflüsse auf mögliche Unternehmensbereiche

©Micha Klootwijk/Fotolia

REISESICHERHEIT IM AUSLAND: WEIT MEHR ALS „NUR“ GESUNDHEITSSCHUTZ

Die zunehmende Globalisierung und die Vernetzung der Märkte führt zwangsläufig dazu, dass mehr Geschäftsreisen unternommen werden. Besonders, wenn es um die Erschließung neuer Märkte in kritischen Territorien oder Entwicklungsländern geht, dürfen Unternehmen nicht wählerisch sein. Die Risiken einer Reise spielen dabei eine sekundäre Rolle, doch genau im Risikomanagement und dem Schutz der eigenen Mitarbeiter liegt der Knackpunkt der Reisesicherheit.

Ob Unfälle, Krankheiten, kriminelle Übergriffe, Naturkatastrophen, politische Unruhen, terroristische Akte, Industrie- und Wirtschaftsspionage oder gar der Risikofaktor „Geschlecht“, dies alles sind Risiken, denen sich Reisende jederzeit gegenübersehen. Sicherheitsrelevante oder medizinische Vorfälle beeinträchtigen den Erfolg einer Auslandsreise oder führen sogar zum Abbruch. Dies hat zur Folge, dass die Arbeitsleistung nicht erfolgreich zu Ende gebracht werden kann. Die bestehenden Gefahren sind allgemein bekannt, dennoch gehen Reisende und Unternehmen teilweise äußerst sorglos mit ihrer Sicherheit bzw. der Sicherheit ihrer Mitarbeiter um. Doch man kann und muss sogar aktiv etwas unternehmen, um die Reiserisiken zu minimieren und ein Risiko- und Sicherheitsbewusstsein zu schaffen.

Da sich Sicherheit nur schwer messen lässt, ist es für Sicherheitsverantwortliche besonders schwierig, den Nutzen einer Maßnahme betriebswirtschaftlich darzustellen. Sicherheit erzielt keinen Gewinn, sondern hat den primären Zweck, Schaden zu verhindern. Aber gerade im Bereich der Reisesicherheitsmaßnahmen kann mit gesetzlichen Verpflichtungen argumentiert werden.

DEN PRÄVENTIVEN SCHUTZMASSNAHMEN ALS ARBEITGEBER GERECHT WERDEN

Das Hauptrisiko des Unternehmens bei Reisen im In- und Ausland ist das Haftungsrisiko. Die Fürsorgepflicht des Arbeitgebers resultiert aus den §§ 241, 617-619 BGB, die sich auf die Verpflichtung zu präventiven Schutzmaßnahmen beziehen. Hierzu zählen neben der Sicherstellung des Sozialversicherungs- und Gesundheitsschutzes der Abschluss einer Unfallversicherung und die Veranlassung möglicher Schutzimpfungen oder notwendiger Vorsorgeuntersuchungen (bspw. Tropentauglichkeit) für das Reiseland. Bei länger andauernden Aufenthalten sollten Schutzmaßnahmen vor Ort ebenso eruiert werden wie die persönliche Eignung und Gesundheit des Reisenden. Dies ist hinlänglich bekannt. Aber es gibt weitere Unternehmerpflichten, die bei Auslandsreisen greifen.

Räume, Vorrichtungen oder Gerätschaften sind ebenfalls so einzurichten und zu unterhalten, dass Mitarbeiter gegenüber Gefahren für Leib und Leben geschützt sind. Mit diesen Maßnahmen lässt sich aber lediglich das Haftungsrisiko minimieren, sie führen aber keinesfalls zur Enthaftung. Weitere Forderungen beziehen sich aber auch auf die Informationsverpflichtung vor und während der Reise, die sich aus dem Arbeitsschutzgesetz ableiten lassen.

> *HAFTUNGSBEISPIEL:*
> *EIN MITARBEITER WIRD IM REISELAND IN EINEN UNFALL VERWICKELT. NOTVERSORGUNG DURCH RETTUNGSKRÄFTE UND KRANKENHÄUSER IM REISELAND. RÜCKHOLUNG DES MITARBEITERS. DIES FÜHRT ZU ENORMEN KOSTEN, FÜR DIE DAS UNTERNEHMEN AUFKOMMEN MUSS.*

Dies beinhaltet die Analyse möglicher Risiken, die Aufklärung der Mitarbeiter zum Verhalten auf Reisen und die Reisevorbereitung. Reisende sollten stets aktuell über alle sicherheitsrelevanten Aspekte, etwaige Besonderheiten und lokale Rechtsvorschriften informiert werden. Aber auch Entscheidungsträger sind zu definieren, die 24/7 erreichbar sind und Rückholpläne sind auszuarbeiten. Über einschlägige Versicherungen sollte man ebenso nachdenken wie über interkulturelle Trainings oder Sicherheitstrainings, um der Erfüllung der Fürsorgepflicht zusätzlich nachzukommen. Die Intensität der Fürsorgepflicht bestimmt sich nach der Art und Dauer des Auslandseinsatzes, dem Reiseland und vor allem dem Risikoprofil. Die Maßnahmen müssen bezogen auf den Einzelfall angemessen, erforderlich und zumutbar sein. Aber auch der reisende Mitarbeiter hat

©Sergey Nivens/Fotolia

die Mitwirkungsverpflichtung, sich an die Vorgaben und Abläufe zu halten.

MASSNAHMEN, DIE ES IN PUNCTO REISESICHERHEIT GEBEN SOLLTE:

- Ansprechpartner definieren, an die sich ihre Mitarbeiter 24/7 wenden können.
- Informationsbereitstellung vor der Reise.
- Datendiebstahl vorbeugen mit Verhaltensempfehlungen.
- Das Wissen, wo sich ihre Mitarbeiter aufhalten.
- Aktuelle Informationen an Reisende weitergeben.
- Kenntnis der Vor-Ort-Kontakte bzgl. Verlust von Papieren etc.
- Rückholpläne bei Erkrankung bzw. Pläne zur Erstversorgung auf europäischem Niveau.
- Evakuierungspläne bei politischen Unruhen, Naturereignissen, Epidemien etc.

EINE INHALTSÜBERSICHT EINER REISE- UND SICHERHEITSRICHTLINIE HABEN WIR ONLINE FÜR SIE ZUR VERFÜGUNG GESTELLT.

DEN FORDERUNGEN KÖNNEN SIE NUR NACHKOMMEN, WENN SIE

1. Eine Reisesicherheitsrichtlinie herausgeben (Kontaktpersonen, Ansprechpartner, Verhalten auf Reisen, Handlungsempfehlungen, Faustregeln etc.).
2. Eine medizinische Gesundheitsbetreuung vor, während und nach der Reise implementieren.
3. Bei Reisen in Krisengebiete eine rechtliche Beratung und die Versicherer mit ins Boot holen.
4. Für jedes Land, in dem sie tätig sind, aktuelle Sicherheitsinformationen sowie Informationen zu Kontaktpersonen, Bedrohungslagen etc. für ihre Mitarbeiter zur Verfügung stellen.
5. In Spezialfällen sollte es persönliche Gespräche mit Mitarbeitern geben, um explizit Fragestellungen zu erörtern.

Alle Maßnahmen sollten einfach in bestehende Prozesse im Unternehmen integrierbar und für alle Mitarbeiter verfügbar und verständlich sein. In unserem Downloadbereich finden Sie eine Inhaltsübersicht einer Reise- und Sicherheitsrichtlinie, die Sie im Unternehmen einsetzen können.

Vorbereitende sowie begleitende Reisesicherheitsmaßnahmen und belastbare Notfallprozesse können die Risiken auf Auslandsreisen wirksam minimieren, Folgen von Vorfällen mindern und zudem das Sicherheitsgefühl der Mitarbeiter erhöhen. Gesunde Vorsicht hat nichts mit Paranoia zu tun, sondern es ist wichtig, dass man die Gefahren und Risiken einer Reise kennt und diese ernst nimmt.

INTERVIEW MIT TOBIAS PUNDSCHUS

Abteilungsleiter Unternehmenssicherheit, Notfall– und Krisenmanagement, Flughafen Hannover

Tobias Pundschus hat als Diplom-Verwaltungswirt mit der Befähigung für den Höheren Dienst seine beruflichen Wurzeln bei der Bundespolizei. Während seiner langjährigen polizeilichen Tätigkeit oblag ihm u. a. die Leitung verschiedener Bundespolizeiinspektionen in grenzpolizeilichen und luftsicherheitsrechtlichen Aufgaben. Des Weiteren war Herr Pundschus als Dozent für Recht und polizeiliche Einsatztaktik an verschiedenen Polizeischulen der Bundespolizei in Walsrode und Lübeck tätig. Seit Oktober 2006 ist er als Abteilungsleiter Unternehmenssicherheit und Notfall- und Krisenmanagement am Flughafen Hannover-Langenhagen für das Security Management-System des Flughafenbetreibers verantwortlich. Zudem lehrt er seit mehreren Jahren im Studiengang „Risiko- und Sicherheitsmanagement“ an der Hochschule für Öffentliche Verwaltung in Bremen Themen der „Aviation Security“. Zusätzlich ist er in mehreren Arbeitsgruppen verschiedener Luftfahrtverbände in Sicherheitsfragen aktiv.

HERR PUNDSCHUS, ZU ALLERERST MÖCHTE ICH IHNEN RECHT HERZLICH ZUM DIESJÄHRIGEN OUTSTANDING SECURITY PERFORMANCE AWARD (OSPA) IN DER KATEGORIE „HERAUSRAGENDE SICHERHEITSPARTNERSCHAFT“ GRATULIEREN. WAS HAT SIE DAZU VERANLASST, SICH FÜR DIESEN AWARD ZU BEWERBEN?

Vielen Dank für Ihre Glückwünsche. Der OSPA würdigt die Leistungen von Personen und Unternehmen, die sich in Sicherheitsaufgaben besonders verdient gemacht haben. Am Flughafen Hannover-Langenhagen pflegen wir eine langjährige von Vertrauen und Transparenz geprägte Sicherheitspartnerschaft mit den Behörden des Bundes und des Landes, der Stadt und Region Hannover, der Stadt Langenhagen, den Airlines, Sicherheitsdienstleistern und anderen. Wir haben uns für eine Bewerbung entschieden, da diese Auszeichnung u. a. die Möglichkeit schafft, unseren Partnern auf eine ganz besondere Art und Weise „Danke“ zu sagen.

MIT DEM DEUTSCHEN FUSSBALLBUND UND DEM KOMPETENZZENTRUM INTERNATIONALE SICHERHEIT STANDEN SIE IN EINEM ZIEMLICH HARTEN WETTBEWERB IN DER KATEGORIE „HERAUSRAGENDE SICHERHEITSPARTNERSCHAFT“. WARUM HAT GERADE IHR KONZEPT DIE JUROREN ÜBERZEUGT?

Mit den terroristischen Anschlägen von Brüssel und Istanbul ist deutlich geworden, dass nun auch die öffentlichen Bereiche der Flughäfen zum Ziel von Attentätern geworden sind. Wie alle Flughäfen in Deutschland setzt auch der Flughafen Hannover-Langenhagen alles daran, Passagiere, Gäste und Beschäftigte vor Bedrohungen bestmöglich zu schützen.

Hierfür haben die beteiligten Partner gemeinsam mit dem Flughafenbetreiber in den vergangenen Jahren eine Vielzahl von Maßnahmen umgesetzt und in Übungen und Einsätzen trainiert und erprobt. Zur Festigung aller Prozesse finden regelmäßige Notfallübungen statt. Herausragend hierbei waren die Großübungen Exaflight2009 und HAJ_ex2014. In diesen Vollübungen haben wir über 12 Stunden mit jeweils weit über 1000 Teilnehmern die Massengeiselnahme von Passagieren in einem Luftfahrzeug und einen Flugzeugabsturz als Großschadenslage unter absoluten Realbedingungen geübt. Beide Übungen dauerten in ihren Vorbereitungen jeweils weit über 1 Jahr. Diese besondere und bis dahin einzigartige Form der Zusammenarbeit mit unseren Sicherheitspartnern hat die Jury der OSPA augenscheinlich überzeugt.

OHNE EINE VERNETZUNG IN SICHERHEITSFRAGEN ERREICHT MAN NUR WENIG, UM LETZTLICH DAS RISIKO FÜR DAS UNTERNEHMEN ZU MINIMIEREN.
WIE SCHÄTZEN SIE DEN STELLENWERT VON SICHERHEIT IN UNTERNEHMEN (INBESONDERE BEI KLEINEN UND MITTELSTÄNDISCHEN UNTERNEHMEN) EIN?

Ich lese immer wieder Beiträge vom „stiefmütterlichen Dasein“ der Sicherheitsabteilungen in Unternehmen und, dass sie dort häufig zu wenig wahrgenommen werden oder dass es gar keine Abteilung oder Verantwortlichen für dieses Thema gibt. Das ist natürlich kein erfreulicher Zustand. Der Stellenwert von Unternehmenssicherheit leitet sich meiner Meinung nach maßgeblich vom eigenen Rollenverständnis ab. Es reicht eben nicht mehr aus, mit erhobenem Zeigefinger belehrend und vorschreibend das Thema Sicherheit in den alleinigen Fokus zu stellen und bei Nichtbeachtung mit Phrasen von „Haftung“ und „Verantwortung“ oder Ähnlichem zu argumentieren. So gewinnt man keine Mehrheiten in der Belegschaft und nimmt niemanden mit. Vielmehr gilt es zu verdeutlichen, dass ein gut aufgestelltes Sicherheitsmanagement die unternehmerischen Prozesse absichert und – je nach Unternehmen – ein eigener Kernprozess ist.

SICHERHEIT IM UNTERNEHMEN WIRD VON VIELEN VERANTWORTLICHEN NACH WIE VOR MIT DEM KLASSISCHEN WACHMANN, DEM METERHOHEN ZAUN UND DER RUNDUM-VIDEOÜBERWACHUNG ASSOZIIERT.
DOCH SICHERHEIT IST WESENTLICH UMFASSENDER UND KANN AUCH MEHR LEISTEN, WENN SIE RICHTIG GEHANDHABT WIRD.
WELCHE BEREICHE GEHÖREN AUS IHRER SICHT UNTER EINEN HUT?

Fragmentierungen von Zuständigkeiten bewirken uneinheitliche Sicherheitsstandards und Inkonsistenzen zu internen sowie externen Schnittstellen. Eingeschränkte Durchgriffsmöglichkeiten der Unternehmenssicherheit bei Entscheidungen in Sicherheitsfragen und unterschiedliche Ansprechpartner für Dritte – durch die Verteilung von Verantwortlichkeiten im Unternehmen bei Sicherheitsthemen – erschweren die Nachhaltigkeit und Effizienz. Schon im Allgemeinen Preußischen Landrecht wurde erkannt, „Wem die Gesetze ein Recht geben, dem bewilligen sie auch die Mittel, ohne welche dasselbe nicht ausgeübt werden kann.“. Und so ist es auch heute noch. Unternehmenssicherheit muss von allen Bereichen als strategischer Begleiter unternehmerischer Prozesse verstanden werden und auch als solcher eingebunden sein.

VERSTEHE ICH SIE RICHTIG, DASS AUS IHRER SICHT ALLE BEREICHE DER SICHERHEIT GEBÜNDELT WERDEN SOLLTEN?

Ja. Ich sehe das so.
Know-how, Transparenz und Professionalität in den operativen Prozessen sowie eine echte „Governance“-Funktion sind die Eckpfeiler eines nachhaltigen Security Management-Systems für Unternehmen. Ich favorisiere ein interdisziplinäres kooperatives Security Management-System unter der verantwortlichen koordinierenden Federführung der Unternehmenssicherheit, in dessen Fokus Maßnahmen der Sicherheit für Menschen, betriebsnotwendige Infrastrukturen und schützenswerte Informationen vor kriminellen Übergriffen von innen und außen stehen.

Hier ist der Leiter der Unternehmenssicherheit gefragt. Der Verantwortungsbereich muss personell und fachlich so aufgestellt sein, dass Expertisen aus Erfahrungen in allen Bereichen, Quelleninformationen, Verbandstätigkeiten und lokalen und/oder überregionalen Sicherheitsnetzwerken durch die Unternehmenssicherheit bereitgestellt werden können.

VIELE SICHERHEITSTHEMEN SIND IN DEN VERGANGENEN JAHREN DURCH DIE MEDIEN GEGANGEN: CYBERSICHERHEIT, DATENSCHUTZ, SOCIAL ENGINEERING, CEO-FRAUD, KNOW-HOW-SCHUTZ, BEDROHUNGSMANAGEMENT, UM NUR EINIGE ZU NENNEN. WIE SEHEN SIE KÜNFTIGE ENTWICKLUNGEN DER SICHERHEITSBRANCHE?

Für Unternehmen mit öffentlich zugänglichen Bereichen wie Flughäfen werden auch zukünftig die Bedrohungslagen aus terroristisch motivierten Anschlägen eine der Hauptbedrohungen sein. Umfangreiche bauliche, technische und prozessuale Maßnahmen in den öffentlich zugänglichen Bereichen, wie z. B. in Israel, waren bisher an deutschen Flughäfen unüblich. Die geänderte Sicherheitslage durch den internationalen Terrorismus zwingt uns zu einer neuen Bewertung von geeigneten Maßnahmen für eine wirksame Abwehrstrategie. Gleichwohl können öffentliche Räume nicht verbarrikadiert werden.

Das neue Videoüberwachungsverbesserungsgesetz vom Mai 2017 regelt die Befugnis, öffentlich zugängliche Räume mittels Videokameras zu beobachten. Betreiber „großflächiger Anlagen“ haben nun bessere Möglichkeiten einer Videoüberwachung, wenn bereits die „Erhöhung der Sicherheit der anwesenden Personen das für die Genehmigung erforderliche berechtigte Interesse des Betreibers der Anlage…“ eine Begründung darstellt.

Im Zuge der Digitalisierung rückt auch das Thema „Informationssicherheit“ neu in den Fokus.
„Informationssicherheit“ wird jedoch häufig nur aus dem Blickwinkel der IT-gestützten Informationssysteme gesehen. Ich glaube, das springt zu kurz. Informationssicherheit ist mehr als nur Datenschutz, Firewall und Werbeblocker. Die Prozesshoheit für den Schutz sicherheitssensibler Informationen und deren Absicherung vor Verlust durch Innen- und Außentäter gehören in die Verantwortung der Unternehmenssicherheit.
Zudem bedarf es klar definierter Richtlinien im Umgang mit Social Media und Social Engineering.

Zudem wird das Thema „Reisesicherheit“ zukünftig an Bedeutung gewinnen. Unternehmen agieren zunehmend globaler. Ein Blick in das Arbeitsschutzgesetz zeigt, dass dem Arbeitgeber hier gesetzliche Pflichten zugewiesen sind, denn die Beschäftigten reisen im Auftrag des Unternehmens.

Verleihung des OSPA-Awards

Die nächsten Jahre werden die Unternehmenssicherheitsverantwortlichen vor sehr komplexe Herausforderungen stellen.
Ich sehe die richtige Antwort hierauf nicht in der „Copy & Paste“-Methode bei der Entwicklung von Security Management-Konzepten. Vielmehr sind die potentiellen Risiken zu antizipieren, die dem jeweiligen Unternehmen drohen. Dessen bedrohte Schutzgüter müssen individuell ermittelt, analysiert, bewertet und mit konkreten Gegensteuerungsmaßnahmen und zugewiesenen Verantwortlichkeiten unterlegt werden. Der Erfolg dieser Maßnahmen ist verbindlich durch Audits, Trainings, Übungen und ähnlichem zu messen, um diese gegebenenfalls den Erfordernissen anzupassen.

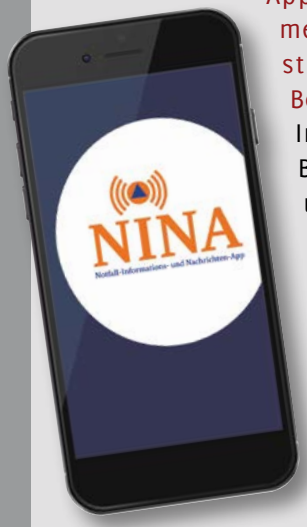
VIELEN DANK FÜR DAS INTERESSANTE GESPRÄCH UND DIE ZAHLREICHEN EINBLICKE, DIE SIE UNS AUS IHREM ARBEITSUMFELD GEWÄHRT HABEN.

In diesem Bereich stellen wir Ihnen nützliche Tools, Sicherheitsmessen sowie Behörden, Verbände und Institutionen mit Sicherheitsaufgaben vor. Zusätzlich finden Sie hier auch ausgewählte (Fach-) Bücher, die Ihnen die Welt der „Sicherheit“ noch anschaulicher vermitteln werden.

TOOL

AKTUELLE WARNMELDUNGEN FÜR IHRE STANDORTE – WARN-APP NINA

Die Warn-APP NINA („Notfall-Informations- und Nachrichten-App“) informiert Sie zeitnah mit Warnmeldungen zu Hochwasserlagen, Gefahrstoffausbreitungen, Wetterwarnungen, Bombenentschärfungen oder Großbränden.



Im Namen des Bundes betreibt das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) die Warn-App NINA. Dieser Informationskanal der zuständigen Behörden des Zivil- und Katastrophenschutzes stellt einen schnellen und effizienten Informationskanal zum Schutz der Bevölkerung dar und gibt gleichzeitig grundlegende Informationen und Notfalltipps zu den Themen des Bevölkerungsschutzes. Diese kostenfreie APP kann auf allen Smartphones installiert werden und informiert Sie via Push-Funktion über Warnmeldungen für Ihre voreingestellten Standorte.

Gute Gründe, warum Sie die Warn-APP NINA nutzen sollten:

1. Halten Sie sich stets über Gefahrenlagen ihrer Standorte informiert, um zeitnah reagieren zu können!
2. Die APP sollte auf dienstlich genutzten Smartphones installiert sein. Auch für den Privatgebrauch empfiehlt sich die Nutzung.
3. Gerade bei Geschäftsreisen innerhalb des Bundesgebietes kann eine Warnung mit entsprechenden Hinweisen nützlich sein.
4. Eine kostenfreie Alternative, um jederzeit über Gefahrenlagen ihrer Standorte informiert zu sein.

Halten Sie sich lieber einmal zu viel informiert, bevor Ihnen Gefahrenlagen entgehen!

BUCHTIPP

HANDBUCH REISESICHERHEIT

Sicher auf Reisen – geschäftlich & privat

Dieses Buch stellt eine Einführung in die umfassende Thematik der Reisesicherheit dar. Fachlich fundiert und mit vielen Praxisbeispielen erläutert, erhält der Leser praxisorientierte Handlungsempfehlungen zum Vorgehen bei Reisetätigkeiten für den privaten und geschäftlichen Gebrauch.

Welchen Risiken steht man gegenüber, wie kann man dem vorbeugen oder sich davor schützen? Was ist zu tun, wenn etwas passiert ist? Diese Fragen und Themen rund um die Vor- und Nachbereitung einer Reise sowie die Maßnahmen während der Reise werden aufgegriffen und praxisnah beschrieben. Insbesondere wird auf die Fürsorgeverpflichtungen des Arbeitgebers und die Mitwirkungspflichten des (Dienst-) Reisenden eingegangen.

Das Buch schafft eine solide Basis für sicherheitsbewusstes Handeln auf Reisen und für ihre Reisesicherheitsorganisation im Unternehmen. Nutzen Sie es als Grundlage, um die Reisesicherheitsvorkehrungen in ihrem Unternehmen zu optimieren.

ZU DEN AUTOREN

Um Ihnen die gesamte Bandbreite der Sicherheit mit fundierten und praxisnahen Einblicken vermitteln zu können, verfolgen wir bei SICHERHEIT. Das Fachmagazin. das erfolgreiche Prinzip der Mehrautorenschaft. Wir arbeiten – passend zu den spezifischen Themen – ausschließlich mit fachlich versierten Experten mit jahrzehntelanger praktischer Berufserfahrung auf den jeweiligen Gebieten zusammen.

IMPRESSUM

SICHERHEIT. Das Fachmagazin. c/o SIUS Consulting® • Dorfaue 8b • 15738 Zeuthen
Telefon: +49 (0) 30 / 700 36 96 -5 • E-Mail: kontakt@sicherheit-das-fachmagazin.de • Geschäftsführer: Michael Blaumoser
Umsatzsteuer-ID: DE279558068 • ISSN: 2569-3816 • Erscheinungsweise: 4 x pro Jahr • Bildquelle: www.fotolia.com

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.