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 KERNTHEMEN

- Wirtschaftsschutz
- Sicherheitsvorkehrungen
- Krisen- und Notfallmanagement
- Security Awareness
- Reisesicherheit

E-PAPER

SICHERHEIT. Das Fachmagazin. als ePaper bringt Ihnen alle Vorzüge eines gedruckten Magazins auf Ihren Bildschirm: ob 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 CO_2

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

„EIN „KLEINES GESPRÄCH“ KANN FÜR SIE ZU EINEM ECHTEN „MEHR AN SICHERHEIT“ FÜHREN.

Kontaktpflege

GEWINNBRINGENDER AUSTAUSCH MIT POLIZEI, FEUERWEHR UND CO.

Networking ist das A und O im Berufsleben, um sich gegenseitig zu unterstützen, neue sach- und fachdienliche Erkenntnisse zu erhalten, Kooperationen zu schließen oder Wissen effektiv miteinander zu vernetzen. Doch mal Hand aufs Herz: befinden sich in Ihrem Netzwerk auch die örtlichen Ansprechpartner von Polizei, Feuerwehr und Co.?

Ob Einbruch, Diebstahl, Industrie- und Wirtschaftsspionage, Cyberangriffe oder andere Bedrohungen – in jedem Unternehmen kann es zu Delikten kommen, die dem Strafgesetz unterliegen und somit sach- und fachkundig durch behördliche Ermittlungen aufgearbeitet und geahndet werden sollten. Aber auch im Krisenfall wie beispielsweise bei einem Brand oder beim Austritt von Gefahrstoffen haben Sie mit Behördenvertretern zu tun, die für die lückenlose Aufklärung der Vorkommnisse zuständig sind.

Gerade für derartige Ereignissituationen ist es von Vorteil, wenn man bereits im Vorfeld die zuständigen Behördenvertreter und diese ggf. wiederum sogar die Örtlichkeiten des Unternehmens kennen. Hierzu gibt es beispielsweise bei der lokalen Polizei sogenannte Kontaktbeamte (auch Kontaktpolizist, Revierpolizist, Bürgernaher Beamter oder Schutzmann vor Ort genannt), die als Ansprechpartner bzw. Schnittstelle zu Bürgern und Unternehmen fungieren. Sie erteilen polizeispezifische Auskünfte und beraten zu allgemeinen sicherheitsspezifischen Fragestellungen – insbesondere im präventiven Bereich. Darüber hinaus können sie den Kontakt zu anderen Sicherheitsbehörden vermitteln, sofern der individuelle Sachverhalt den eigenen Zuständigkeitsbereich überschreitet.

Suchen Sie am besten aktiv den Kontakt zu den zuständigen Behördenvertretern, um sich gegenseitig kennenzulernen und ggf. Ortsbegehungen zu organisieren und durchzuführen. Dies kann u. a. folgende Vorteile bieten:

- Stärkung der Zusammenarbeit („Präventionsaspekt“).
- Schnellere und effektivere Abstimmungen im Ereignisfall.
- Ggf. Vorhaltung spezieller Lagepläne zur optimalen Gefahrenabwehr im Ereignisfall.
- Vermittlung besserer Ortskenntnisse und spezifischer Besonderheiten vor Ort.
- Vorabstimmung zur Presse- und Öffentlichkeitsarbeit.
- Austausch über besondere Lagebilder und/oder Bedrohungssituationen.
- Besseres Gespür für die Tätigkeiten und Möglichkeiten des anderen.
- Abgleich der gegenseitigen Leistungsfähigkeit im Ereignisfall XY.

Derartige Gespräche sollten zum einen allgemeine kriminalpräventive Themen erörtern, die beispielsweise zum Tragen kommen, wenn der Notruf gewählt wird (Anfahrt, Ansprechpartner, Unterstützung vor Ort, ggf. separate Nummer für Rückfragen etc.). Zum anderen sollten Notfall- und Krisenszenarien sowie die ereignisspezifische Vorgehensweise, gegenseitige Erwartungshaltung und individuelle Leistungsfähigkeit miteinander abgestimmt werden, um das Krisen- und Notfallmanagement dahingehend ganzheitlich und nachhaltig zu optimieren.

KRITERIEN BEI DER AUSWAHL EINER EXTERNEN SICHERHEITSBERATUNG

Für Sicherheitsverantwortliche oder sonstige damit beauftragte Stellen im Unternehmen kann die Entscheidung, eine externe Sicherheitsberatung zu beauftragen, einen Konflikt bedeuten: Zum einen könnte dies von anderen als Wissenslücke innerhalb des eigenen Kompetenzbereichs aufgefasst werden, zum anderen ist es aber auch unmöglich, dass sich der Sicherheitsverantwortliche/die beauftragte Stelle in allen sicherheitsspezifischen Belangen vollumfänglich auskennt.

Da der Begriff „Unternehmensberater“ rechtlich nicht geschützt ist und auch keinen gesetzlich geregelten Zulassungsvoraussetzungen unterliegt, darf sich in Deutschland jeder Berater nennen, der sich dazu berufen fühlt. Gerade dieser Umstand macht es für Auftraggeber mitunter so schwierig, den „richtigen“ Sicherheitsberater zu finden. „Richtig“ bedeutet in diesem Zusammenhang, eine fachlich versierte und auf das jeweilige Aufgabengebiet spezialisierte Person zu finden, die nicht nur das Vertrauen des Auftraggebers genießt, sondern insbesondere auch über eine hinreichende auftragsspezifische Kompetenz verfügt. Denn eins muss allen Auftraggebern beim Einkauf von Sicherheitsberatungsleistungen klar sein: Sicherheit ist nicht gleich Sicherheit!

Der Einsatz externer Sicherheitsberater erfolgt meist für in sich geschlossene Projekte oder als „Interims-Lösung“ über einen bestimmten Zeitraum. Die Gründe für den Einsatz externer Sicherheitsexpertise sind vielfältig:

- fehlende interne Kapazitäten (Zeit, Personal)
- benötigtes Spezialwissen
- neutrale objektive Position
- Stärkung der eigenen Einschätzung

Was auch immer die Motivation des Auftraggebers ist: Ein Sicherheitsberater sollte neben der fachlichen Eignung immer auch persönlich zum Auftraggeber passen, um die gestellte Aufgabe und alle damit einhergehenden Hürden bestmöglich meistern zu können. Denn gerade der zwischenmenschliche Aspekt spielt in Projekten häufig eine entscheidende Rolle, insbesondere dann, wenn es während des Projekts zu speziellen zwischenmenschlichen Herausforderungen und/oder Unstimmigkeiten kommt und dabei „die Sache“ nicht immer im Vordergrund steht.

BEI DER AUSWAHL EINES SICHERHEITSBERATERS GIBT ES SO MANCHES ZU BEACHTEN

Grundsätzlich sollte ein Sicherheitsberater präventiv und reaktiv zur ganzheitlichen (Sicherheits-)Betrachtung befähigt sein. Dies bedeutet, dass er nicht nur oberflächlich die (eine) Problemstellung/Aufgabe betrachtet, sondern daraus resultierende Interaktionen ableiten sollte. Der Sicherheitsberater muss in der Lage sein, in komplexen Situationen das strategische Ziel nicht aus den Augen zu verlieren und sich somit in Einzelprobleme zu verrennen. Ein Sicherheitsberater muss ergebnis- und entscheidungsorientiert arbeiten. Die Hauptentscheidung trägt jedoch am Ende stets der Sicherheitsverantwortliche/die beauftragende Stelle im Unternehmen gemeinsam mit der Führungsebene, denn ein Berater kann stets „nur“ Varianten, Tendenzen und Lösungsmöglichkeiten aufzeigen und empfehlen. Der Sicherheitsberater sollte grundsätzlich dazu in der Lage sein, die fachliche Objektivität kontinuierlich zu wahren. Das bedeutet, dass aus fachlicher Sicht auch gegen die Meinung des Auftraggebers sachlich argumentiert werden sollte, wenn es der Sache und dem Auftraggeber dienlich ist. Denn es ist nicht Aufgabe eines externen Beraters, dem Kunden nach dem Mund zu reden.

> „EIN (EXTERNER) SICHERHEITSBERATER MUSS STETS EINE UNTERSTÜTZUNG DARSTELLEN UND/ODER HILFE ZUR (INTERNEN) SELBSTHILFE GEBEN.

3 SCHRITTE ZUR EFFEKTIVEN PERSONALAUSWAHL

1. AUFGABENSTELLUNG DEFINIEREN

Für jeden Auftraggeber ist es essenziell, dass die Aufgabe des Auftrags bereits im Vorfeld konkret festgelegt wird und nicht die erste Auftragsphase dazu genutzt wird, das eigentliche Ziel des Beratungsauftrages zu definieren. Bei komplexen Fragestellungen oder für den Fall, dass eine Sicherheitsanalyse, ein Sicherheitskonzept oder ein anderes Grundlagendokument/-system als Ausgangspunkt vorliegt und herangezogen werden soll, kann dies jedoch durchaus legitim sein. Bei einem klaren Problem sollte es jedoch stets eine klare Aufgabenstellung geben.

⇨ **HERANGEHENSWEISE:** Beratungsunternehmen können vorab telefonisch kontaktiert oder zu einem unverbindlichen Gespräch in die Räumlichkeiten des Auftraggebers eingeladen werden. Dabei sollten diese stets einheitlich und mit denselben Voraussetzungen/Anforderungen konfrontiert werden. Auf diese Weise erhält der Auftraggeber auch gleich einen fachlichen Input, beispielsweise zur Herangehensweise, Klärung von Begrifflichkeiten, Besonderheiten bei derartigen Projekten etc., welcher am Ende in die Angebotsanfrage/Ausschreibung einfließen kann. Hintergrundfragen zum Prozedere, dem zeitlichen und inhaltlichen Ablauf und den Möglichkeiten in Form von Arbeitspaketen können dabei ebenfalls eruiert werden. Somit ist der Auftraggeber am Ende in der Lage, die Anforderungen/Aufgaben detailierter in einer zweiten Runde, beispielsweise im Rahmen einer Angebotsanfrage/Ausschreibung, zu beschreiben. Dabei sollte jedoch grundsätzlich berücksichtigt werden, dass konkrete sicherheitsspezifische Themen, die am Telefon oder persönlich vor Ort besprochen werden, vorab mittels einer Geheimhaltungsvereinbarung o. ä. im Rahmen der eigenen Möglichkeiten weitestgehend „geschützt" werden sollten. Denn in den meisten Fällen geht es bei den Themen „Sicherheit" und „Sicherheitsberatung" um schützenswerte und vertrauensvolle Informationen.

Die persönliche und fachliche Eignung eines Sicherheitsberaters lässt sich nicht allein durch ein klassisches Ausschreibungsverfahren feststellen, sondern bedarf mindestens eines ausgiebigen persönlichen Gesprächs.

2. BESTMÖGLICHE EVALUATION

Der Auftraggeber sollte sich im Vorfeld ein klares und umfassendes Bild des Beratungsunternehmens und der für das Projekt vorgesehenen Fachberater verschaffen. Dies kann beispielsweise anhand der folgenden Fragen geschehen:

- Welche Personen sind in dem Unternehmen beschäftigt (Webseite, Social-Media-Profile etc.)?
- Wie steht es um die Seriosität des Unternehmens? Welches „Bild" liefern Suchmaschinenergebnisse über das Unternehmen? Hat sich das Unternehmen spezialisiert oder wird womöglich ALLES angeboten? Passt das Leistungsportfolio zum vorgesehenen Projekt?
- Finden sich Informationen zur Unabhängigkeit und Produktneutralität des Unternehmens?
- Handelt es sich um ein Sicherheits**DIENSTLEISTUNG**sunternehmen (Stellung von Sicherheitspersonal) oder um ein Sicherheits**BERATUNG**sunternehmen (Stellung von Sicherheitsberatern)?

3. ANSPRUCH UND WIRKLICHKEIT

Der beste Qualitätsindikator sind immer noch Referenzen und praktische Erfahrungsberichte anderer Kunden mit dem jeweiligen Unternehmen. Dies bedeutet jedoch nicht immer, dass ähnliche Projekt in der gleichen Branche schon einmal absolviert worden sind, sondern dass mindestens eine (praktische/projektbezogene) Erfahrung im selben Themengebiet bereits besteht.

⇨ **HERANGEHENSWEISE:** Fordern Sie Arbeitsproben an, die beispielsweise die Herangehensweise an die Aufgabenstellung inkl. etwaiger Meilensteine etc. beinhaltet. Fordern Sie die Angabe von Referenzen und nehmen Sie sich die Zeit, sich nach deren Erfahrung in der Zusammenarbeit zu erkundigen. Dabei sollten Sie jedoch berücksichtigen, dass es in der Sicherheitsberatung immer noch um das Thema „Sicherheit" und „Vertraulichkeit" geht und manche Kunden genau aus diesen Gründen nicht oder nur sehr eingeschränkt auskunftsfreudig sind.

Für manche Projekte kann es auch durchaus sinnvoll und legitim sein, mehrere Sicherheitsexperten für verschiedene Themenfelder oder Arbeitspakete zu beauftragen. Denn wie bereits beschrieben: Sicherheit ist nicht gleich Sicherheit! Die Themenfelder sind derart vielfältig und komplex, dass Auftraggeber stets am besten beraten sind, wenn sie sich Spezialisten aus dem jeweiligen Gebiet heranziehen und niemals „Einen für Alles" beauftragen, denn das wird zwangsläufig zu Qualitäts- und Ergebniseinbußen führen.

INSOURCING VON SICHERHEITSDIENSTLEISTUNGEN: BEGINN EINES STRUKTURELLEN WANDELS?!

Kostenreduzierung, Besinnung auf das Kerngeschäft, Schaffung gesteigerter Flexibilität oder Minimierung des Geschäftsrisikos waren in der Vergangenheit nur einige der Argumente, die Unternehmen als klare Vorteile für ein Outsourcing von Sicherheitsdienstleistungen sahen. Doch mittlerweile macht sich ein spürbarer Gegentrend bemerkbar, extern vergebene Sicherheitsdienstleistungen und das damit einhergehende betriebliche Sicherheits-Know-how wieder in Unternehmen zurückzuführen.

In den 90er und 2000er Jahren gab es branchenübergreifend die Trendwende, unternehmensinterne (Service-)Dienstleistungen wie beispielsweise Reinigung, Sicherheit, Facility Management etc. an externe Dienstleistungsunternehmen zu vergeben. Doch mittlerweile gibt es viele Unternehmen, die dieses Konzept in Frage stellen und neu bewerten. Insourcing oder Outsourcing? Beide Modelle haben – abhängig von den individuellen unternehmensspezifischen Anforderungen – ihre Daseinsberechtigung.

EIN DEFINITIONSVERSUCH

OUTSOURCING ist eine Ableitung aus den englischen Begriffen „out“ und „source“ („von außerhalb beziehen“) und beschreibt die Übertragung von bisher unternehmensintern erbrachten Leistungen an einen externen Dritten (Fremdunternehmen). Hierbei kann man jedoch noch einmal zwischen zwei Formen unterscheiden:

INTERNES OUTSOURCING
Hierbei wird die Leistung zukünftig von einem Tochterunternehmen erbracht.

EXTERNES OUTSOURCING
Hierbei wird die Leistung zukünftig von einem Fremdunternehmen (Dritten) erbracht.

INSOURCING bezeichnet die Rückführung von bisher von einem Tochterunternehmen oder Fremdunternehmen (Dritten) via Outsourcing erbrachten Leistungen in das Unternehmen.

HERAUSFORDERUNGEN BEIM OUTSOURCING VON SICHERHEITSDIENSTLEISTUNGEN

Zu den am häufigsten ausgelagerten Sicherheitsdienstleistungen zählen:

- Objekt- und Werkschutz
- Rezeptions- und Empfangsdienst
- Revier- und Streifendienst
- Alarm- und Interventionsdienst
- Notruf- und Serviceleitstelle
- Geld- und Werttransport
- Veranstaltungsschutz
- Personenschutz/Begleitschutz

Die in der Praxis immer wieder anzutreffenden Herausforderungen bzw. Problemstellungen beim Thema „Outsourcing von Sicherheitsdienstleistungen“ sind vielerorts:

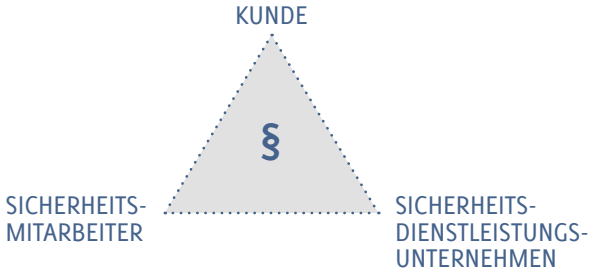
- falsche und/oder fehlerhafte (Dienst-)Leistungsbeschreibung
- keine oder zu geringe Qualifikationsanforderungen an das Sicherheitsdienstleistungsunternehmen und dessen (Führungs-)Personal
- Unkenntnis des Auftraggebers über etwaige branchenspezifische Qualitätsstandards und Zertifizierungen
- Einkauf nach dem Billigbieterprinzip
- falsche oder fehlerhafte Dienstleisterauswahl
- unzureichende auftraggeberseitige Führung/Überwachung der extern vergebenen Sicherheitsdienstleistungen und -prozesse
- mangelhafte Kenntnis des Auftraggebers über die eigenen Sicherheitsprozesse
- optimierungsbedürftige Rahmenbedingungen (Arbeitsumgebung, Räumlichkeiten, Arbeitsmittel etc.)
- etc.

Im Ergebnis resultieren daraus meist zwangsläufig erhebliche Performance-Schwächen des Sicherheitsdienstleisters, die am Ende wiederum entsprechende Leistungs- und Qualitätseinbußen für den Auftraggeber zur Folge haben.

EXTERNE VORGABEN VERKOMPLIZIEREN EXTERNE DIENSTLEISTUNGSPROZESSE

Hinzu kommt, dass im April 2017 das neue Arbeitnehmerüberlassungsgesetz (AÜG) in Kraft getreten ist, was bei vielen Unternehmen zum Umdenken im Umgang mit bisher im Unternehmen eingesetzten Sicherheitsmitarbeitern geführt haben sollte. Denn so, wie viele Sicherheitsmitarbeiter in Unternehmen, bei denen sie im Einsatz sind, bisher geführt wurden, fallen sie unter das AÜG bzw. unter den Passus der „verdeckten Arbeitnehmerüberlassung“.

Des Weiteren muss auch die EU-Datenschutzgrundverordnung (EU-DSGVO) gerade im Umgang mit personenbezogenen Daten – beispielsweise im Rahmen von Telefondiensten, Besucheranmeldungen, E-Mail-Verkehr, Sicherheitsmeldungen etc. – differenzierter betrachtet werden, da diese im bisherigen Dreiecksverhältnis komplexer abgebildet werden muss. ›››



RAHMENBEDINGUNGEN IM ZUSAMMENHANG MIT DEM AÜG

Seit dem 01.04.2017 sind Neuregelungen im Arbeitnehmerüberlassungsrecht in Kraft. Verstöße sind für alle Beteiligten bußgeldbewehrt und können dazu führen, dass Leiharbeitnehmer einen Anspruch auf dauerhafte Beschäftigung beim Entleiher erhalten. Nachfolgend die wichtigsten Eckpunkte:

- Konkrete Weisungen oder Anweisungen dürfen nur an „offene“ Arbeitnehmerüberlassungskräfte ergehen (jedoch nicht an Dienstleistungskräfte!).
- Die Höchstüberlassungsdauer von „offenen“ Arbeitnehmerüberlassungskräften beträgt 18 Monate.
- Nach spätestens 9 Monaten ununterbrochener Einsatzdauer gilt, dass ein Leiharbeitnehmer genauso entlohnt werden muss, wie ein Stammarbeitnehmer („Equal Pay“).
- Die Arbeitnehmervertreter müssen im Vorfeld einer Arbeitnehmerüberlassung umfassend informiert werden.
- Leiharbeitnehmer, die mindestens 6 Monate und 1 Tag entliehen wurden, werden bei der Berechnung von Schwellenwerten berücksichtigt.
- Künftig gibt es umfassende Pflichten zur Kennzeichnung und Dokumentation.

BEI DIENSTLEISTUNGSVERTRÄGEN LÄSST SICH DAS RISIKO EINER „VERDECKTEN ARBEITNEHMERÜBERLASSUNG“ NIEMALS VOLLSTÄNDIG AUSSCHLIESSEN.

(C) Gorodenkoff Productions OU - stock.adobe.com

GRUNDSÄTZLICH SOLLTEN BEI ALLEN OUTGESOURCTEN PROZESSEN ENTSPRECHENDE VORKEHRUNGEN GETROFFEN WERDEN, DIE SICHERSTELLEN, DASS IM FALLE EINES DIENSTLEISTERAUSFALLS ODER EINES (GGF. VORZEITIGEN) VERTRAGSENDES DIE OUTGESOURCTEN PROZESSE/GESCHÄFTSTÄTIGKEITEN KEINESFALLS NACHHALTIG NEGATIV BEEINTRÄCHTIGT WERDEN.

Das erhöhte Lohngefüge, sich verändernde Qualitätsstandards sowie der Fachkräftemangel, der die Rekrutierung zuverlässiger, engagierter und geeigneter Sicherheitsmitarbeiter, die bei Sicherheitsdienstleistern eingesetzt werden, schwieriger werden lässt, führen dazu, dass bei vielen Unternehmen eine neue Betrachtung und unternehmerische Bewertung der bisher outgesourcten Sicherheitsdienstleistungen erfolgt.

TIPP FÜR DIE PRAXIS: Der „IT-Grundschutzkatalog" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) kann hierbei Unterstützung bieten, da dieser im Baustein „B 1.11" das Thema Outsourcing konkret thematisiert und im Umkehrschluss auch in gewisser Hinsicht auf das Thema Insourcing adaptiert werden kann.

IST INSOURCING NUN WIEDER „IN"?

Der generelle Trend geht dazu über, dass die Erbringung von Dienstleistungen komplexer und anspruchsvoller wird und die Verantwortung von (Dienstleistungs-)Personen und (Dienstleistungs-)Bereichen weiter steigt. Gerade in der Unternehmenssicherheit sind in den letzten Jahren vermehrt Anforderungen an den Know-how-Schutz, die frühzeitige Erkennung von Schwachstellen und die adäquate Reaktion auf Sicherheitsereignisse hinzugekommen.

Somit steht für viele die Frage im Raum: Soll die bis dato outgesourcte Sicherheitsdienstleistung auch weiterhin bei einem externen Anbieter verbleiben oder ist Insourcing hier vielleicht doch die bessere und mitunter „sicherere" Lösung?

DROHNEN: VIELFÄLTIGER EINSATZ IN DER SICHERHEIT

Tagtäglich liest man Berichte über den fehlerhaften Umgang mit Drohnen, der Frage nach rechtlichen Regelungen, Persönlichkeitsverletzungen und dergleichen. Doch im zielgerichteten und rechtlich abgeklärten Rahmen kann eine Drohne oder ein unbemanntes Flugsystem in vielen Branchen als Multitalent unterstützende Dienste leisten. Ob Luftaufnahmen, Inspektionen, Dokumentationen, Filmaufnahmen, Zählungen, Warentransport, Rettungseinsätze, Vermessungen oder Überwachungen.

Der Einsatz von Drohnen bietet einen enormen Nutzen in vielen Anwendungsfeldern der zivilen Sicherheit. So gibt es bereits einige Unternehmen aus der Sicherheitsbranche und Konzernsicherheitsverantwortliche, die erfolgreich Drohnen einsetzen, häufig initiiert auf Grund des Interesses einzelner technologiebegeisterter Mitarbeiter.

Trotz des enormen Nutzens und der vielen an Drohnen Interessierten und Technologiebegeisterten kommt es in der zivilen Sicherheit bisher noch nicht zum flächendeckenden Einsatz, da ein Drohneneinsatz auch enorme Risiken birgt, mit denen sich jeder Nutzer auseinandersetzen sollte.

> DER STETIG WACHSENDE ANTEIL DER ANWENDUNGSFELDER FÜR UNBEMANNTE SYSTEME ODER DROHNEN FINDET AUCH – UND DAS ZU RECHT – SEINEN WEG IN DIE SICHERHEIT. “

UMFRAGE: DROHNENNUTZER IN DER SICHERHEIT

Von Januar 2019 bis Juli 2019 hat Frank Potthast eine bundesweite Onlineumfrage durchgeführt, um einen ersten Überblick über den aktuellen Stand der Anwendungsfelder und Nutzer von Drohnen in der Sicherheitsbranche zu gewinnen. Die Evaluierung wurde unterteilt in die Bereiche „Anwender“ und „Nichtanwender“ mit einzelnen Unterfragen.

ZIELGRUPPE WAREN TEILNEHMER AUS:

- Objektschutz
- Revierdienst
- Veranstaltungssicherheit
- Empfangsdienst
- Brand-/Arbeitsschutz
- Personenschutz
- und anderen Sicherheitsfunktionen

VERWENDEN SIE DROHNEN BEREITS IN IHREM UNTERNEHMEN?

KÖNNEN SIE SCH ZUKÜNFTIG DEN EINSATZ VON DROHNEN VORSTELLEN?

Das Ergebnis zeigt deutlich, dass viele Unternehmen innovativ sein wollen, ohne sich genau mit der Thematik und den damit verbundenen Anforderungen auseinanderzusetzen. Viele Technikbegeisterte sehen den überzeugenden Mehrwert für die Einsatzunterstützung, ohne sich jedoch umfassend mit den Risiken zu beschäftigen. ›››

HERAUSFORDERUNGEN BEI DER GEWERBLICHEN DROHNENNUTZUNG

Die Risiken der Drohnennutzung liegen insbesondere in

- der fehlenden Versicherung,
- der Unkenntnis über Verbotszonen,
- der fehlerhaften Bedienung von Drohnen und
- im rechtlichen Umgang (Überflug, Persönlichkeitsrechte etc.).

RECHTLICHE RAHMENBEDINGUNGEN

An dieser Stelle ist nur eine Grobskizze möglich, da einzelne Aspekte explizit für die jeweilige Anwendung anhand der gültigen (sich ändernden) Gesetzeslage und landesspezifischen Anforderungen bzw. behördenseitigen Vorgaben beleuchtet werden müssen.

Im Luftverkehrsgesetz (LuftVG) und der Luftverkehrsordnung (LuftVO) sind aktuell die UAV-Regularien für den Privatanwender und Hobby-/Modellflug erfasst. Ergänzungen für den gewerblichen Einsatz von Drohnen sind zwar enthalten, aber eine genauere, detailliertere Definition besteht aktuell nicht. Mit der Durchführungsverordnung (EU) 2019/947 soll sich dies ab Juni 2020 ändern, so dass beispielsweise der grenznahe oder sogar grenzüberschreitende Einsatz von Drohnen zukünftig möglich ist.

BEISPIEL EINZELFALLBETRACHTUNG

DROHNENFLUG BEI NACHT Durch die Änderung der LuftVO § 21 a Absatz 1 Nummer 5 LuftVO im Jahr 2017 wurde klargestellt, dass das Fliegen bei Nacht erlaubnispflichtig ist. Das Fliegen bei Nacht ist jedoch nicht im Verbotskatalog des § 21b Absatz 1 LuftVO enthalten. Das Fliegen nach der Dämmerung oder in der Nacht ist lediglich erlaubnispflichtig durch die zuständige Landesluftfahrtbehörde. Dies stellt rechtlich gesehen einen sehr großen Unterschied dar.

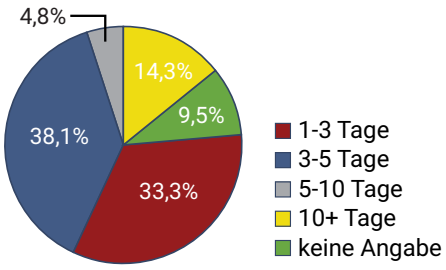
VERSICHERUNG UND HAFTUNGSFRAGEN

Im gewerblichen Bereich sollten die Haftungsfrage und somit der sachgerechte Einsatz im Fokus stehen und auch eine entsprechende Versicherung vorgehalten werden. Ohne Kenntnisnachweis des Piloten und Informationen der eingesetzten Systeme können Versicherer keine Rückversicherung erhalten und somit keine entsprechenden Haftpflichtversicherungen für Gefahrenlagen ausstellen.

SCHULUNG UND AUSBILDUNG

Ein weiterer wichtiger Bereich ist die Ausbildung von Drohnenpiloten. Recherchen, persönliche Gespräche und die Evaluierung haben gezeigt, dass es Ausbildungen für angehende Drohnenpiloten von 1 bis zu 7 Tagen gibt. Hierbei wird zu 70 % der Schwerpunkt auf das Erlernen der Steuerung und das Handling der Drohne gelegt. Inhalte wie Recht, Sicherheitsrichtlinien, Meteorologie und andere theoretische Inhalte werden dabei oftmals nur am Rande in einem kurzen Frontalunterricht vermittelt. So ließen nur 91 % der befragten Unternehmen die Piloten ausbilden, die Übrigen

Wie lange dauerte die Ausbildung?



9 % gaben an, keine Ausbildung zu benötigen!

Es bedarf neuartiger Kooperations- und Ausbildungsmodelle (der reine Nachweis der Flugkenntnisse ist nicht ausreichend), die die Interessen aller Akteure berücksichtigen und entsprechende Anreize in Richtung zivile Sicherheit schaffen: So müssen etwa die Sicherheitsverantwortlichen in Behörden und Organisationen mit Sicherheitsaufgaben sowie im privatwirtschaftlichen Bereich in Abstimmung mit den Luftfahrtbehörden ihre sicherheits- und ausbildungsrelevanten Qualitäts-anforderungen für den Drohneneinsatz im Bereich der Sicherheit definieren. Hierbei ist es ein Unterschied, ob der Einsatz im Rahmen der Veranstaltungssicherung, der kritischen Infrastrukturen oder der Geländeobservierung erfolgt, denn in der neuen DVO 2019/947 wird ab Juni 2020 durch die einzelnen Landesluftsicherheitsbehörden definiert, welche Anforderungen an die einzelnen Verwendungsarten und das Drohnensystem gestellt werden etc. In der Kurzumfrage wurde von Potthast die Frage gestellt, ob Unternehmer bei entsprechenden Regelungen ab Juni 2020 verstärkt auf die neue Technik setzen würden. 69 % beantworteten diese Frage mit „Ja“.

TECHNISCHE ANFORDERUNGEN

Viele Hersteller vertreiben inzwischen kostengünstige Drohnensysteme für den Privatmarkt, die eher nicht für den gewerblichen Bereich konzipiert sind. Dennoch orientieren sich viele gewerbliche Nutzer aufgrund eingeschränkter Budgets oder mangelnder Sachkenntnis an diesem Markt. Gewerbliche Nutzer sollten in Punkto „Sicherheit beim Drohneneinsatz“ keine Abstriche machen. Nachfolgend finden sich einige relevante Ausstattungs- und Funktionsmerkmale, über die eine Drohne für den Einsatz in der Sicherheit mindestens verfügen sollte:

- Fail-Safe (Sicherheitseinrichtung)
- Coming-Home (Rückkehrfunktion)
- GPS-Hold (Positionshaltung)
- Aktiver/Passiver Kollisionsschutz
- Virtual Cage-Funktion (GPS-Käfigfunktion)
- Flugzeit 20 min.+
- Windstabil bis 10 m/s
- RX/TX nicht im WLAN-Bereich (Funkstrecke)

„UNTERNEHMEN SIND BESTREBT, IN ALLEN BEREICHEN BEI NEUANSCHAFFUNGEN DIE „NEUESTEN MODELLE MIT DEN MEISTEN FEATURES" ZU IMPLEMENTIEREN. WARUM DANN BEIM DROHNENEINSATZ (ZU LASTEN DER SICHERHEIT) SPAREN ODER DIESE INEFFIZIENT EINSETZEN?

Innerhalb der konkreten Sicherheitsszenarien im Einsatz stellen sich dabei unterschiedliche Anforderungen bei der technischen Konfiguration (z. B. Sensorik, Materialien, Frequenzen). Bei der Veranstaltungssicherheit ist es beispielsweise unabdingbar, dass das System nicht durch Mobilfunk-/WLAN-Netze gestört wird und einen „Virtual Cage" erzeugen kann. Beim Einsatz in der Objektüberwachung spielt hingegen beispielsweise der Kollisionsschutz eine entscheidende Rolle.

Die Hauptaufgaben beim Einsatz von Drohnen in der gewerblichen Nutzung liegen darin,

- sich explizit mit dem rechtlichen Rahmen und den Erlaubnispflichten auseinanderzusetzen,
- den versicherungsseitigen und haftungsrechtlichen Rahmen für die Einsatzszenarien zu klären,
- die örtlich zuständigen Behörden einzubeziehen,
- die richtige Drohne anzuschaffen,
- die Drohnenpiloten regelmäßig umfassend zu schulen (auch in Theorie!),
- die Eigenarten der Topografie der Einsatzumgebung zu beachten sowie
- alle Prozesse und Szenarien inkl. „Fail-Safe" zu definieren.

Nur so ist der (richtige) gewerbliche Einsatz im rechtlichen Rahmen und mit Sicherheit möglich!

Dieser Artikel ist mit freundlicher Unterstützung von Frank Potthast entstanden, der in seinem Buch „Drohnen bei Security & Co." ausführlich über diese Thematik schreibt.

SCHLÜSSELFAKTOREN EINER EFFEKTIVEN KRISEN- UND NOTFALLPRÄVENTION

Unternehmen sind einer Vielzahl von Risiken ausgesetzt, die zu umfassenden Gefährdungen und existenzbedrohlichen Krisen führen können. Jederzeit kann ein unvorhergesehenes Ereignis eintreffen, wobei dieses selbstverständlich nicht immer Krisen- oder gar Katastrophencharakter haben muss. Doch auch weniger umfassende Störfälle können dafür sorgen, dass der Unternehmensbetrieb stillsteht und sich gravierende Schäden einstellen. Für viele Unternehmen ist es daher wesentlich, eine effektive Organisationsstruktur zu schaffen, die mit verschiedenen Krisenszenarien nachhaltig und kompetent umgehen kann.

> „EIN KRISENMANAGEMENT-SYSTEM IST FÜR EIN MODERNES RISIKOMANAGEMENT UNVERZICHTBAR UND SOLL DIE SICHERHEIT IM UNTERNEHMEN ERHÖHEN.

Der „garantierte" Erfolg von unternehmensinternen Krisen- und Notfallpräventionsmaßnahmen ist meist nur schwer messbar, da man im Vorfeld in vielen Teilen nur von theoretischen Annahmen ausgehen kann, was die quantitativen und qualitativen Messfaktoren betrifft. Lediglich die tatsächlichen Ausfallkosten von beispielsweise einer Produktionsstunde, nicht nutzbaren Gebäudeteilen/Standorten oder nicht verfügbaren technischen Komponenten etc. lässt sich im Vorfeld ziemlich konkret berechnen und individuell darstellen. Daher fällt es Verantwortlichen für das Krisen- und Notfallmanagement in vielen Unternehmen auch schwer, die notwendigen finanziellen, personellen und/oder organisatorischen Ressourcen für das Thema „Krisen- und Notfallprävention" zu erhalten, denn meist werden derartige Investitionen vielerorts mit dem Spruch abgelehnt: „Es ist doch noch nie etwas passiert!".

Aus diesem Grund kann es für Verantwortliche umso wichtiger sein, die Schlüsselfaktoren für Präventionsmaßnahmen im Bereich des Krisen- und Notfallmanagements zu kennen, um sich im Unternehmen optimal vorzubereiten und dementsprechend aufzustellen. Als grundsätzliche Schlüsselfaktoren im Krisen- und Notfallmanagement zählen beispielsweise die

- interdisziplinäre Auseinandersetzung mit dem Thema.
- Ausweitung der Überlegungen auf alle Bereiche, Standorte und Unternehmensteile.
- Zusammenführung der Informationen und die Konsolidierung in ein einheitliches und ganzheitliches Krisen- und Notfallmanagementsystem.
- Implementierung in die Unternehmenskultur und die Integration in bestehende Prozesse.
- Aufrechterhaltung, Sensibilisierung und Fortschreibung des Themas anhand von Praxiserkenntnissen aus Krisen-/Notfallübungen, internen Vorkommnissen und Erfahrungswerten sowie branchenspezifischen oder regulatorischen Veränderungen.

RELEVANZENTSCHEIDUNG

Grundsätzlich dienen als Entscheidungsgrundlage für die Einführung eines Krisen- und Notfallmanagementsystems folgende Fragestellungen, die sich jedes Unternehmen unabhängig von Brandschutz- oder Arbeitssicherheitsvorgaben stellen sollte:

1. Gibt es eine rechtliche, branchenspezifische oder vertragliche Erforderlichkeit für ein Krisen- und Notfallmanagementsystem?
2. Stellen Behörden, Kunden oder Geschäftspartner spezielle Anforderungen an ein Krisen- und Notfallmanagementsystem?
3. Sind konkrete Umgebungsfaktoren vorhanden, die ein Krisen- und Notfallmanagement notwendig erscheinen lassen (Lage, Umgebung, Nachbarschaft etc.)?
4. Wie sind die Haftungsrisiken für Führungskräfte aktuell zu bewerten (Fürsorge- und Sorgfaltspflicht, Organisationshaftungsrisiken etc.) und könnte ein Krisen- und Notfallmanagementsystem hier unter Umständen hilfreich sein?
5. Bestehen hohe unternehmerische Abhängigkeiten zwischen einzelnen Standorten/Gebäudeteilen/Bereichen und/oder Dritten?

Wenn die Relevanzentscheidung zu dem Ergebnis führt, ein Krisen- und Notfallmanagementsystem im Unternehmen aufzubauen und zu implementieren, gibt es gewisse Erfolgsfaktoren, die dabei herangezogen werden können.

ERFOLGSFAKTOREN

Grundsätzlich entscheiden acht Bausteine, ob Unternehmen auf Ereignisse nur reagieren oder das Thema Krisen- und Notfallmanagement proaktiv vorantreiben und damit im Fall der Fälle gegenüber (Schadens-)Ereignissen bestmöglich gewappnet sind.

KRISEN- UND NOTFALLPRÄVENTIONSMASSNAHMEN STELLEN I. D. R. INFORMATIONEN, RESSOURCEN UND ROUTINEN ZUR VERFÜGUNG, UM IN EINEM EREIGNISFALL SCHNELLSTMÖGLICH VOM „NORMALBETRIEB" IN DEN „AUSNAHMEZUSTAND" UMZUSCHALTEN.

… DAS KRISEN- UND NOTFALLHANDBUCH

- ☐ Krisen- und Notfallhandbuch vorhanden
- ☐ Krisen- und Notfallhandbuch unterliegt einer Revision
- ☐ Handlungsanweisungen, Checklisten und Pläne
- ☐ Kompaktzugriff auf wesentliche Bestandteile im Ereignisfall möglich
- ☐ Aufbewahrung auch im physischen Ausdruck an unterschiedlichen Stellen
- ☐ Übergeordnete/behördenseitige Hilfsmaßnahmen sind abgebildet

… FÜR DEN MITARBEITER- UND BETROFFENENSCHUTZ

- ☐ Sensibilisierung für das Verhalten in Not- und Krisensituationen
- ☐ Ausbildung von Brandschutzhelfern, Ersthelfern und Räumungshelfern
- ☐ Regelmäßige Durchführung von Räumungsübungen und Optimierung des Räumungskonzeptes
- ☐ Verhaltensstandards an Sammelstellen (Sammelplätzen) inkl. Kommunikationsempfehlungen
- ☐ Externe Hilfskräfte (Polizei, Feuerwehr, Rettungsdienst etc.) sind eingebunden und üben mit
- ☐ Psychosoziale Notfallversorgung für Mitarbeiter und Betroffene gewährleistet
- ☐ Betreuung und Verpflegung des Krisenstabs gewährleistet

… IM ALARMMANAGEMENT

- ☐ Dokumentation des Alarmierungs- und Meldeverfahrens
- ☐ Aktuelles Kontakt- und Ansprechpartnerverzeichnis
- ☐ Verfügbarkeit des Kontakt- und Ansprechpartnerverzeichnisses (auch als physischer Ausdruck)
- ☐ Einbindung des Verzeichnisses in die Kommunikationsmedien der Krisenstabsmitglieder
- ☐ Regelmäßige Alarmierungsübungen inkl. Einberufung des Krisenstabs
- ☐ Interne und externe Schnittstellen bekannt und eingebunden

… FÜR DIE KRISENSTABSARBEIT

- ☐ Plausible Rollenbesetzung der Krisenstabsmitglieder
- ☐ Übernahme der Aufgaben und Verantwortlichkeiten
- ☐ Ereignisspezifische Zusammensetzung des Krisenstabs gewährleistet (Kernteam und erweiterter Krisenstab)
- ☐ Krisenstabsassistenzen benannt
- ☐ Krisen-/Notfallszenarien bekannt
- ☐ Regelmäßige Durchführung von Schulungen, Rollen- und Planspielen sowie Krisen-/Notfallübungen
- ☐ Aufbrechen der herkömmlichen Aufbau- und Ablauforganisation samt Hierarchien im Ereignisfall

… DIE AUSSTATTUNG

- ☐ Benennung des Krisenstabsraums/Ausweichflächen
- ☐ Bestückung des Krisenstabsraums und/oder einer mobilen Krisenstabskiste mit allen notwendigen und zwingend benötigten (Versorgungs-)Materialien
- ☐ Kommunikation mit und ohne Strom/Internet/Telefon berücksichtigen
- ☐ Pläne und Kontaktlisten vorhalten

… IN DER KRISENBEWÄLTIGUNG

- ☐ Entscheidungsfreudigkeit im Krisenstab
- ☐ Stetiges Neubewerten der Lage
- ☐ Budget vorhalten
- ☐ Krisen-/Notfallbewältigungspläne durchgehen
- ☐ Rechtssicheres Sammeln und Archivieren von Informationen im Ereignisfall

… DIE KRISENKOMMUNIKATION

- ☐ Kommunikationsstrategien (intern/extern) bekannt
- ☐ Pressesprecher und Stellvertreter geschult
- ☐ Verhaltensregeln für Mitarbeiter
- ☐ Haltestatements vorbereitet
- ☐ Pressearbeit vorbereitet
- ☐ Abstimmung mit Pressestellen betroffener Stellen
- ☐ Vorhalten von ggf. „Dark-Sites", Kommunikationshotlines, Softwaretools etc.

… NACH DER EREIGNISSITUATION

- ☐ Interne und externe Ereignisnachbereitung sichergestellt
- ☐ Ereignisdokumentation inkl. „lessons learned"
- ☐ Umsetzung ggf. neuer präventiver (Optimierungs-) Maßnahmen
- ☐ Psychosoziale Überwachung/Weiterbetreuung von Mitarbeitern veranlassen
- ☐ Ursprungszustand herstellen

„KRISEN- UND NOTFALL-MANAGEMENT BEDEUTET AUCH: WER NICHT HANDELT, WIRD BEHANDELT!"

CYBERANGRIFF

DIE FRAGE LAUTET NICHT OB, SONDERN WANN!

Laut dem Branchenverband „Bitkom“ steigt die Zahl der Cyberangriffe und damit auch der Schaden: 43 Milliarden Euro etwa betrug er in Deutschland in den Jahren 2017 und 2018. Angegriffen wurden sieben von zehn Unternehmen[1]. Neun von zehn Cyberangriffen starten mit E-Mails, die bösartige Programme ins interne Netzwerk speisen und im schlimmsten Fall das ganze Unternehmen lahmlegen. Bei der zunehmenden Automatisierung von solchen Angriffsmethoden ist die Frage nicht mehr, ob ein Angriff kommt, sondern wann.

Wie kommt es zu einem Cyberangriff?

EIN BEISPIEL: Es ist Jahresabschluss, das ganze Team steht unter Stress und im Postfach landet eine E-Mail aus der Buchhaltung mit der Bitte, die Zahlen im Anhang umgehend zu prüfen. Dass der Absendername etwas anders als sonst aussieht, fällt dem Empfänger nicht weiter auf – und schon ist der Anhang geöffnet.

Wir leben im Zeitalter ständiger Erreichbarkeit und kommunizieren digital auf vielfältigen Kanälen wie Videotelefonie, E-Mail, Messenger und in sozialen Medien und Foren. Die E-Mail ist seit den 90er Jahren des vergangenen Jahrhunderts fester Bestandteil der Kommunikation zwischen Menschen, aber auch zwischen Unternehmen und hat sich als Kommunikationsstandard etabliert.

Angreifer konzentrieren sich in den letzten Jahren bevorzugt auf kleine und mittelständische Unternehmen, da sie dort kaum Abwehrmechanismen erwarten und leichtes Spiel mit ihren Opfern haben.

GEFAHREN DER E-MAIL-KOMMUNIKATION

Im Jahr 2017 gelangte die Ransomware „NotPetya“ per E-Mail in das interne Netz des weltgrößten Containerversenders Maersk. Ransomware sind Erpressungstrojaner, die Daten abgreifen und die Nutzung ganzer Systeme ausschalten können. Meist wird gegen die Zahlung von Bitcoins die Rückgabe der Daten und die Freischaltung des Systems versprochen. Im Fall von Maersk dauerte es zehn Tage, die 4.000 infizierten Server mit 45.000 angeschlossenen PCs und 2.500 Programmen wiederherzustellen. Der wirtschaftliche Schaden war immens.

Neben den entstandenen Kosten können bei einem Cyberangriff auch andere Folgen entstehen: geistiges

[1] *https://www.bitkom.org/Presse/Presseinformation/Attacken-auf-deutsche-Industrie-verursachten-43-Milliarden-Euro-Schaden.html*

IM JAHR 2018 WURDEN ALLEIN IN DEUTSCHLAND 848 MILLIARDEN E-MAILS VERSENDET – ZEHN JAHRE ZUVOR WAREN ES NOCH 217 MILLIARDEN[2] – WOBEI 2018 ÜBER FÜNFZIG PROZENT DER E-MAILS IN UNTERNEHMEN SPAM WAREN[3] .

Eigentum kann kopiert werden oder abhandenkommen, kostenintensive Versuchsreihen müssen erneut umgesetzt werden, Gerichtsverfahren können anhänglich sein, Produktionsprozesse werden unterbrochen und Produkte beschädigt, was zu einer Verknappung am Markt führen kann.

Auch intern sind vor allem unverschlüsselte E-Mails ein Sicherheitsrisiko. Selbst geschulte Mitarbeiter erkennen nicht jede fingierte E-Mail oder öffnen doch eine Spam-Mail, da Spammer mittlerweile sehr geschickt vorgehen. Selbst Führungskräfte und IT-Administratoren sind nicht sicher. Denn hier ist nicht nur die Gefahr eines Cyberangriffs gegeben, sondern Sabotage und Spionage können hier ihren Ursprung nehmen.

LAUT EINER STUDIE WURDEN IN DEUTSCHLAND IM VERGANGENEN JAHR BEI 92 % DER BEFRAGTEN UNTERNEHMEN SICHERHEITSVERLETZUNGEN FESTGESTELLT. BEI 43 % DER BEFRAGTEN UNTERNEHMEN WAREN ANGRIFFE IN DEN LETZTEN ZWÖLF MONATEN DREI BIS FÜNF MAL ERFOLGREICH[4].

ALTERNATIVEN ZUR E-MAIL: EFFIZIENZSTEIGERUNG DURCH MODERNE KOMMUNIKATION

Neben dem klassischen Brief, der heute gerne als „Snail Mail“ degradiert wird und dem Fax, das vor allem von Anwälten noch aus rechtlichen Gründen genutzt wird, ist die E-Mail überall präsent. Doch wer kennt es nicht – ewig lange Antwortketten per E-Mail, in denen jeder noch mal zustimmt, verstopfen das Postfach – genauso wie eine Unzahl an Newslettern. Im Privatgebrauch sind Messenger mit Gruppenfunktionen längst Standard, um Verabredungen und Veranstaltungen zu planen sowie Freundschaften zu pflegen – aber wie sieht es in der Geschäftswelt aus? Mit den Ansprüchen der jungen Generation an schnellem Austausch und vielfältigen Medieneinsatz stehen moderne Unternehmen vor einem Problem. Viele junge Erwachsene sind mit dem Smartphone in der Hand aufgewachsen und haben andere Kommunikationsroutinen als ältere Generationen.

HERAUSFORDERUNGEN BEI MESSENGERN

Die Nutzung von privaten Messengern mit Diensthandys bzw. die dienstliche Kommunikation über private

Mobiltelefone gestaltet sich rechtlich schwierig, da Kunden- und Unternehmensinformationen über unsichere Plattformen ausgetauscht werden. Zum einen entsteht eine sogenannte „Schatten-IT“, über die das Unternehmen und die IT-Abteilung keine Kontrolle hat. Somit kann nicht sichergestellt werden, dass die Governance-Regeln des Unternehmens bzw. der IT-Sicherheit eingehalten werden. Im Fall eines Datenverlusts ist so nicht klar definiert, wer die Verantwortung übernimmt. Zum anderen ist der Gebrauch von privaten Messengern nicht immer konform mit der EU-Datenschutzgrundverordnung (EU-DSGVO), da der Zugriff auf das gesamte Adressbuch des Nutzers gewährt wird. Das bedeutet, dass Kundendaten an den jeweiligen Konzern weitergeleitet werden könnten, ohne dass die Personen im Adressbuch damit einverstanden sind, was wiederum eine Abmahnung des Unternehmens zur Folge haben könnte.

Eine moderne und effiziente Alternative zur E-Mail und privaten Messengern sind sogenannte Kollaborationsplattformen. Hier können in Einzelgesprächen Inhalte zügig erledigt und in Gruppen allgemeine Themen besprochen werden. Zustimmungen oder Ablehnungen lassen sich durch Kommentare in Form von Emojis oder Abstimmungen transparent aufzeigen. Auch Sprachanrufe, Videotelefonie und das Teilen von Anhängen findet in einer sicheren Umgebung statt. Dank einer Ende-zu-Ende-Verschlüsselung kann von außen niemand mehr mitlesen und kritische Daten und Firmengeheimnisse sind stets geschützt. ›››

+ EINE ÜBERPRÜFUNG DER BESTEHENDEN SYSTEME
+ KOMMUNIKATIONSLÖSUNGEN FÜR DEN ERNSTFALL
+ EIN GESTEIGERTES BEWUSSTSEIN FÜR EXTERNE GEFAHREN BEI DEN MITARBEITERN

= **RISIKOMINIMIERUNG**

[2] https://de.statista.com/statistik/daten/studie/392576/umfrage/anzahl-der-versendeten-e-mails-in-deutschland-pro-jahr/
[3] https://de.statista.com/statistik/daten/studie/446308/umfrage/spam-anteil-weltweit-in-unternehmen/
[4] https://www.it-daily.net/analysen/20649-eskalierende-cyberangriffe-anzahl-und-komplexitaet-nehmen-zu

VERHALTEN IM FALLE EINES CYBERANGRIFFS

Grundsätzlich ist der Einsatz von Verschlüsselung anzuraten, von denen es verschiedene Level gibt. Denn gerade im Ereignisfall, wenn alle damit beschäftigt sind, wieder Herr der Lage zu werden, den Fehler zu finden und zu beheben, kommt es zu einer Vielzahl von Kommunikationsvorgängen auf unterschiedlichsten Wegen. Gerade dann wird eine „sichere Kommunikation" vernachlässigt, denn es muss alles schnell gehen. Doch vielleicht hat der Angreifer gerade darauf gewartet, den schwachen Moment auszunutzen oder andere Hacker werden auf das Unternehmen aufmerksam. Insbesondere für diese Fälle sollten Unternehmen sichere Kollaborationsplattformen bereithalten, denn eine sichere Kommunikation kann über Gedeih und Verderb eines Unternehmens entscheiden. Ein Umstieg von E-Mail auf Kollaborationsplattform ist ein Weg zu sicherer Kommunikation, effizienter Arbeit und einer Modernisierung des Unternehmens.

Dieser Artikel ist mit freundlicher Unterstützung von Morten Brøgger (Geschäftsführer der Kollaborationsplattform Wire) entstanden.

NOTFALLPLAN CYBERANGRIFF

1 VERTEIDIGUNGSSTRATEGIEN ERARBEITEN

Überlegen Sie, wie Sie sich verteidigen bzw. schützen können. Nutzen Sie Ende-zu-Ende-Verschlüsselung für die Kommunikation mit unabhängigen Schlüsseln, so dass Hacker nur mit einem Teil des Schlüssels nicht viel anfangen können.

2 BUSINESS CONTINUITY PLAN ÜBERPRÜFEN UND DEFINIEREN

Überprüfen Sie ihr betriebliches Kontinuitätsmanagement. Wenn ihre IT-Systeme das Backup in der Cloud haben und die IT lokal basiert ist, wie lange dauert es, die IT nach einem Angriff wiederherzustellen und vollumfänglich einsatzfähig zu machen?

3 GEHEN SIE IHRE KOMMUNIKATIONS- UND KOLLABORATIONSBEDÜRFNISSE DURCH

Stellen Sie sicher, dass die Kommunikation im Fall eines Angriffs widerstandsfähig ist oder über ein sicheres Backup verfügt, falls der Rest des Netzwerks kompromittiert ist. Gerade wenn das Netzwerk angegriffen wird, muss sichergestellt sein, dass eine Zusammenarbeit und ein Informationsaustausch trotzdem funktioniert.

4 MITARBEITERSENSIBILISIERUNG UND NOTFALLVERFAHREN KENNEN

90 % der Angriffe starten mit einer E-Mail im Postfach eines Mitarbeiters. Meist werden solche E-Mails aus Unwissenheit des Mitarbeiters geöffnet und der verbreitete Virus kann im Ernstfall Daten löschen oder sogar das ganze IT-System lahmlegen. Jeder einzelne Mitarbeiter sollte daher sowohl zum Thema Datenschutz und EU-DSGVO geschult werden als auch darüber, was zu tun ist, wenn es wirklich zu einem Cyberangriff kommt.

5 REVISION DES NOTFALLPLANS

Prüfen Sie Ihren Notfallplan jährlich und machen Sie dessen Umsetzung für alle Mitarbeiter zum Teil des Betriebsalltags.

PRODUKTPIRATERIE:

PLAGIATE ALS GEFAHR FÜR DIE DEUTSCHE WIRTSCHAFT

> „PLAGIATE UND FÄLSCHUNGEN SIND EINFALLSLOS, MORALISCH VERWERFLICH UND SIE FÜHREN ZU STILLSTAND UND HEMMUNG DES FORTSCHRITTS."

Mangels eigener Ideen und aus Profitgier werden sie oftmals billig und unter menschenverachtenden Arbeitsbedingungen hergestellt. Plagiate und Fälschungen verursachen teils existenzgefährdende Schäden bei innovativen Herstellern: Von Umsatzeinbußen über den Verlust von Arbeitsplätzen und unberechtigten Haftungsrisiken bis hin zu mangelnden Erträgen für zukünftige Produktentwicklungen. Zudem bergen billige Nachahmungen nicht zu unterschätzende Sicherheitsrisiken. All dies macht deutlich: Produkt- und Markenpiraterie ist weder Kompliment noch harmloses Kavaliersdelikt, sondern Wirtschaftskriminalität mit gravierenden negativen Auswirkungen.

Die Erscheinungsformen von Plagiaten sind branchenübergreifend und reichen von Designplagiaten über Technologieklau bis hin zu Markenfälschungen. Angeboten werden die nachgemachten Waren in allen Preis- und Qualitätsabstufungen: Von gefährlichen Billigfälschungen bis hin zu qualitativ hochwertigen Plagiaten, die kaum günstiger oder manchmal sogar teurer als das Originalprodukt sind. Gerade in Zeiten von „Social Media" und „Influencer Marketing" sind für Markenhersteller ungerechtfertigte Reputationsschäden meist noch gravierender als finanzielle Schäden. Enttäuschte Kunden wenden sich angesichts der Vielzahl von Alternativanbietern schneller denn je von der Marke ab und beeinflussen quer über den Globus Freunde und Follower mit ihren Erfahrungen, Meinungen und Empfehlungen.

(UNFREIWILLIG) IM VISIER DER FÄLSCHER

Grundsätzlich stehen renommierte Marken- und Luxusartikel genauso wie Produkte „Made in Germany" im permanenten Fokus von Nachahmern. Besonders betroffen ist der Maschinenbau als deutsche Schlüsselindustrie. Der Zoll beschlagnahmt aber auch aus anderen Bereichen regelmäßig Fälschungen wie

- Bekleidung,
- Sportartikel und Accessoires,
- Medikamente, Lebensmittel,
- Kosmetika sowie
- Elektronik und (Kfz-)Ersatzteile.

Dass das Thema mittlerweile alle Branchen betrifft, zeigen auch die vielen unterschiedlichen Nachahmerprodukte, denen von der Aktion Plagiarius e. V. in über 40 Jahren der ›››

Bei Plagiaten und Fälschungen handelt es sich um Diebstahl geistigen Eigentums bzw. die Verletzung von Urheberrechten oder gewerblichen Schutzrechten (Marke, Design, Patent, Gebrauchsmuster).

PLAGIAT: Beim Plagiat kopiert der Nachahmer das Produkt (Diebstahl geistigen Eigentums), d. h. das Design und/oder die Technik eines erfolgreichen Produktes werden übernommen und unter eigenem Namen verkauft.

FÄLSCHUNG: Bei der Fälschung übernimmt der Nachahmer zusätzlich den Markennamen und gibt sich als renommierter Originalhersteller aus.

Negativ-Preis „Plagiarius“ verliehen wurde: Haushaltwaren, Sanitärprodukte, Werkzeuge, (Büro-)Möbel, Kinderspielzeuge, Hundeleinen, Kniebandagen, aber auch technische Produkte, wie z. B. Druckmessgeräte, Kühlmittelpumpen, Motorsägen, Hochdruckreiniger, …

Durch den hohen Bekanntheitsgrad zeigt der „Plagiarius“ regelmäßig erfolgreich seine abschreckende Wirkung: Aus Angst vor öffentlicher Blamage haben über die Jahre hinweg zahlreiche Nachahmer noch vor der Jurysitzung eine Einigung mit dem Originalhersteller gesucht und es wurden beispielsweise Restbestände der Plagiate und Fälschungen vom Markt genommen, Unterlassungserklärungen unterschrieben oder Lieferanten preisgegeben.

> **“ PRINZIPIELL IST NICHTS VOR FÄLSCHUNGEN SICHER, WAS AM MARKT ERFOLGREICH IST UND GROSSE PROFITE VERSPRICHT.**

AUFRUF! 1977 VOM DESIGNER PROF. RIDO BUSSE INS LEBEN GERUFEN, WIRD DER NEGATIV-PREIS „PLAGIARIUS“ JÄHRLICH AUF DER FRANKFURTER KONSUMGÜTERMESSE „AMBIENTE“ AN HERSTELLER UND HÄNDLER BESONDERS DREISTER PLAGIATE UND FÄLSCHUNGEN VERLIEHEN. EINSENDESCHLUSS FÜR DEN PLAGIARIUS-WETTBEWERB 2020 IST DER 30. NOVEMBER 2019. BETROFFENE UNTERNEHMER KÖNNEN ORIGINALPRODUKT UND PLAGIAT EINREICHEN UND DEN NACHAHMER ALS PREISTRÄGER DES NEGATIV-PREISES VORSCHLAGEN. AUSFÜHRLICHE INFORMATIONEN GIBT ES UNTER WWW.PLAGIARIUS.COM

CHINA: FÄLSCHERNATION, WERKBANK DES WESTENS UND AUF DEM WEG ZU „MADE IN CHINA 2025“

Allein 2017 haben die europäischen Zollbehörden laut EU-Kommission an den EU-Außengrenzen mehr als 31 Millionen rechtsverletzende Produkte mit einem Gesamtwert von über 580 Millionen Euro beschlagnahmt – und das ist nur die Spitze des Eisbergs. China und die Sonderverwaltungszone Hongkong sind einerseits nach wie vor Herkunftsland Nr. 1 für Fälschungen. Gleichzeitig aber verfolgt China seit Jahren mit Nachdruck und mit Investitionen in Milliardenhöhe seinen ehrgeizigen Zehnjahresplan „Made in China 2025“: Das Land will zu den technologisch führenden Industrieländern aufschließen. Weg von der verlängerten Werkbank des Westens hin zum ernsthaften Mitbewerber auf den Weltmärkten. Diese Strategie Chinas beinhaltet auch die gezielte Übernahme westlicher Unternehmen, die zukunftsweisende Schlüsseltechnologien besetzen. Fakt ist, dass innovative chinesische Firmen in einem Plagiat weder ein Kavaliersdelikt noch ein Kompliment sehen, sondern konsequent ihre Rechte gegen Nachahmer durchsetzen.

AUCH IN WESTLICHEN INDUSTRIENATIONEN WIRD KOPIERT

Zoll-Statistiken berücksichtigen nur Waren, die aus Drittländern in das jeweilige Gebiet (z. B. EU oder USA) eingeführt werden, sie erfassen keine Rechtsverletzungen innerhalb dieser Regionen. Fakt ist, unlautere Nachahmungen werden häufig auch in Industrieländern hergestellt, vertrieben oder sogar von dort in Auftrag gegeben. Und immer häufiger

NEGATIV-PREIS „PLAGIARIUS“

**LINKS DAS ORIGINALPRODUKT
RECHTS DAS PLAGIAT/DIE FÄLSCHUNG**

1


2


4

3


5

stammen Originalhersteller und Plagiator aus demselben Land – auch aus Deutschland.

Die Plagiate werden dann beispielsweise von ideenarmen Mitbewerbern oder ehemaligen Produktions- bzw. Vertriebspartnern in Auftrag gegeben. Sehr gezielt prüfen Mitbewerber die Existenz von gewerblichen Schutzrechten und wenn keine eingetragen sind, werden Anspruchsdenken und Skrupel über Bord geworfen und fremde Design- und Techniklösungen als eigene Leistung erstellt und ausgegeben.

> **LUKRATIVE GEWINNE VOR AUGEN, NEHMEN FÄLSCHER ALLE PROBLEME UND RISIKEN, DIE FÜR MARKENHERSTELLER, ABER AUCH DIE KÄUFER BESTEHEN, BILLIGEND IN KAUF. DIE TÄTERSTRUKTUR REICHT VOM IDEENARMEN WETTBEWERBER ÜBER RÜCKSICHTSLOSE HÄNDLER BIS HIN ZUR ORGANISIERTEN KRIMINALITÄT.**

Das belegen sowohl die Erfahrungen der Aktion Plagiarius e. V. als auch des Branchenverbandes „Verband Deutscher Maschinen- und Anlagenbau e. V." (VDMA).

ORGANISIERTE KRIMINALITÄT ENTDECKT DEN HANDEL MIT MARKENFÄLSCHUNGEN

Die Profite insbesondere bei billigen Fälschungen sind sehr lukrativ (mehrere Hundert Prozent) und mit denen im Drogenhandel vergleichbar. Gleichzeitig sind die Strafen auf die Herstellung und den Handel mit Plagiaten viel zu niedrig und haben keinerlei abschreckende Wirkung.
Entsprechend haben sich in den letzten Jahren Kriminelle zu weltweiten Fälscher-Netzwerken zusammengeschlossen. Europol und das Europäische Amt für geistiges Eigentum (EUIPO) beobachten bei Fälscherbanden eine stark wachsende Professionalisierung in Bezug auf Produktionsverfahren und Vertriebsstrukturen. Fälscherbanden greifen auf vorhandene Strukturen aus Drogen-, Waffen- und Menschenhandel zu und setzen für den globalen Vertrieb von Fälschungen auf Internet, „Social Media-Plattformen" und Messenger-Dienste.

Die Strafverfolgung solch krimineller Netzwerke ist teilweise schwierig, da diese weltweit agieren, Daten nur unzureichend geteilt werden, Fälschungen immer besser und somit schwerer zu identifizieren sind und auch die Gesetze sich unterscheiden. Neben der Strafbarkeit aus dem Marken-, Design- und Sortenschutzgesetz sowie dem Patentrecht können Betrugsstraftatbestände zu mehrjährigen Haftstrafen führen.

VERBRAUCHER = OPFER UND TÄTER! DENN ANGEBOT = NACHFRAGE

Insbesondere Faktoren wie Globalisierung, digitale Kommunikation, das Internet und leichtgläubige (Online-) Schnäppchenjäger haben für eine geradezu explosionsartige Ausbreitung von Produkt- und Markenpiraterie gesorgt.

Fakt ist, solange es eine Nachfrage gibt, wird diese auch bedient – mit Originalprodukten ebenso wie mit Fälschungen, die sich oft nur auf den ersten Blick täuschend ähnlich sehen. Gleiches Aussehen bedeutet keineswegs zwangsläufig gleiche Qualität, Leistungsfähigkeit und vor allem Sicherheit. Dieser Illusion sollten sich Verbraucher nicht blauäugig ›››

LINKS DAS ORIGINALPRODUKT
RECHTS DAS PLAGIAT/DIE FÄLSCHUNG

Bildquelle: Aktion Plagiarius e. V.

1. *Grohe Brausenset 2003*
2. *AC-Schnitzer Felge 2012*
3. *Siemens Wasserkocher 2001*
4. *Hoppe Türbeschlag 2009*
5. *Zweibrüder Taschenlampe 2013*
6. *Interstuhl Bürostuhl 2017*
7. *Weinmann Beatmungsgerät 2015*
8. *Victorinox Taschenmesser 2018*
9. *Steinel Bewegungsmelder 2019*

hingeben. Weder aus Unwissenheit noch aus fehlendem Unrechtsbewusstsein oder mangelnder Wertschätzung für das Original und schon gar nicht auf der Jagd nach dem vermeintlich besten Schnäppchen oder Statussymbol.

Die Europäische Union gilt als einer der Hauptabsatzmärkte für nachgemachte Produkte. Unternehmen und Verbraucher sollten sich bewusst für Originalprodukte – und somit für Sicherheit – entscheiden.

ABWEHRMASSNAHMEN VON PRODUKT- UND MARKENPIRATERIE

Für eine bestmögliche Abwehr von Produkt- und Markenpiraterie ist es sinnvoll auf eine ganzheitliche Strategie aus juristischen, organisatorischen und technischen Maßnahmen zu setzen.

Minderwertige Fälschungen, so gut sie vielleicht auf den ersten Blick aussehen mögen, können zu brenzligen Haftungsfällen, teuren Rückrufaktionen und irreparablen Imageschäden führen. Das gilt insbesondere für sicherheitsrelevante (z. B. Bremsbeläge) oder elektronische Produkte (Akku-Ladegeräte, Wasserkocher etc.). Die Zollbehörden und Interpol haben beispielsweise schon verunreinigte Parfums und Kosmetika, technische Produkte mit mangelhafter Elektronik, gepanschte Lebensmittel, fehlerhaftes oder schadstoffreiches Kinderspielzeug, falsch oder gar nicht dosierte Medikamente u. v. m. aus dem Verkehr gezogen.

... BEI PRODUKTEINFÜHRUNG

Grundsätzlich gilt in Deutschland wie in vielen anderen Ländern Nachahmungsfreiheit. Daher ist vor der Markteinführung eines neuen Produktes das Eintragen von gewerblichen Schutzrechten – Marke, Patent, Design – unerlässlich. Ohne solche Schutzrechte sind Kopien zwar dreist und unfair, aus rechtlicher Sicht aber in vielen Fällen legal, wenn nicht z. B. unlauteres Wettbewerbsverhalten nachgewiesen werden kann.

Mit eingetragenen gewerblichen Schutzrechten z. B. beim

- Deutschen Patentamt- und Markenamt,
- Europäischen Patentamt,
- Europäischen Amt für geistiges Eigentum (EUIPO),
- bei der World Intellectual Property Organisation (WIPO)
- oder bei den nationalen Ämtern der relevanten Herstellungs- und Absatzländer

hingegen haben Betroffene die Möglichkeit, den Plagiator zur Rechenschaft ziehen zu können. Dies bedeutet Unterlassungs- oder Schadenersatzansprüche sowie Auskunftsrechte können geltend gemacht und der Klageweg kann genutzt werden. Da das Motto vieler Fälscher „Mehr Schein als Sein“ ist, hat sich auch bei technischen Produkten die zusätzliche Absicherung über eingetragenen Designschutz bewährt.

Wer eingetragene gewerbliche Schutzrechte hat, kann zudem einerseits den Zoll beauftragen, rechtsverletzende Waren bereits an den Außengrenzen aus dem Verkehr zu ziehen. Zum anderen können und sollten Plagiate und Fälschungen auch im Internet regelmäßig – entweder in Eigenregie oder über Dienstleister – aufgespürt werden, um dann einen Antrag auf Löschung zu stellen sowie den Fall zu verfolgen.

Zur Abwehr von unberechtigten Produkthaftungsklagen eignen sich u. a. Sicherheitsmerkmale wie RFID-Codes oder Farb-Codes, die zur eindeutigen Identifizierung an Produkt und/oder Verpackung angebracht werden. Eine Vielzahl von Dienstleistern bietet entsprechende Lösungen sowohl sichtbarer als auch verdeckter Merkmale an. Darüber hinaus können technische Maßnahmen ergriffen werden, die z. B. das sogenannte „Reverse Engineering“ oder ungewünschte „Überproduktionen“ verhindern. Je nach Unternehmensgröße und -struktur kümmern sich Experten aus den Bereichen Produktentwicklung, Qualitätsmanagement, Vertrieb, Recht und die Unternehmensleitung um diese Themen. Unterstützen können teilweise auch IHK und Branchenverbände.

> JEDER BEEINDRUCKT GERN DEN CHEF UND PROFILIERT SICH MIT KOSTENEINSPARUNGEN. QUALITÄT UND SICHERHEIT HABEN ABER IHREN PREIS, SO DASS „BILLIG“ MANCHMAL AM ENDE ZU EINEM TEUREN UNTERFANGEN WIRD.

... BEI EINKÄUFERN ODER HÄNDLERN

Ein umfangreiches Produktsortiment rechtfertigt nicht die Vernachlässigung der Prüfpflichten beim Einkauf und Wareneingang. Händler, die von einem vielfältigen, häufig wechselnden Warenangebot profitieren, können die damit einhergehenden Prüfpflichten nicht mit der Entschuldigung von sich weisen, dass die Anzahl der Waren unüberschaubar groß sei. Grundsätzlich müssen alle im Handel erhältlichen Produkte technisch einwandfrei und sicher sein. Und sie dürfen keine eingetragenen Patente, Design- oder Markenrechte Dritter verletzen. Das bedeutet, dass man Wettbewerbsprodukte in den eigenen Vertriebsgebieten gut kennen und auf mögliche Schutzrechte überprüfen sollte. Gleichermaßen sollte dies auch bei der Vertragsgestaltung mit Lieferanten berücksichtigt werden. Allein schon um unberechtigten Haftungsforderungen, Schadenersatzzahlungen und Imageverlusten vorzubeugen.

Gerade bei der Recherche und Bestellung von Waren im Internet sollten die verantwortlichen Einkäufer sehr genau hinsehen und nicht voreilig und kritiklos auf „Kaufen“

klicken. Auf namhaften globalen eCommerce-Plattformen werden neben Originalwaren nachweislich massenweise rechtswidrige Plagiate und Fälschungen angeboten. Meist von Drittanbietern, die nach Bedarf ihre (Schein-)Identitäten wechseln und sich erfolgreich in der Anonymität des Internets verstecken. Auch die Anzahl von sogenannten „Fake-Shops" wächst. Einkäufer sollten sorgfältig die allgemeine Seriosität des Anbieters sowie Impressum, Zahlungsbedingungen (Achtung bei „nur Vorkasse"!), Widerrufmöglichkeiten, Bewertungen, Erreichbarkeit etc. prüfen.

Der vertrauensvolle Kontakt zu Herstellern und die sorgfältige Auswahl qualifizierter Lieferanten ist ebenso wichtig wie regelmäßige Kontrollen der Produktionsstandorte bezüglich der Einhaltung von Arbeits-, Qualitäts- und Sicherheitsstandards – dies ist auch für viele Zertifizierungen notwendig. Außerdem hilft es aufmerksam zu sein, auf kleinste Veränderungen (wie beispielsweise billige Materialien, schlechte Verarbeitung, schwache Druckqualität der Etiketten etc.) zu achten und Abstand zu nehmen von unrealistischen Angeboten dubioser Anbieter, insbesondere im Internet.

Viele Hersteller setzen mittlerweile Sicherheitsmerkmale, „Track & Trace-Systeme", RFID-Chips, Erstöffnungsschutz etc. ein, so dass regelmäßige Kontrollen am Wareneingang in enger Abstimmung mit dem Einkauf etabliert werden sollten. Im Zweifel ist immer der Hersteller zu kontaktieren.

Eines sollte man sich bei diesem Thema merken:

„WER SICH NICHT FRÜHZEITIG WEHRT, SENDET FALSCHE SIGNALE UND IST AUCH ZUKÜNFTIG EIN LEICHTES OPFER FÜR RÜCKSICHTSLOSE NACHAHMER!

MUSEUM PLAGIARIUS IN SOLINGEN

350 Plagiate und deren dreiste Fälschungen – staunen Sie selbst!

Das Museum Plagiarius in Solingen zeigt in seiner einzigartigen Ausstellung mehr als 350 Plagiarius-Preisträger der unterschiedlichsten Branchen – jeweils Original und Plagiat im direkten Vergleich.
Außerdem dabei: Typische vom Zoll beschlagnahmte Markenfälschungen. In Führungen werden spannende Fakten und Details vermittelt.

Erfahren Sie mehr unter: **www.museum-plagiarius.de**

Dieser Artikel ist mit freundlicher Unterstützung von Christine Lacroix vom Aktion Plagiarius e. V. entstanden. Ziel der Aktion Plagiarius e. V. ist es, die skrupellosen Geschäftspraktiken von Produkt- und Markenpiraten ins öffentliche Bewusstsein zu rücken und Industrie, Politik und Verbraucher für die Problematik zu sensibilisieren. Aktion Plagiarius e. V. möchte dazu beitragen, dass Konsumenten kreativen Leistungen (wieder) mehr Wertschätzung entgegenbringen und eine Produktentstehung bis hin zur Marktreife auch entsprechend honoriert werden muss.

Links das Originalprodukt – rechts das Plagiat/die Fälschung
v. l. Druckmessgerät 2017, Rutscher „PUKY Racer" 2018, Küchen-Schneidgerät „Nicer Dicer Plus" 2018

Bildquelle: Aktion Plagiarius e. V.

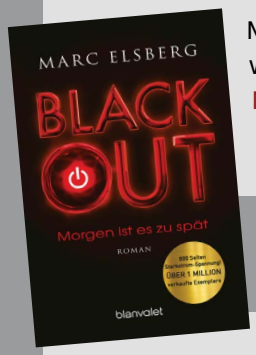
In diesem Bereich stellen wir Ihnen nützliche Tools, Sicherheitsmessen sowie Behörden, Verbände und Institutionen mit Sicherheitsaufgaben vor. Zusätzlich finden Sie hier auch ausgewählte (Fach-)Bücher, die Ihnen die Welt der „Sicherheit“ noch anschaulicher vermitteln werden.

BUCHTIPP

BLACKOUT. MORGEN IST ES ZU SPÄT!

Alle Prozesse des täglichen Lebens sind auf der Verfügbarkeit von Strom aufgebaut. Nahrungszubereitung, Duschen, Toilettenspülung, Mediennutzung, Ampeln, Zapfsäulen, Alarmsysteme etc.

Das Buch „BLACKOUT“ von Marc Elsberg verdeutlicht uns diese Allgegenwärtigkeit sehr anschaulich in Form eines Thrillers, denn er beschreibt darin über einen Zeitraum von 14 Tagen die verheerenden Auswirkungen eines flächendeckenden Stromausfalls in Europa.



Nutzen Sie diese Lektüre beispielsweise als Anregung, um Ihr Krisen- und Notfallmanagementsystem im Unternehmen weiterzuentwickeln.

Wir verlosen 4 Exemplare des Spiegel-Bestsellers, die uns vom Blanvalet Verlag zur Verfügung gestellt wurden.

Sie möchten an der Verlosung teilnehmen? So einfach geht es: Schreiben Sie uns einfach eine E-Mail mit dem Betreff: Blackout an redaktion@sicherheit-das-fachmagazin.de (solange der Vorrat reicht).

TOOL

WIE SICHER IST IHR PASSWORT? TESTEN SIE ES NOCH HEUTE!

Generell sollten nur sichere Passwörter verwendet werden. Wie sicher das von Ihnen gewählte Passwort ist, können Sie nun über eine App testen. Die Anwendung „How Secure Is My Password?“ zeigt Ihnen, wie lange es für einen Computer dauern würde, das jeweilige Passwort zu knacken. Darüber hinaus werden zu dem gewählten Passwort Verbesserungsmöglichkeiten für mehr Passwortsicherheit aufgezeigt.

Auf der Webseite finden Sie zudem einen Sensibilisierungsfilm, den Sie im Rahmen einer Security-Awareness-Kampagne im Unternehmen einsetzen können.

Erfahren Sie mehr unter:
www.howsecureismypassword.net

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.stock.adobe.com