AUSGABE 12

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

NOTFALL-/KRISENKISTE: EFFEKTIVE VORSORGE FÜR EIN AUTARKES (ÜBER-)LEBEN IM ERNSTFALL

In den Medien verfolgen wir in regelmäßigen Abständen verheerende (Natur-)Katastrophen und anderweitige (Schadens-)Ereignisse, die dazu führen, dass ein Großteil der notwendigen infrastrukturellen Versorgung der Bevölkerung nicht mehr zur Verfügung steht. Schwere Naturkatastrophen, langanhaltende Stromausfälle oder der flächendeckende Ausfall der Wasserversorgung sind in Deutschland zwar eher seltene Phänomene, dennoch sind wir keineswegs davor gefeit.

Katastrophen treten i. d. R. plötzlich und unvorhergesehen auf. Somit ist die Zeit, sich darauf vorzubereiten, im Ernstfall meist nicht mehr in vollem Umfang vorhanden. Um auch in kritischen Situationen die eigene Versorgung und gewisse infrastrukturelle Rahmenbedingungen gesichert zu wissen, ist eine adäquate Vorbereitung auf derartige Ereignisse essenziell. Auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ruft seit vielen Jahren dazu auf, dass sich vor allem Privathaushalte eine eigene Notbevorratung anlegen sollten. Doch wie genau sieht so etwas aus?

ZUSAMMENSTELLUNG EINER NOTFALL-/KRISENKISTE

DEFINITION: Eine Notfall-/Krisenkiste dient dazu, dem Besitzer sowie ggf. weiteren Personen ein autarkes (Über-)Leben ohne Abhängigkeit zur Außenwelt für einen gewissen Zeitraum zu gewährleisten.

In einer gut ausgestatteten Notfall-/Krisenkiste sollten sich Gegenstände aus den folgenden Kategorien wiederfinden:

- Nahrungs- und Wärmeversorgung
- Wind- und Wetterschutz
- Erste Hilfe
- Navigation, Information und Energieversorgung
- Brandschutz
- Schutz und Sicherheit
- Körperpflege
- Entsorgung

Unser Kompetenzpartner – die Sicherheits- und Krisenmanagementberatung „SIUS Consulting“ – hat Ihnen im Zusammenhang mit diesem Artikel zwei wissenswerte YouTube-Videos zu den Themen „Notfall-/Krisenkiste“ sowie „Notfall-/Krisenrucksack“ erstellt. Am schnellsten gelangen Sie zum jeweiligen Video, indem Sie in der Suchmaske von YouTube die Begriffe „Krisenkiste“ bzw. „Krisenrucksack“ eingeben.

Weitere relevante Dinge, wie z. B. geeignete Kleidung oder Medikamentenvorräte sollten ebenfalls bedacht werden. Zudem muss sich der konkrete Inhaltsumfang einer Notfall-/Krisenkiste stets an der Anzahl der zu versorgenden Personen und dem abzusichernden Zeitraum orientieren.

„WIRTSCHAFTSSPIONAGE“ UND „INDUSTRIESPIONAGE“ IN DEUTSCHLAND

In der Bundesrepublik Deutschland gibt es eine Vielzahl von innovativen Unternehmen und wissenschaftlicher Einrichtungen. Und genau für deren unternehmerisches oder wissenschaftliches Know-how interessieren sich Nachrichtendienste fremder Staaten (sogenannte „Auslandsnachrichtendienste“). Insbesondere für die von Wirtschaftsspionage betroffenen Unternehmen kann dies einen hohen und vor allem langfristigen wirtschaftlichen Schaden zur Folge haben.

Unter dem Begriff „Wirtschaftsspionage“ versteht man die staatlich gelenkte Ausforschung von Wirtschaftsunternehmen durch Nachrichtendienste fremder Staaten. Richtet sich die Spionagetätigkeit gegen wissenschaftliche Einrichtungen, spricht man von der sogenannten „Wissenschaftsspionage“.

Die Abwehr inländischer Spionageaktivitäten ist in der Bundesrepublik Deutschland grundsätzlich Aufgabe des Verfassungsschutzes.

Neben der „Wirtschaftsspionage“ gibt es darüber hinaus auch noch die sogenannte „Industriespionage“ (auch „Konkurrenzausspähung“ genannt). Diese ist nicht staatlich gelenkt, sondern wird von konkurrierenden Unternehmen betrieben. Für die Bearbeitung dieser Straftaten ist die Polizei zuständig.

GEFÄHRDUNGSEINSCHÄTZUNG DER AUSSPÄHUNGSAKTIVITÄTEN

Spionageaktivitäten fremder Staaten richten sich gegen Wirtschaftsunternehmen, sowie Wissenschafts- und Forschungseinrichtungen. Der potenzielle Schaden durch gezielte Wirtschaftsspionage ist enorm, denn der ungewollte Abfluss von Know-how gefährdet

- unmittelbar den wirtschaftlichen Erfolg eines Unternehmens,
- mittelbar aber auch die Wettbewerbsfähigkeit und Stabilität der deutschen Wirtschaft.

Sowohl Wirtschaftsspionage als auch Industriespionage spielen sich grundsätzlich nicht nach einem einheitlichen Muster ab. Staaten und Unternehmen betreiben Ausspähungen in Abhängigkeit ihrer spezifischen Bedürfnisse und unter Berücksichtigung der ihnen zur Verfügung stehenden Mittel und Möglichkeiten. Staaten mit Technologiedefiziten haben es eher auf wirtschaftsnahe Forschungsergebnisse und konkrete Produkte abgesehen, um diese beispielsweise zuerst auf den Markt bringen zu können oder das Design des Konkurrenten zu kennen. Während hoch industrialisierte Länder in erster Linie an wirtschaftlichen und wirtschaftspolitischen Strategien interessiert sind wie Expansionsstrategien, Kooperationen etc.

Die in aller Regel kurzfristiger angelegte Industriespionage zielt dagegen eher auf detaillierte Informationen und Entwicklungen zu Märkten, Technologien und Kundenpotenzial ab.

Im Fokus der Ausforschungsbemühungen stehen hauptsächlich technologieorientierte und innovative Unternehmen sowie wissenschaftliche Einrichtungen. Aktuell lassen sich folgende Branchen herausheben, die im Fokus von Spionageaktivitäten stehen:

- Informations- und Kommunikationstechnik
- Biotechnologie
- Optoelektronik
- Automobil- und Maschinenbau
- Luft- und Raumfahrttechnik
- Energie- und Umwelttechnologie

Spionagetätigkeiten richten sich dabei nicht nur an Konzerne oder große Unternehmen. Besonders gefährdet sind die in diesen Bereichen tätigen kleinen und mittelständischen Unternehmen, die zwar über wertvolles Know-how, aber oftmals nicht über die personellen und finanziellen Ressourcen verfügen, um ganzheitliche Sicherheitskonzepte zu etablieren. Zudem ist das Sicherheitsbewusstsein in vielen dieser Unternehmen nicht besonders ausgeprägt, weil sie sich der Gefährdung nicht bewusst sind und sich somit die Sicherheitsmaßnahmen (aus eigener Sicht) wirtschaftlich nicht rechnen – obwohl diese im Verhältnis zum potenziellen Schaden marginal ausfallen.

15 ANZEICHEN FÜR EINEN SPIONAGEANGRIFF

Als Basis für die Herangehensweise an aufzustellende Sicherheitsmaßnahmen dient das Wissen, welche Anzeichen es für einen Spionageangriff gibt, um daraus Maßnahmen ableiten zu können. Mögliche Anzeichen für einen Spionageangriff auf Ihr Unternehmen können beispielsweise sein:

- vermehrte elektronische Angriffe auf Ihre Informations- und Telekommunikationssysteme
- Auffinden von Schadprogrammen in Ihren Informations- und Telekommunikationssystemen
- Auffinden von Abhöreinrichtungen wie z. B. Wanzen, getarnte Bild-, Video- und Tonaufnahmegeräte oder dergleichen
- auffälliges oder ungewöhnliches Verhalten von Mitarbeitern, Praktikanten, Werkstudenten, Geschäftspartnern, Fremdfirmenmitarbeitern oder Dienstleistern
- ungewöhnliche Anwesenheit oder Arbeitszeiten von Mitarbeitern, Praktikanten, Werkstudenten, Geschäftspartnern, Fremdfirmen oder Dienstleistern
- auffällige Neugier oder ungewöhnliches Interesse am Unternehmen seitens interner oder externer Personen
- zwielichtige Ansprachen und Aushorchversuche durch bekannte oder unbekannte Personen im beruflichen oder privaten Umfeld (z. B. auf Messen, Veranstaltungen, Geschäftsreisen, im Privatbereich usw.)
- Unstimmigkeiten oder Ungereimtheiten im beruflichen Werdegang von Mitarbeitern, Praktikanten, Werkstudenten oder Geschäftspartnern
- Erhalt zweifelhafter Initiativbewerbungen
- Verstoß gegen Zutritts- und Zugriffsbeschränkungen
- untypische Einbruchs- und/oder Diebstahldelikte
- plötzlich eintretender Auftragsrückgang
- unerklärlich ansteigende Personalfluktuation
- vermehrte Personalabwanderung zu Marktbegleitern
- Verbreitung rufschädigender Firmeninterna

Fast jedes Unternehmen kann Ziel von Spionage sein – entscheidend ist nicht die Größe, sondern ausschließlich, ob wertvolles Know-how vorhanden ist.

Unternehmen, die in kritischen Ländern tätig sind, sind in besonderer Weise dem Risiko ausgesetzt, Opfer von Know-how-Diebstahl zu werden.

Know-how-Schutz sollte als Teil der Unternehmenskultur aufgebaut und fortentwickelt werden – der Aufbau eines individuell angepassten Sicherheitskonzeptes bietet hierfür eine wichtige Grundlage.

©sebra - stock.adobe.com

BEI FRAGEN RUND UM DAS THEMA „KNOW-HOW-SCHUTZ“ SOWIE FÜR DIE MITTEILUNG VON SACHVERHALTEN MIT SPIONAGERELEVANTEM HINTERGRUND STEHEN IHNEN DIE „LANDESÄMTER FÜR VERFASSUNGSSCHUTZ“ JEDERZEIT BERATEND ZUR SEITE.

EINZELASPEKTE DER WIRTSCHAFTSSPIONAGE UND DARAUS RESULTIERENDE SICHERHEITSMASSNAHMEN GREIFEN WIR REGELMÄSSIG IN UNSEREN AUSGABEN AUF. SCHAUEN SIE BEISPIELSWEISE IN AUSGABE 4, 5 ODER 9.

HINTERGRUNDWISSEN

NACHRICHTENDIENSTE IN DEUTSCHLAND

Nachrichtendienste sammeln Informationen über die innere und äußere Sicherheit eines Staates und werten diese aus. Hierbei können sie sowohl „offen“ als auch „verdeckt“ operieren. Die Ergebnisse der gewonnenen Informationen werden in Berichten zusammengefasst und den politischen Entscheidungsträgern sowie den zuständigen Kontrollgremien zur Verfügung gestellt. In der Bundesrepublik Deutschland existieren drei Nachrichtendienste, die in die Zuständigkeitsbereiche „Inlandsnachrichtendienst“ und „Auslandsnachrichtendienst“ unterteilt sind.

NACHRICHTENDIENSTE IN DEUTSCHLAND

DER VERFASSUNGSSCHUTZ

… ist der Inlandsnachrichtendienst der Bundesrepublik Deutschland. Hauptaufgabe des Verfassungsschutzes ist es, Bedrohungen für die im Grundgesetz verankerte, freiheitliche demokratische Grundordnung und die öffentliche Sicherheit weit im Vorfeld polizeilicher Maßnahmen zu erkennen, einzuschätzen und hierdurch eine Bekämpfung zu ermöglichen. Da der Verfassungsschutz in Deutschland föderal organisiert ist, existieren dementsprechend 17 Verfassungsschutzbehörden, bestehend aus einem Bundesamt für Verfassungsschutz und 16 Landesämtern für Verfassungsschutz.

DER BUNDESNACHRICHTENDIENST (BND)

… ist der Auslandsnachrichtendienst der Bundesrepublik Deutschland. Der BND hat die Aufgabe, im Ausland Informationen zu sammeln, die von außen- oder sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Neben den Kernaufgaben der Auslandsaufklärung übernimmt der Bundesnachrichtendienst zunehmend auch Aufgaben in der Beobachtung der international operierenden „Organisierten Kriminalität“, insbesondere auf den folgenden Gebieten:

- Waffen- und Technologietransfer,
- Geldwäsche sowie
- Menschenhandel und Rauschgiftschmuggel.

DER MILITÄRISCHE ABSCHIRMDIENST (MAD)

… ist der Nachrichtendienst der Bundeswehr. Auf dem Gebiet der Bundesrepublik Deutschland hat dieser in Form einer zivilen Verfassungsschutzbehörde des Bundes die Aufgabe, extremistische, sicherheitsgefährdende und geheimdienstliche Bestrebungen und Tätigkeiten innerhalb der Bundeswehr zu beobachten. Die Hauptaufgaben des Militärischen Abschirmdienstes liegen dabei in der Abwehr von Spionageaktivitäten sowie im Aufspüren verfassungsfeindlicher Bestrebungen innerhalb der Bundeswehr.

NACHRICHTENDIENSTE FREMDER STAATEN

Wie in den meisten Ländern dieser Welt sind auch in der Bundesrepublik Deutschland Nachrichtendienste fremder Staaten aktiv, um Informationen aus allen Bereichen des öffentlichen Lebens zu gewinnen wie beispielsweise

- politische,
- wirtschaftliche sowie
- militärische Entwicklungen und Entscheidungen.

Hinsichtlich ihrer Organisation und Befugnisse sind Nachrichtendienste fremder Staaten – je nach Herkunftsland – unterschiedlich ausgestaltet.

Quelle: Bundesamt für Verfassungsschutz

SICHERHEIT IST UNSERE STÄRKE

UNSERE LEISTUNGEN

- SICHERHEITSBERATUNG
- SICHERHEITSKONZEPTIONEN
- REISESICHERHEIT IM AUSLAND
- EXT. SICHERHEITSMANAGEMENT
- KRISEN- UND NOTFALLMANAGEMENT
- BUSINESS-CONTINUITY-MANAGEMENT
- SECURITY-AWARENESS VIA E-LEARNING

Besuchen Sie uns online:
www.sius-consulting.com

SIUS
Consulting

ERLÄUTERUNG DER UNTERSCHIEDLICHEN BEGRIFFLICHKEITEN IM NOTFALL- UND KRISENMANAGEMENT

Risikomanagement, Business Continuity Management, Notfall- und Krisenmanagement, Notfallplan(-ung), Störfallmanagement, Katastrophenvorsorge etc. – es existiert eine Reihe von unterschiedlichen Begrifflichkeiten, die die Abhandlung in gewissen (meist kritischen) Ereignissituationen abbilden und beschreiben. Doch jeder Begriff hat im Kern einen anderen Ursprung und verfolgt mitunter auch ein anderes Ziel.

> „EGAL AUS WELCHEM GRUND MAN SICH MIT DEM THEMA „SCHADENSEREIGNIS" AUSEINANDERSETZT – ES SOLLTE STETS EINE GANZHEITLICHE BETRACHTUNG STATTFINDEN, ALLE UNTERNEHMENSBEREICHE FRÜHZEITIG AKTIV EINBEZOGEN UND INSBESONDERE NACHHALTIG GEPLANT WERDEN.

Der Umgang mit Gefahren und Risiken und das i. d. R. damit einhergehende Notfall- und Krisenmanagement erlangten in den vergangenen Jahren eine zunehmende Bedeutung für Unternehmen, Behörden und Organisationen weltweit. Vielerorts wurden verschiedene Gefahren und Risiken inkl. deren (Schadens-)Eintrittswahrscheinlichkeiten ermittelt und analysiert sowie darauf aufbauend geeignete Mechanismen und Maßnahmen etabliert, um die diversen potenziellen (Schadens-)Ereignisse und (Schadens-)Ausmaße frühzeitig zu erfassen, unmittelbar zu beheben oder – sofern nicht möglich – zumindest weitestgehend „unbeschadet" zu überstehen.

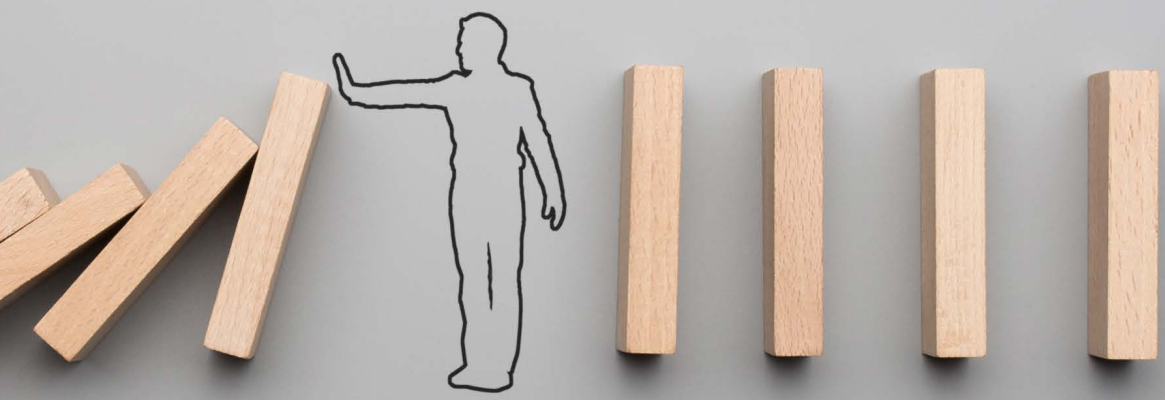
WÖRTLICHE BETRACHTUNG EINZELNER BEGRIFFE

Die wörtliche Betrachtung der einzelnen Begrifflichkeiten gibt einen ersten Anhaltspunkt, was sich dahinter verbirgt und worauf die Abhandlung abzielt. Fakt ist: es gibt keine allgemeingültigen Definitionen, denn je nach Herkunft des Arbeitsgebietes zielen die Begriffe auf unterschiedlichste Mechanismen ab. Im Risikomanagement gibt es beispielsweise die finanziellen Risiken aus dem Bereich der Betriebswirtschaft, die psychologischen Risiken, die technischen Risiken, Produktrisiken, Beschaffungsrisiken etc.

Daher betrachten wir die Begriffe im Nachfolgenden ausschließlich im Zusammenhang mit der „**UNTERNEHMENSSICHERHEIT**" und mit Blick auf **POTENZIELLE SCHADENSEREIGNISSE**.

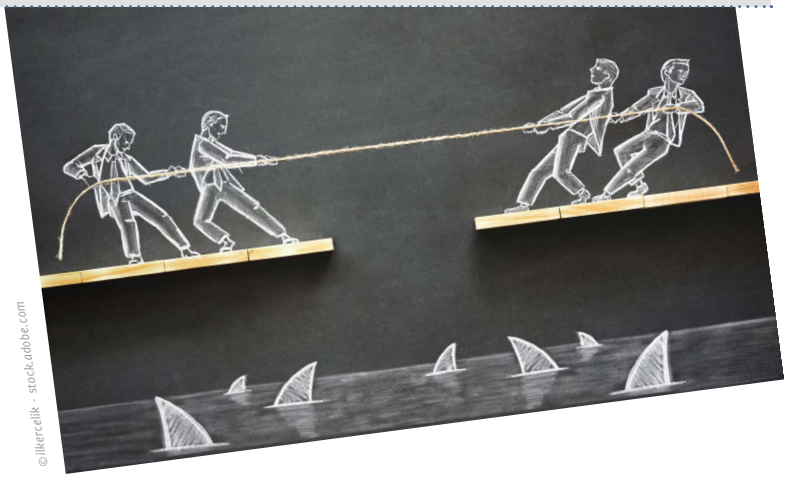
Das **RISIKOMANAGEMENT** dient dazu, Risiken zu identifizieren, zu analysieren und zu bewerten. Das bedeutet, dass potenzielle Schadensereignisse, die die Organisation betreffen, identifiziert und analysiert werden (*„Was könnte passieren und wie würde sich jenes Ereignis auf Personen, Sachwerte und die Umwelt auswirken?"*). Die Bewertung der Risiken erfolgt i. d. R. anhand von konkret messbaren Schwellenwerten und/oder der eigenen Risikoakzeptanz (*„Ab wann führt Ereignis X zu einem kritischen Ergebnis für das Unternehmen?"*). Risiken können dabei entweder aus dem Unternehmen heraus verursacht oder von außen hineingetragen werden.

Beispiele: Ausfall wichtiger Lieferanten, Ausfall infrastruktureller Einrichtungen, Arbeitsniederlegung, Sabotage, Informationsdiebstahl etc.



Das **NOTFALL- UND KRISENMANAGEMENT (NKM)** als Führungsmanagementmethode dient der ganzheitlichen Vorbereitung (und Planbarkeit) auf (unvorhersehbare) Schadensereignisse. Ein NKM kann potenzielle Gefahren und Risiken zwar nicht verhindern, allerdings ermöglicht es z. B. durch vordefinierte Strukturen (Aufbau- und Ablauforganisation) oder adäquate Melde- und Bewältigungsprozesse eine souveräne und systematische Handlungs- und Entscheidungsfähigkeit im Ernstfall. Hierdurch lassen sich Schäden für Menschen, Sachwerte und/oder die Umwelt frühzeitig eingrenzen, minimieren oder gar vollends abwenden.

Beispiele: Erstellung von Alarmierungs- und Meldeketten, Definition der Krisenstabsbesetzung sowie Festlegung geeigneter Räumlichkeiten, Erstellung ereignisspezifischer Notfall- und Krisenpläne, Erarbeitung und Vorhaltung eines Krisenkommunikationsplans, Durchführung von regelmäßigen Schulungen und Übungen zur Vorbereitung aller handelnden Akteure und Entscheidungsträger, stetige Aktualisierung und Fortschreibung aller damit einhergehenden Dokumente wie z. B. Notfall- und Krisenhandbuch, Pläne, Checklisten, Handlungsanweisungen etc.



Das **BUSINESS CONTINUITY MANAGEMENT (BCM)** zielt darauf ab, potenzielle Risiken zu vermeiden bzw. bei deren Eintritt abzumindern, indem z. B. konkrete Strategien, Pläne, Handlungsanweisungen und Prozesse (vor-) definiert werden, welche die Fortführung der Geschäftstätigkeit in den Vordergrund stellen. Das BCM ist eine Managementmethode, die feststellt, welche (zeitkritischen) Prozesse bei Schadensereignissen (z B. Betriebsstörung, Betriebsausfall, Ressourcenausfall etc.) zwingend aufrechterhalten werden müssen und welche präventiven Maßnahmen für diesen „Notbetrieb“ bzw. einen schnellen „Fortführungsbetrieb“ oder „Wiederanlauf“ notwendig sind. Betriebliche Prioritäten werden dabei ebenso definiert wie konkret notwendige Ressourcen, um die wirtschaftliche Existenz und damit den Fortbestand des Unternehmens trotz (Schadens-)Ereignis zu sichern.

Beispiele: Für den Ausfall der IT-Infrastruktur werden Redundanzen geschaffen oder definiert, für größere Personalausfälle werden aufgaben- bzw. funktionsspezifische Mindestbesetzungen festgelegt sowie Verträge mit Leiharbeitsfirmen vorgehalten etc.

Lesen Sie weiter auf Seite 10 ›››

Der Begriff **NOTFALLPLAN(-UNG)** kann sowohl aus dem BCM als auch dem NKM resultieren. Im NKM beschreiben Notfallpläne beispielsweise die ereignisspezifischen übergeordneten Regelungen im Hinblick auf die Ablauforganisation. Im BCM hingegen beschreiben Notfallpläne Regelungen im Hinblick auf Verantwortlichkeiten, Organisationseinheiten, Richtlinien und Verhaltensregelungen. Dabei agiert die Notfallplanung des NKM stets im Hinblick auf das gesamte Unternehmen, wohingegen die Notfallplanung im BCM die Behebung und somit die Fortführung eines konkret betroffenen Bereichs (Wiederanlauf) fokussiert.

Beispiel: IT-Ausfall

NKM-NOTFALLPLAN: Szenarienübergeordnete Krisenstabsmitglieder und Fachberater, Festlegung des Umgangs mit Anwendern (z. B. EDV-Nutzung untersagen, Personal bis zur Behebung nach Hause schicken, Ersatzbeschaffung/Neubeschaffung freigeben), interne und externe Kommunikationsstrategie definieren etc.

BCM-NOTFALLPLAN: Verantwortlich ist z. B. die IT-Leitung in enger Zusammenarbeit mit den entsprechenden Organisationseinheiten (z. B. Administratoren, Fachbereiche, Services), Herausgabe von Verhaltensempfehlungen für die Anwender im Unternehmen (Produktion, Verwaltung …) etc.

VIELE BEGRIFFE = UNTERSCHIEDLICHE BEDEUTUNG FÜR FACHPERSONEN UND „LAIEN“

Die Erläuterung der vorgenannten Begrifflichkeiten in unterschiedlichen Kontexten und unter Zuhilfenahme diverser rechtlicher Rahmenbedingungen oder branchenüblicher Standards könnte noch viele Seiten füllen. Viel wichtiger ist jedoch, dass Sie sich innerhalb Ihres Wirkungskreises im Unternehmen auf eine eindeutige, verständliche und nachvollziehbare Bedeutung der Begriffe einigen. Die Kontextklärung ist bekanntlich z. B. auch dann wichtig, wenn beispielsweise Angebote für Beratungsleistungen, Handbücher, Pläne, Schulungen, Workshops oder Übungen eingeholt werden sollen.

GETREU DEM PRINZIP:

„WAS SAGT DER KUNDE → WAS VERSTEHT DER ANBIETER“ ODER „WAS MEINT DER KUNDE → WAS BIETET DER ANBIETER“

Betrachtung der Begriffe im Zusammenhang mit der **„UNTERNEHMENSSICHERHEIT“** und mit Blick auf **POTENZIELLE SCHADENSEREIGNISSE**.

Das **STÖRFALLMANAGEMENT** bezeichnet gemeinhin den Umgang mit Alarmfällen oder (technischen) Störungen. Im Bereich der Unternehmenssicherheit bzw. des NKM bezeichnet ein Störungen gemäß gesetzlich verankerter Definition (beispielsweise im Bereich der „Chemiesicherheit“) eine Emission, einen Brand oder eine Explosion, die (Betriebs-)Bereiche innerhalb und/oder außerhalb betrifft und zu einer ernsten Gefahr für Mensch und Umwelt wird bzw. werden kann. Aber auch im Bereich des „Strahlenschutzes“ findet der Begriff Verwendung (beispielsweise in der Kerntechnik). Unternehmen, die unter derartige gesetzliche Regelungen fallen, müssen z. B. einen Alarm- und Gefahrenabwehrplan erarbeiten und vorhalten, der wiederum dem NKM bzw. BCM in Teilen sehr ähnelt.

Die **KATASTROPHENVORSORGE** bzw. der Begriff der „Katastrophe“ bezeichnet außerbetriebliche (Großschadens-)Ereignisse in Bezug auf den (behördlichen) Zivil- und Katastrophenschutz und die Blaulichtorganisationen im weitesten Sinne. In Unternehmen wird als Synonym i. d. R. der Begriff „Krise“ und somit das Notfall- und Krisenmanagement verwendet. Dennoch gibt es auch hier vereinzelt Mischformen, wie z. B. im Bereich der kritischen Infrastrukturen. Beispielsweise zu nennen sind hier Krankenhäuser, die im Rahmen der (behördlichen) Katastrophenvorsorge im Zusammenhang mit den Katastrophenschutzgesetzen der jeweiligen Bundesländer agieren, aber auch im Bereich des NKM – das wiederum auf ganz andere (betriebliche) Szenarien abzielt – aufgestellt sein sollten.

„MASKEN-TÜRSTEHER“ ERLEICHTERN DEN GESCHÄFTSALLTAG

Die zweite Corona-Welle hat an Fahrt aufgenommen. Seit ein paar Wochen befindet sich Deutschland wieder im „Teil-Lockdown“. Das Tragen des Mund-Nasen-Schutzes sollte mittlerweile Alltag in der Öffentlichkeit sein. Doch weit gefehlt! Wer sich ab sofort nicht an die Hygieneregeln hält und beispielsweise beim Betreten eines Geschäftes, einer öffentlichen Einrichtung oder in Bürogebäuden ohne Maske erscheint, bekommt etwas zu hören.

Damit ist nicht die Stimme eines Mitarbeiters gemeint, die in Zeiten der Corona-Pandemie an den Eingängen positioniert sind und auf die Einhaltung der Corona-Infektionsschutzmaßnahmen hinweisen. Maskenmuffel können fortan von einem Alarmton ermahnt werden, der von einem Scanner ausgeht und automatisch erkennt, ob jemand eine Maske trägt oder nicht.

FUNKTIONSWEISE VON MASKENSCANNERN

Die Funktionsweise solcher Geräte ist einfach: Ein Tablet mit einer hochauflösenden Kamera wird auf Augenhöhe in Eingangsbereichen, Fluren oder in Geschäften aufgestellt. Der Scanner schlägt sofort Alarm, wenn eine Person an dem Gerät vorbeigeht, die keinen oder einen nicht richtig positionierten (z. B. nur am Kinn, nicht bis über die Nase) Mund-Nasen-Schutz trägt. Das Display leuchtet in einem solchen Fall sofort rot und weist darauf hin, einen Mund-Nasen-Schutz zu tragen.

Maskenscanner sind mit einem Akku ausgestattet. Auf diese Weise lassen sie sich jederzeit dort aufstellen, wo sie gebraucht werden. Zusatzfunktionen, wie das Bedanken bei Personen, die sich an die Regeln halten oder bei denen das automatische Fiebermessen integriert ist, sind ebenfalls auf dem Markt erhältlich.

Auch auf das Thema des Datenschutzes wird bei solchen Produkten geachtet. Maskenscanner arbeiten i. d. R. als sogenannte „Stand-Alone-Lösung“ im Offline-Betrieb – ohne Verbindung ins WLAN, LAN oder Internet. Es werden beispielsweise bei dem Maskenscanner MaskControl® keine personenbezogenen Daten gespeichert, da der Video-Feed in Echtzeit (Momentaufnahme) ausgewertet wird.

VORTEILE VON ELEKTRONISCHEN TÜRSTEHERN

Infektionsschutzthemen und somit auch das Tragen des Mund-Nasen-Schutzes werden uns noch lange begleiten. Die Vorteile liegen klar auf der Hand:

- Reduzierung der Personalkosten (ca. 2.500 EUR für den Kauf eines Maskenscanners oder ca. 3.200 EUR für einen Mitarbeiter im Eingangsbereich/pro Monat)
- Mietoption für Maskenscanner
- Förderung für bestimmte Branchen (z. B. Krankenhäuser, Pflegeeinrichtungen)
- Wahrung der Infektionsschutzmaßnahmen mindert Bußgeldforderungen
- Anpassung der Ansprache und des Alarmsignals möglich
- Einsatz rund um die Uhr

Dieser Artikel ist mit freundlicher Unterstützung von Martin Walter (MaskControl®) und Heiner Harke (PART OF SUCCESS GmbH) entstanden.

„DAS ROBERT KOCH-INSTITUT GEHT AKTUELL DAVON AUS, DASS DIE MASKE AUCH DANN NOCH GETRAGEN WERDEN MUSS, WENN DER LANGERSEHNTE IMPFSTOFF ENDLICH DA IST.

Abb.: MaskControl®

VERDÄCHTIGE POSTSENDUNGEN:

MODERNE POSTEINGANGS-KONTROLLE DURCH (SICHERHEITS-)TECHNISCH GESTÜTZTE LÖSUNGEN

Der Austausch von Informationen findet heutzutage häufig über digitale Plattformen wie E-Mail oder Messenger-Dienste statt. Dennoch gibt es wichtige Dokumente, persönliche Briefe oder amtliche Unterlagen, die per Post zugestellt werden (müssen). Der Versand von Päckchen und Paketen hat in den vergangenen Jahren – nicht zuletzt durch diverse Onlinedienste – sogar zugenommen. Daher besteht auch weiterhin die Gefahr, dass mittels Brief, Päckchen oder Paket gefährliche (explosive) Inhalte versendet werden.

Der Auszug der Briefbomben(-anschläge) der vergangenen Jahre verdeutlicht einmal mehr, wie latent die Gefahr ist, und zwar für jeden von uns, der Brief- und Postsendungen öffnet. Die Anzahl nicht bekanntgewordener Briefbombenanschläge ist laut inoffiziellen Informationen aus den Sicherheitsbehörden deutlich höher. Gleiches gilt für die Anzahl an Postsendungen mit gefährlichen Gegenständen. Dies können z. B. Messer oder auch Rasierklingen sein, die den Adressaten beim Öffnen der Sendung verletzen sollen. Aber auch der Versand von Betäubungsmitteln auf dem Postweg ist keine Seltenheit und sollte entsprechend detektiert werden können.

GEFAHREN UND RISIKEN DURCH GEFÄHRLICHE POSTSENDUNGEN

Insbesondere Mitarbeiter/-innen in den Poststellen von Unternehmen, Organisationen oder öffentlichen Einrichtungen wie beispielsweise Ministerien, Behörden, Botschaften, Justizvollzugsanstalten, Gesundheitsämtern oder bei Betreibern kritischer Infrastrukturen sind latent bedroht. Aber auch alle anderen Personen, die Briefe, Päckchen oder Pakete öffnen, wie beispielsweise Assistenzen, Sekretariate, Kollegen der Empfänger und natürlich die Empfänger selbst, können mitunter gefährdet sein.

Briefbombe in Paris an den Internationalen Währungsfonds (IWF) im Jahr 2017

Serie von 16 Briefbomben an prominente Demokraten und Kritiker von Donald Trump in den USA im Jahr 2018

Mehrere Briefbomben an diverse Empfänger in London im Jahr 2019

Briefbombenfund im Kanzleramt im Jahr 2019

Serie von 11 Briefbomben in den Niederlanden seit Anfang des Jahres 2020

BEKANNTGEWORDENE BRIEFBOMBEN(-ANSCHLÄGE) JÜNGSTER VERGANGENHEIT

HUNDERTE BRIEFE, PÄCKCHEN UND PAKETE KOMMEN IN UNTERNEHMEN, BEHÖRDEN UND ORGANISATIONEN TÄGLICH AN – DARUNTER IN SELTENEN FÄLLEN AUCH SOLCHE MIT GEFÄHRLICHEM INHALT.

Den typischen Empfänger von Briefbomben gibt es genauso wenig wie den typischen Versender von Briefbomben. Aber die Vergangenheit zeigt, dass insbesondere Politiker/-innen und Prominente bzw. in der Öffentlichkeit stehende Personen, aber auch Entscheidungsträger, die schnell zu „Gegnern" werden können, betroffen sind. Die Tatmotive reichen von extremistischen oder politischen Hintergründen bis hin zu kriminell motivierten oder emotionalen und persönlichen Taten.

ERKENNUNGSMERKMALE VERDÄCHTIGER POSTSENDUNGEN

Viele Postsendungen werden heutzutage noch per Hand kontrolliert, also durch optische und haptische Prüfung. Um verdächtige Sendungen zu erkennen, gibt es einige Merkmale, die auf eine verdächtige Postsendung hinweisen können wie z. B.:

- ungewöhnliche Dicke oder Form
- hohes Gewicht bezogen auf die Größe der Postsendung
- optisch passt die Postsendung nicht mit dem vermuteten Inhalt überein
- unübliches/übertriebenes Verpackungsmaterial
- Unebenheiten bzw. fühlbare, harte Gegenstände im Inneren des Umschlags
- ölige Flecken oder Verfärbungen
- strenger/außergewöhnlicher Geruch
- Postsendung ist über das notwendige Maß hinaus frankiert
- ungewöhnliche Zustellungsart (Postsendung wurde nicht durch einen kommerziellen Zusteller ausgeliefert)
- fehlerhafte Empfängeradresse
- Angabe eines Titels, aber keine Namensangabe des Empfängers
- Rechtschreibfehler
- Hinweise wie „Vertraulich", „Persönlich", „Privat", „Nur vom Empfänger zu öffnen"
- fehlender, seltsamer, unbekannter bzw. nicht existenter Absender
- anderer Aufgabeort als im Absender vermerkt

Ein entsprechendes Merkblatt haben wir in unserem Downloadbereich für Sie zur Verfügung gestellt.

Diese Erkennungsmerkmale sind heutzutage kein Geheimnis und somit auch den Versendern von gefährlichen Postsendungen bekannt. Daher ist die manuelle Kontrolle von Postsendungen nicht immer die beste Variante, da die potenziellen Täter die o. g. Merkmale möglichst auszuschließen versuchen. Händische Prüfungen haben oftmals auch das Problem, dass die Postsendungen zusätzlichen mechanischen Belastungen ausgesetzt werden, die zu einer Explosion oder zur Freisetzung von Gefahrstoffen führen können. Letztlich erhöht die händische Prüfung die Gefahr für die prüfenden Personen.

MEHR SICHERHEIT DURCH TECHNISCH GESTÜTZTE POSTEINGANGSKONTROLLE

Um die Sicherheit der Posteingangskontrolle zu erhöhen bzw. potenzielle Gefahren zu reduzieren, gibt es sogenannte „Postscanner", die Briefe und kleine Päckchen – ohne dass diese geöffnet werden müssen – auf Gefahren hin überprüfen. Postscanner visualisieren die Objekte in den Sendungen, wodurch sich Rückschlüsse auf gefährliche Substanzen ziehen lassen.

Neue Technologien technischer Kontrollmethoden können gänzlich auf Röntgenstrahlung verzichten, da sie beispielsweise mit Terahertz-Frequenzen (THz) arbeiten – ähnlich wie Sicherheitsscanner an Flughäfen – und somit aufgrund der geringen Energie für den Menschen ungefährlich sind. Da die Geräte der neuesten Generation nur noch über eine 230 Volt-Steckdose betrieben werden und die Größe eines Druckers aufweisen, sind sie leicht zu transportieren und somit auch für Räumlichkeiten mit wenig Platz gut geeignet. ›››

VERGLEICH RÖNTGENANSICHT UND THZ-SCANNER

Röntgenansicht *Postsendung* *THZ-Scanner*

Röntgengeräte nutzen für den Menschen schädliche Röntgenstrahlung (trotz deren Abschirmung) und benötigen entsprechende Abnahmen, verstärkte Schulungen der Mitarbeiter, Überprüfungen durch Prüfvereine, besondere Anforderungen an die Aufstellflächen und dergleichen. Das bedeutet: trotz der bewährten Technik ist der zusätzliche Aufwand nicht zu unterschätzen.

WAS SIND TERAHERTZWELLEN?

THz-Wellen stehen im Wesentlichen für den Frequenzbereich des elektromagnetischen Spektrums zwischen 0,1 THz und 10 THz. Viele elektrisch nichtleitende Materialien können durchdrungen und somit optisch dargestellt werden. Somit lassen sich Gegenstände in Postsendungen farblich kodiert und in unterschiedlichen Ansichten auf dem Bildschirm darstellen und verborgene, kleine, interne Strukturen und unterschiedliche Materialien in der Sendung werden sichtbar. Beim Durchleuchten des Materials wird neben der Absorption auch die Laufzeit des ausgesendeten Signals durch das Material hindurch gemessen. Dadurch können geringste Unterschiede detektiert werden.

Ein weiterer technischer Vorteil von Terahertz-Scannern gegenüber herkömmlichen vergleichbaren Röntgengeräten ist, dass dünnschichtige Pulverlagen mit THz-Wellen aufgrund der hohen Sensitivität besser erkannt werden können. Des Weiteren bieten derartige Systeme die Überlagerung von Originalbild und gescanntem Bild an, um Bereiche mit gefährlichen Gegenständen besser zuordnen zu können. Diese Information kann beispielsweise an den Empfänger weitergegeben werden mit der Frage, ob eine solche Sendung erwartet wird oder diese direkt an die Ermittlungsbehörden übergeben werden soll.

Überlagerung original und gescanntes Bild

Bildquelle: HÜBNER GmbH & Co. KG

VORTEILE FÜR ANWENDER

Der Einsatz von gesundheitlich unschädlichen THz-Scannern bei der Posteingangskontrolle hat viele Vorteile für den Anwender, wie z. B.:

- keine Röntgenstrahlung
  (dadurch keine Anforderungen aus dem Strahlenschutz)
- hoher Durchsatz (bis zu 1.000 Briefe pro Stunde)
- kurze Einweisungsdauer
- mehr Sicherheit für das Personal
- hohe Mobilität der Geräte
- Inhaltsprüfung, ohne das Postgeheimnis zu berühren
- hohe Sensitivität bei dünnschichtigen Pulverlagen
- intuitive Bedienung
- Überlagerung von Originalbild und gescanntem Bild

Trotz der technischen Möglichkeiten ist es essenziell, Mitarbeiter der Posteingangskontrolle auf das Gefährdungspotenzial hinzuweisen und entsprechend im Erkennen

VERHALTENSREGELN BEIM AUFFINDEN VERDÄCHTIGER POSTSENDUNGEN

- ☐ Ruhe bewahren!
- ☐ Kein Risiko eingehen!
- ☐ Die verdächtige Postsendung
  - ... nicht berühren!
  - ... nicht abtasten!
  - ... nicht bewegen!
  - ... nicht schütteln!
  - ... nicht biegen oder knicken!
- ☐ Keine Öffnungsversuche jedweder Art unternehmen.
- ☐ Keiner extremen Hitze (z. B. Heizung oder direkte Sonneneinstrahlung) oder Kälte aussetzen.
- ☐ Keine Mobiltelefone oder Funkgeräte in unmittelbarer Nähe verwenden.
- ☐ Gegenstand/Sendung nicht ins Wasser legen oder anfeuchten.
- ☐ Alle Personen zum Verlassen des Gefahrenbereichs (z. B. Poststelle, Büro) auffordern und den Bereich absperren (lassen) und dann auch selbst den Gefahrenbereich verlassen.
- ☐ Unverzüglich die internen Sicherheitsprozesse einleiten, wie z. B. die interne Notfallnummer und/oder die Polizei anrufen.
- ☐ Nach dem Eintreffen der Sicherheitskräfte bzw. Polizei/Feuerwehr, diese über die Erkenntnisse und bisherigen Maßnahmen umfassend informieren.

©yuriygolub - stock.adobe.com

und Umgang mit verdächtigen (explosiven) Post- und Paketsendungen zu sensibilisieren. Denn nicht selten kann die Nichtentdeckung gefährlicher (explosiver) Gegenstände zu einer massiven Gefährdung für Leib und Leben führen – daher ist die erste Reaktion oftmals entscheidend für den weiteren Verlauf.

Dem Erkennen von verdächtigen Postsendungen kommt auch zukünftig eine wichtige Aufgabe zu, die sich mit technischen Mitteln unterstützen lässt, um Unternehmen, Behörden und Organisationen bestmöglich zu schützen

KOSTENFREIES E-LEARNING-TRAINING
› UMGANG MIT BOMBENDROHUNGEN, VERDÄCHTIGEN POSTSENDUNGEN UND GEGENSTÄNDEN ‹

Senden Sie einfach eine E-Mail mit dem Betreff **„E-Learning - verdächtige Postsendungen“** an redaktion@sicherheit-das-fachmagazin.de und Sie erhalten einen kostenfreien E-Learning-Zugang*.

**Maximal 1 personenbezogener Zugang pro Unternehmen. Gültigkeit 2 Wochen ab Erhalt der Zugangsdaten.*

Dieser Artikel ist mit freundlicher Unterstützung von Thorsten Sprenger, Head of Terahertz-Technology & Photonics der HÜBNER GmbH & Co. KG, entstanden.

SICHERHEITSMASSNAHMEN IN DEN KÖPFEN VERANKERN: WIE DAS THEMA „SICHERHEIT“ ZU MITARBEITERN VORDRINGEN KANN!

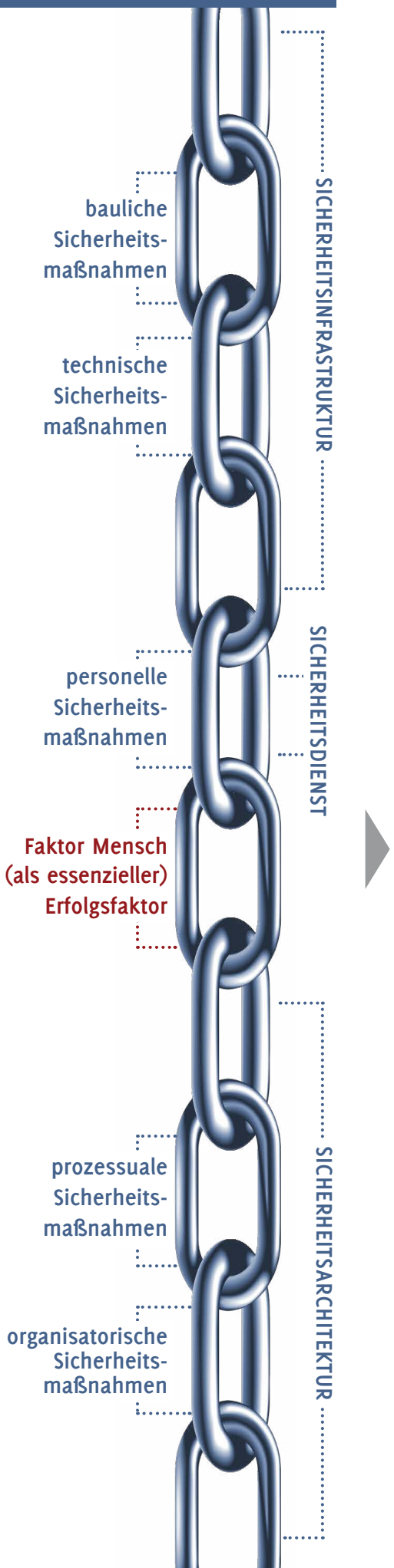
In jedem Betrieb gibt es Mitarbeiter, die die Gefahren und Risiken im Zusammenhang mit den Themen „Unternehmenssicherheit“ und „Wirtschaftsschutz“ inklusive der damit verbundenen Sicherheitsmaßnahmen nicht ernst nehmen. „Auslöser“ von Sicherheitslücken und Sicherheitsvorfällen werden vielerorts bedingt durch Unwissenheit, mangelndem Verständnis für das Thema „Sicherheit“, Unbekümmertheit oder fehlendem Verantwortungsbewusstsein. Viele Sicherheitsverantwortliche fragen sich daher, wie sie Mitarbeitern – aber auch Besuchern, Dienstleistern oder Fremdfirmenmitarbeitern – die vielfältigen Sicherheitsmaßnahmen und Sicherheitsvorkehrungen im Betrieb näherbringen können. Auf diese Frage möchten wir mit diesem Artikel einen ersten Anreiz geben.

Sicherheitsdefizite und Sicherheitslücken lassen sich durch rein technische Maßnahmen nicht lösen. Denn „Sicherheit“ ist stets ein Zusammenspiel von baulichen, technischen, personellen und organisatorischen Sicherheitsmaßnahmen, die nur im Einklang miteinander funktionieren, wenn der Faktor „Mensch“ mit seinen diversen Einflussfaktoren („menschlichem Verhalten“) als Anwender und Nutzer diese auch korrekt und wie vorgesehen anwendet. Menschen sind schon immer das zentrale Bindeglied zwischen der Sicherheitsarchitektur und der Sicherheitsinfrastruktur. Denn der Mensch ist es, der Türen offenlässt, Passwörter zu einfach gestaltet, den Firmenausweis Dritten überlässt, den Laptop mit wichtigen Daten verliert, Informationen zu bereitwillig teilt, vertrauliche Unterlagen offen liegen lässt etc.

Viele Unternehmen etablieren technische Vorsorgemaßnahmen und schaffen Redundanzen. Das ist natürlich gut, jedoch teilweise zu kurz gedacht, denn zu diesen präventiven Maßnahmen, die ein gewisses Problembewusstsein implizieren, gehören strategische Sicherheitsüberlegungen genauso dazu, um alle Glieder der Sicherheitskette zu integrieren.

> „DER MENSCH IST NICHT NUR GRÖSSTER RISIKOFAKTOR, SONDERN VIELMEHR AUCH EIN ESSENZIELLER ERFOLGSFAKTOR FÜR MEHR SICHERHEIT IM UNTERNEHMEN!

Somit ist es der Mensch, der verstanden, erreicht und am Ende auch von der Sinnhaftigkeit der Maßnahmen überzeugt werden muss. Veränderungen und damit einhergehende (neue) Prozesse brauchen immer ihre Zeit. Mitarbeiter, die bis



heute Türen aufgehalten haben, werden es nicht unterlassen, nur weil einmal erwähnt wurde, dies nicht mehr zu tun.

DIE RELEVANZ VON AWARENESS-KAMPAGNEN

Awareness-Maßnahmen sind i. d. R. nur schwer nachweisbar und somit nicht eindeutig messbar. Daher agieren viele Unternehmen wie eh und je und hoffen, dass am Ende nichts passiert und falls doch, dann wird zumindest dieses eine Problem abgestellt.

Doch ein System (eine Organisation, ein Unternehmen) kann nur funktionieren, wenn Menschen intervenierend in sicherheitsrelevante Prozesse oder Arbeitsabläufe eingreifen, um die sichere Fortführung des unternehmerischen Handelns aufrechtzuerhalten. Dies führt uns beispielsweise insbesondere die Informationssicherheit und der Datenschutz regelmäßig vor Augen.

> **WISSEN IST MACHT: DAHER SOLLTEN WISSENSVORSPRÜNGE ALS WETTBEWERBSFAKTOR GENUTZT WERDEN.**

ZUR RISIKOERKENNUNG/-VERMEIDUNG REICHT WISSEN ALLEIN NICHT AUS

Ganzheitliches Lernen besteht aus den Komponenten: **WISSEN, KÖNNEN** und **WOLLEN.**

Wenn wir etwas **wissen**, aktivieren wir Gelerntes und Erfahrenes, erkennen somit Probleme und wissen, was zu tun ist.

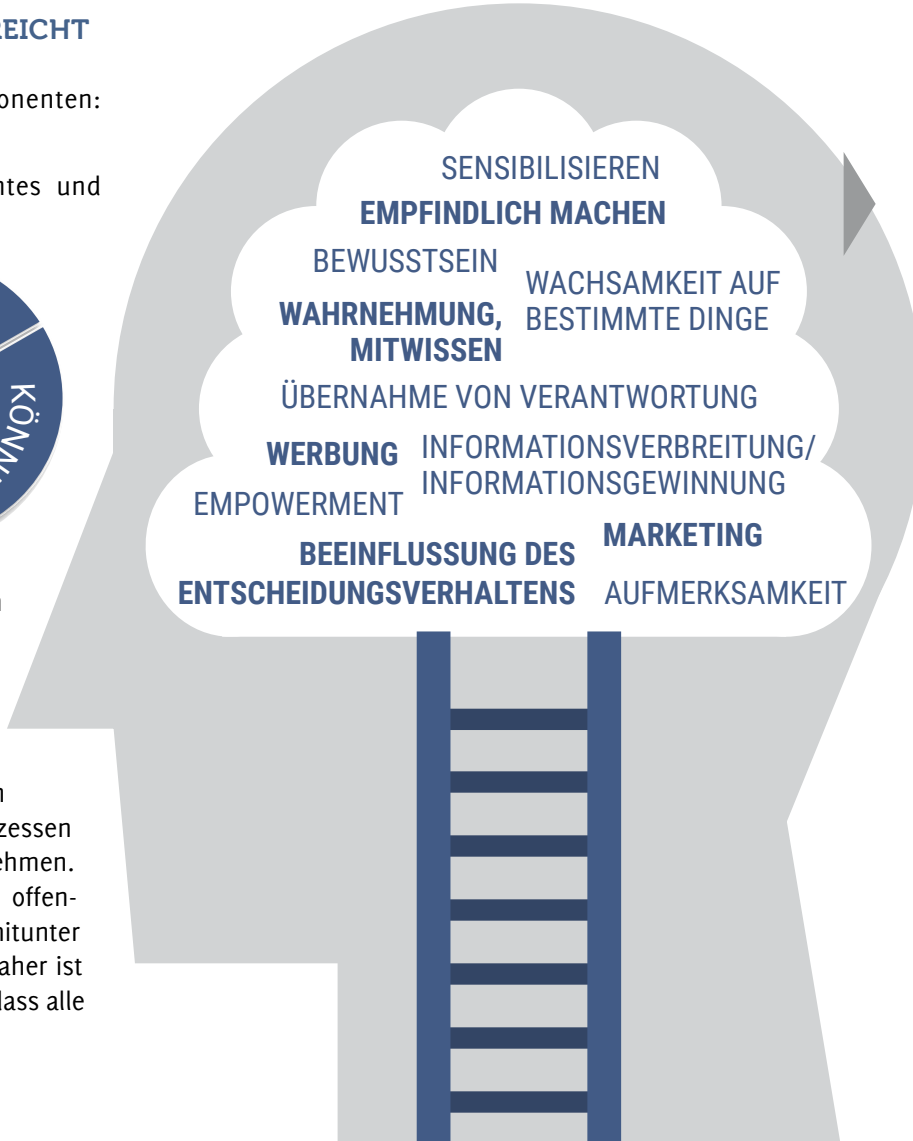
Wenn wir etwas **können**, wenden wir das erworbene Wissen im organisatorischen Umfeld an, in dem sicherheitskonformes Handeln grundsätzlich umsetzbar und möglich ist.

Wenn wir etwas **wollen**, orientieren wir uns an dem Ziel des sicherheitskonformen Handelns. (Intrinsische) Motivation sorgt dabei für den nötigen Antrieb.

Security-Awareness ausschließlich auf den Faktor „Wissen“ zu reduzieren ist zu kurz gedacht. Nachhaltige Effekte der kontinuierlichen Veränderung erzielt man nur mit interaktiven Prozessen und interagierend mit allen Beteiligten im Unternehmen. Ein Mitarbeiter allein (der z. B. unbehelligt Türen offenlässt, Phishing-Mails öffnet etc.) reicht aus, um (mitunter schwerwiegende) Sicherheitslücken zu schaffen. Daher ist für eine Security-Awareness-Kampagne essenziell, dass alle Personen (intern und ggf. extern) im Organisationsgebilde zielgruppengerecht angesprochen werden, um erlerntes Sicherheitswissen und somit sicheres Handeln dauerhaft einzusetzen. Insbesondere die Loyalität und Identifikation der Mitarbeiter mit dem Unternehmen müssen im Rahmen einer guten Awareness-Kampagne thematisiert werden, denn nur motivierte und loyale Mitarbeiter werden sich langfristig an (Sicherheits-)Regeln und (Sicherheits-)Maßnahmen halten sowie an (Sicherheits-)Richtlinien orientieren.

> **DIE INTRINSISCHE MOTIVATION MÖGLICHST ALLER MITARBEITER IST DER SCHLÜSSEL ZU SICHERHEITSBEWUSSTEM HANDELN:** *„ICH MÖCHTE HIER NOCH LANGE ARBEITEN UND BIN ZUFRIEDEN, DESWEGEN SCHÜTZE ICH DAS (MEIN) UNTERNEHMEN."*

Allein der Kontext, in dem Security-Awareness Betrachtung findet, bietet viele Interpretationsmöglichkeiten: IT-Sicherheit, Informationssicherheit, Datenschutz, Risikomanagement, Compliance, Unternehmenssicherheit, Wirtschaftsschutz … ›››



AWARENESS-MASSNAHMEN

Security-Awareness ist ein vielfältiger Begriff mit einer vielfältigen Bedeutung, der aus den unterschiedlichsten Blickwinkeln betrachtet wird. Da wären die psychologischen Aspekte der Werbung und Gestaltung sowie der tiefenpsychologische Ansatz ebenso wie Kommunikationstheorien, Marketingaspekte, die Sicherheits- und Unternehmenskultur als solches und das „Sicherheit lernen". Sensibilisierung lässt sich mit den unterschiedlichsten Mitteln erreichen, die je nach Reifegrad der Organisation, der Unternehmenskultur sowie der Vorkenntnisse und Lernerfahrung unterschiedlich sein können:

- Präsenzschulungen, Workshops
- Webinare, Onlineschulungen
- E-Learning
- Poster, Flyer
- Give Aways
- Spiele
- Newsletter, Blogs, Beiträge, Intranet
- Filme, Hörspiele, Podcasts, Apps
- u. v. m.

KENNEN SIE DAS?

Viele Awareness-Schulungen laufen immer nach dem gleichen Schema ab: allgemeine Phrasen und jedes Jahr dieselben Themen. Mitarbeiter sind oft schon gelangweilt, noch bevor sie den Schulungsraum betreten.

Leider wird das Thema „Sicherheit" im Unternehmen oft als Hindernis wahrgenommen. Sicherheitsmaßnahmen sollen aber nicht hindern oder hemmen, sondern die Mitarbeiter aktiv begleiten, nachhaltige Akzeptanz schaffen und am Ende auch „Spaß" machen.

Unterschiedliche **MASSNAHMEN** und **HERANGEHENSWEISEN** im Bereich „Security-Awareness" sind zwingend notwendig, um die unterschiedlichen Personen (und Lerntypen!) individuell und zielgerichtet anzusprechen.

ETWAS AUDITIVES
z. B. Präsenzschulungen, Podcasts, Hörspiele etc.

ETWAS VISUELLES ZUM LESEN
z. B. Newsletter, Intranet-Rubrik, Bildschirmschoner etc.

ETWAS VISUELLES ZUM ANSCHAUEN
z. B. Poster, Faltblätter, Präsentationsfolien, Videos etc.

ETWAS HAPTISCHES
z. B. Give Aways, Mitmach-Stationen, Live-Demonstrationen etc.

ETWAS KOMMUNIKATIVES
z. B. Mitarbeitergespräch, Workshop, Austausch innerhalb der Belegschaft etc.

Die Möglichkeiten der Kreativität sind schier unendlich. Es müssen jedoch sinnvolle Anreize geschaffen werden, um die Zielgruppen (Personen) im Unternehmen zum Mitdenken anzuregen. Im Vorfeld jeder „Security-Awareness-Idee" sollte das Gespräch mit der Geschäftsführung, dem Betriebsrat/Personalrat sowie den zuständigen (Sicherheits-)Abteilungen wie z. B. IT, Informationssicherheit, Datenschutz, Compliance etc. stehen, nicht zuletzt, um erforderliche Ressourcen zu definieren und gemeinsame Lösungen und Kampagnen abzustimmen und zu verabschieden.

„DENKEN SIE STETS DARAN: IHRE MITARBEITER SIND EINE VERTEIDIGUNGSLINIE ZWISCHEN ANGREIFER UND UNTERNEHMEN!

Bringen Sie ihre Mitarbeiter dazu, mitzudenken und mitzuwirken, denn Sicherheit steht und fällt mit der Aufmerksamkeit und Achtsamkeit der Personen im Unternehmen.

SECURITY AWARENESS

AUFMERKSAMKEIT ERREGEN
\+ WISSEN TRANSFERIEREN
\+ MITARBEITER SENSIBILISIEREN
= SICHERHEITSBEWUSSTSEIN STÄRKEN UND SOMIT SICHERHEIT ETABLIEREN

Mitarbeiter sollten Gefahren und Risiken kennen und wissen, worin ihr individueller Beitrag zu mehr Sicherheit besteht.

GGF. KANN HIER AUCH DIE MARKETINGABTEILUNG EINE HILFREICHE (UND NICHT SELTEN UNTERSCHÄTZTE) STÜTZE SEIN!

In unserem Downloadbereich finden Sie ein kostenfreies Security-Awareness-Poster.

Sicherheit im Home-Office

- EFFEKTIVE SCHUTZMASSNAHMEN BEI DER MOBILEN ARBEIT -

1. Sichere Arbeitsumgebung: Bitte achten Sie beim mobilen Arbeiten stets darauf, dass Sie sich in einer räumlich geschützten und ungestörten Arbeitsumgebung befinden, damit z. B. vertrauliche Gespräche oder der Austausch sensibler Informationen zur Erledigung Ihrer täglichen Aufgaben „sicher“ durchgeführt werden können.

2. Schutz von Daten: Bitte lassen Sie firmeninterne oder firmenbezogene Dokumente, Aufzeichnungen, Notizen etc. weder in physischer noch in elektronischer Form für andere Pearsonen „offen“ bzw. sichtbar liegen – auch nicht bei „nur“ kurzzeitiger Abwesenheit.

3. Schutz von Passwörtern: Bitte achten Sie darauf, firmen- oder arbeitsbezogene Passwörter zu schützen, indem Sie diese weder aufschreiben noch anderen Personen mitteilen oder in sonstiger Weise zugänglich machen.

4. Sicherheit in der Öffentlichkeit: Bitte achten Sie auch außerhalb Ihrer privaten Räumlichkeiten konsequent darauf, dass andere Personen keinen ungeschützten Blick auf Ihren Arbeitsbildschirm oder firmeninterne bzw. firmenbezogene Dokumente, Aufzeichnungen, Notizen etc. erhalten können.

5. Schutz vor Mithören: Bitte achten Sie bei firmeninternen oder firmenbezogenen Telefongesprächen oder Videokonferenzen stets darauf, dass andere Personen hierbei nicht ohne Weiteres mithören bzw. zusehen können.

6. Sicherheit geht vor Höflichkeit: Sollten Sie auf elektronischen oder telefonischen Wegen oder im zwischenmenschlichen Austausch (egal ob beruflich oder privat) dazu aufgefordert werden, vertrauliche Daten oder Informationen preiszugeben bzw. weiterzuleiten oder zu einer anderen Art der angeblich „dringenden Handlung“ aufgefordert werden, gehen Sie am besten mit einer kurzen Rückfrage an der richtigen Stelle auf Nummer sicher, denn dies kann mitunter großen Schaden abwehren.
Denken Sie stets daran: in der heutigen Zeit können sowohl die Absenderadressen von E-Mails als auch die Rufnummernanzeigen auf Telefondisplays gefälscht werden.

> **„Jede (Sicherheits-)Kette ist nur so stark wie ihr schwächstes Glied!“**

7. Melden von Sicherheitsvorfällen (und Verdachtsfällen): Sollte Ihnen ein Sicherheitsvorfall, z. B. in Bezug auf die Themen Compliance, Datenschutz, IT-Sicherheit, Notfall- und Krisenmanagement etc., bekannt werden oder sollten Sie diesbezüglich ggf. einen begründeten (Anfangs-) Verdacht haben, setzen Sie sich bitte umgehend mit der zuständigen Stelle oder Ihrem Vorgesetzten in Verbindung.

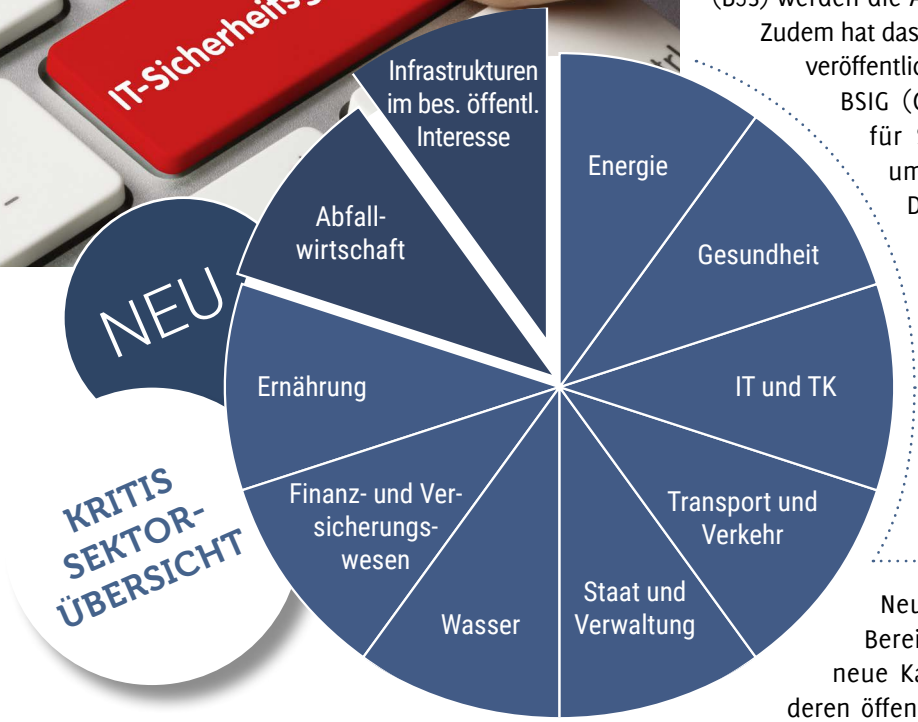
Denken Sie stets an den Spruch:

„Lieber einmal zu viel gemeldet als einmal zu wenig.“

IT-SICHERHEITSGESETZ 2.0: NEUREGELUNGEN FÜR KRITIS-BETREIBER

Die Gefahr durch Cyberangriffe auf die öffentliche Infrastruktur nimmt seit Jahren zu. Mögliche Folgeszenarien sind düster. Wer Schaden anrichten möchte, hat ein leichtes Spiel. Bedrohlich wird es da, wo öffentliche (infrastrukturrelevante) Stellen betroffen sind, wie etwa Krankenhäuser, Energieversorger, staatliche Einrichtungen oder Transportunternehmen. Aus diesem Grund befindet sich das bereits seit 2015 geltende IT-Sicherheitsgesetz in überarbeiteter Form auf der Zielgeraden des Gesetzgebungsprozesses.

> DER GROSSTEIL DER BEKANNTEN IT-SICHERHEITSLÜCKEN IST SEIT MINDESTENS EINEM JAHR BEKANNT. DIES BELEGEN STUDIEN WIE DER „DATA BREACH INVESTIGATIONS REPORT" VON VERIZON, DEMZUFOLGE SOGAR 99,9 % ALLER AUSGENUTZTEN SCHWACHSTELLEN SCHON SEIT ZWÖLF MONATEN ODER LÄNGER BESTEHEN.



Ziel des „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetzes 2.0 oder IT-SiG 2.0) ist kein geringeres, als die IT-Infrastruktur in Deutschland zu einer der sichersten der Welt zu machen. So sind Betreiber „Kritischer Infrastrukturen" (KRITIS) bereits heute dazu verpflichtet, ein Mindestmaß an IT-Sicherheit zu gewährleisten und ihre IT-Systeme am Stand der Technik auszurichten. In „Branchenspezifischen Sicherheitsstandards" (B3S) werden die Anforderungen dafür definiert.

Zudem hat das BSI einen **Anforderungskatalog** veröffentlicht, der die gemäß § 8a Absatz 1 BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) umzusetzenden Maßnahmen konkretisiert. Die Erfüllung dieser Standards müssen KRITIS-Betreiber alle zwei Jahre mithilfe entsprechender Formulare gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachweisen. Außerdem umfasst ein Mindestmaß an IT-Sicherheit die Benennung eines Sicherheitsbeauftragten sowie die unverzügliche Meldung von Störungen an das BSI.

Neu hinzu kommt mit dem IT-SiG 2.0 der Bereich der Entsorgung. Außerdem wird die neue Kategorie der „Infrastrukturen im besonderen öffentlichen Interesse" eingeführt, welche die Rüstungsindustrie, die Bereiche Kultur und Medien sowie Anlagen und Systeme umfassen, deren Beeinträchtigung zu Schäden bei Unternehmen aus dem Bereich der Prime Standards der Frankfurter Börse führen würden. Diese Kategorie zählt zwar nicht zu den kritischen Infrastrukturen, wird aber hinsichtlich der Verpflichtungen so behandelt.

DIE EINFÜHRUNG UND UMSETZUNG EINES UNTERNEHMENSWEITEN IT-SICHERHEITSKONZEPTS IST LANGWIERIG UND RESSOURCENINTENSIV. KRITIS-BETREIBER SOLLTEN ES DESWEGEN BEREITS JETZT AUF DEN WEG BRINGEN.

1. OPTIMIERTE ANGRIFFSERKENNUNG

KRITIS-Betreiber müssen mit Inkrafttreten des IT-SiG 2.0 eine Angriffserkennung umsetzen und damit sicherstellen, dass sie neben einer Anti-Viren-Lösung und einer Firewall zusätzlich ein System implementieren, welches automatisiert und in Echtzeit über Sicherheitsausfälle informiert. Für KRITIS-Betreiber kommt dazu etwa ein „Intrusion Detection/Prevention System“ (IDS/IPS) oder ein „Security Information and Event Management“ (SIEM) infrage. Dabei wird davon ausgegangen, dass relevante Daten über die IT-Sicherheit eines Unternehmens, einer Behörde oder einer Organisation an verschiedenen Stellen anfallen. Es ist jedoch ratsam, alle Daten zentral zu sammeln, da so vom üblichen Schema abweichende Muster besser zu erkennen sind. Tritt ein Sicherheitsvorfall ein, müssen Betreiber einer kritischen Infrastruktur das BSI anhand eines Meldeformulars unter anderem über Art, Dauer, mögliche Intention und eventuelle Auswirkungen informieren. Auch physische Schäden wie Zerstörung, Diebstahl, Manipulation oder Verlust (beispielsweise nach einem Einbruch) sind hierbei zu erfassen.

Ein Musterformular haben wir Ihnen in unserem Downloadbereich zur Verfügung gestellt.

2. REGELN FÜR HERSTELLER VON IT-PRODUKTEN

Neben den Betreibern kritischer Infrastrukturen müssen zukünftig auch Zulieferer und Hersteller von KRITIS-Kernkomponenten die Standards des BSI erfüllen und dies entsprechend nachweisen, um Schwachstellen in den Basiskomponenten weitgehend ausschließen zu können. Hierzu zählen unter anderem Hersteller von Hard- und Software-Produkten, die in den Systemen von kritischen Infrastrukturen zum Einsatz kommen. Somit sollen nur Komponenten verbaut werden, zu denen eine Vertrauenswürdigkeitsvereinbarung abgegeben wurde und die über ein freiwillig vergebenes IT-Sicherheitskennzeichen (vergeben vom BSI) verfügen. Auf diese Weise wird sichergestellt, dass die gesamte Zuliefererkette der KRITIS-Komponenten die geforderten Sicherheitskriterien erfüllt.

NEUE ANFORDERUNGEN AN BETREIBER KRITISCHER INFRASTRUKTUREN

Im Wesentlichen müssen sich KRITIS-Betreiber auf vier Neuerungen einstellen:

1. Eine Angriffserkennung muss eingeführt und
2. der Einsatz vertrauenswürdiger KRITIS-Komponenten nachgewiesen werden.
3. Außerdem sind eine drastische Erhöhung der Bußgelder sowie die
4. Ausdehnung der Befugnisse des BSI zu erwarten.

3. ERHÖHUNG VON BUSSGELDERN

Entsprechend der EU-DSGVO wird das bislang maximale Bußgeld (je Verstoß) gegen die Auflagen des IT-SiG 2.0 von 100.000 Euro auf 20.000.000 Euro oder vier Prozent des weltweiten Unternehmensumsatzes erhöht. Außerdem wird die Liste der Tatbestände erweitert, bei denen ein Bußgeld verhängt werden kann. Diese umfassen unter anderem die mangelnde Mitwirkung an der Wiederherstellung der Sicherheit oder der Funktionsfähigkeit eines betroffenen Systems. Außerdem wird die Pflicht der Hersteller zur Auskunftserteilung sowie die Erreichbarkeit der einzurichtenden Kontaktstelle sanktioniert.

4. ERWEITERTE BEFUGNISSE DES BSI

Das BSI kann in Zukunft bereits im Verdachtsfall eines unzureichenden Schutzes öffentlicher IT-Systeme von KRITIS-Betreibern eigenständig und ohne vorherige Ankündigung – im Rahmen von Krisenreaktionsplänen – Maßnahmen zur Aufspürung von Sicherheitslücken umsetzen. Wie ein Angreifer kann das BSI dann in die möglicherweise bedrohten Systeme eindringen, um die Betreiber über etwaige Gefahren zu informieren.

GANZHEITLICHE ANSÄTZE UND BETRACHTUNGSWEISEN RÜCKEN IN DEN FOKUS.

MIT EINEM IT-SICHERHEITSKONZEPT CYBERANGRIFFEN ZUVORKOMMEN

Die Verabschiedung des IT-SiG 2.0 ist zeitlich noch nicht absehbar. Aber auch nach der Veröffentlichung haben KRITIS-Betreiber eine Übergangsfrist, bis alle Anforderungen umgesetzt sein müssen. Die zeitlichen und personellen Ressourcen bei der Einführung eines IT-Sicherheitskonzepts sollten Betreiber kritischer Infrastrukturen jedoch nicht unterschätzen. Dabei ist ein IT-Sicherheitskonzept mit zeitlichem Vorlauf wirksamer als eines, das in letzter Minute auf den Weg gebracht wird. KRITIS-Betreiber sollten neben allen gesetzlichen Vorgaben vor allem aber in IT-Sicherheit investieren, bevor ein zerstörerischer Cyberangriff die Infrastruktur mit verheerenden Folgen lahmlegt und sie dann doch dazu zwingt, Investitionen zu tätigen und den Schaden zu beseitigen. Auch wenn der Referentenentwurf bisher noch zentrale Fragen offenlässt, verdeutlicht er einmal mehr die Bedeutung der IT-Sicherheit.

Dieser Artikel ist mit freundlicher Unterstützung von Marco Gräf, Teamleiter Vertrieb und Kommunikationsinfrastruktur bei der Q-SOFT GmbH, entstanden.

Sicher-Gebildet.de
Qualität bildet den Unterschied

SICHERHEITS-UNTERWEISUNGEN VIA E-LEARNING (24/7)

RECHTSSICHER + REVISIONSSICHER + ZERTIFIZIERT

www.Sicher-Gebildet.de

AUSZUG MESSETERMINE UND VERANSTALTUNGEN

Das Messejahr 2020 ist anders gelaufen als gedacht. Viele Anbieter haben auf innovative Konzepte zurückgegriffen, um Themen und Produkte in die Büros und Unternehmen zu tragen. Aber der Besuch einer Fachmesse, die Inspiration durch Gespräche und ausgestellte Produkte, die Präsentation fachlicher Neuheiten und vielversprechender Forschungsergebnisse ist doch noch etwas anderes.
Hoffen wir auf 2021!

2021

FEBRUAR

24. – 25.02. **SEC-IT // Hannover**
Der Treffpunkt für Security-Anwender und -Anbieter

APRIL

27. – 28.04. **VFS KONGRESS // Kassel**
Kreativ Innovativ – Künstliche Intelligenz für mehr Sicherheit?

MAI

10. – 11.05. **DEUTSCHER PRÄVENTIONSTAG // Köln**
Prävention orientiert! ... planen ... schulen ... austauschen ...

JUNI

14. – 19.06. **INTERSCHUTZ // Hannover**
Teams, Taktik, Technik – Schutz und Rettung vernetzt

23. – 24.06. **SICHERHEITSEXPO // München**
Sicherheitsfachmesse

OKTOBER

07. – 09.10. **FLORIAN // Dresden**
Fachmesse für Feuerwehr, Zivil- und Katastrophenschutz

NOVEMBER

10. – 11.11. **PROTECT // Leipzig**
Konferenz zum Schutz kritischer Infrastrukturen

DEZEMBER

08. – 09.12. **VDS BRANDSCHUTZTAGE // Köln**
Fachtagung und Begleitmesse

PLANEN SIE SCHON HEUTE IHR MESSEJAHR!

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.

FRAGEBOGEN

ONLINE-FRAGEBOGEN ZUM „KNOW-HOW-SCHUTZ“

Know-how und somit auch der Schutz von Wissen sind entscheidende Erfolgsfaktoren für die Wirtschaft. Doch wie gut Know-how-Schutz funktioniert, lässt sich in den meisten Fällen nur schwer messen. Doch eines steht fest: Nur, wenn angemessene Geheimhaltungsmaßnahmen ergriffen wurden, kann ein effektiver Know-how-Schutz funktionieren und die Innovationskraft und Wettbewerbsfähigkeit des eigenen Betriebs aufrechterhalten werden.

Die Firma „CMS Law“ hat einen kostenfreien Online-Fragebogen entwickelt, um sich einen Überblick zum Thema „Know-how-Schutz“ verschaffen zu können und dabei zu erfahren, wo man selbst in Bezug auf den Schutz der eigenen „Kronjuwelen“ steht und wie mit sensiblen Daten und Informationen im Unternehmen umgegangen wird. Nutzen Sie diese kostenfreie Möglichkeit, um ggf. erforderlichen Handlungsbedarf zu eruieren und Hintergrundinformationen sowie Anregungen zum Know-how-Schutz zu erhalten.

Link: www.know-how-protect.de

BUCHTIPP

NATO SPECIAL FORCES

Das Kommando-International Special Operations Magazine (K-ISOM) hat zum 70-jährigen Bestehen der NATO ein Buch veröffentlicht, welches den Wandel der NATO-Spezialkräfte vom reinen Verteidigungsbündnis hin zu einer militärisch-politischen Organisation, die die Sicherheit der Mitgliedstaaten wahren soll, beschreibt und insbesondere die neuen (künftigen) Herausforderungen thematisiert.

Auf 208 Seiten werden die Spezialkräfte der einzelnen Länder vorgestellt sowie die Einsätze, Konflikte und Herausforderungen der letzten 20 Jahre. Als relativ neue Themen wird insbesondere auf die hybride Kriegsführung, den Einsatz weiblicher Spezialkräfte und die beiden großen Themen der Gegenwart und Zukunft: Drohnen-Operator und Cybersecurity explizit eingegangen.

Mit dem Buch „Nato Special Forces“ ist ein Gesamtübersichtswerk entstanden, was den aktuellen Stand darstellt, Hintergründe erläutert und gegenwärtige Fragestellungen aufzeigt.
Neben diversen Spezialbüchern, die herausgebracht wurden, betreibt K-ISOM auch einen Merchandising Shop und bringt ein gleichnamiges Fachmagazin heraus.

E-Mail an: bestellung@k-isom.com

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

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.