AUSGABE 2

SICHERHEIT. DAS FACHMAGAZIN.

SICHERHEIT AUF DEN PUNKT GEBRACHT.

EXKLUSIV Seite 12

Kostenfreies E-Learning-Training zum Thema Datenschutz & Datensicherheit (inkl. EU-DSGVO)

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.

UNSERE THEMEN

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

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.*

E-PAPER

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

Ihre Vorteile:

› Ressourcenschonend durch nachhaltige Einsparungen beim Verbrauch von Papier, Treibstoff und CO_2

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

UNTERSTÜTZEN SIE MIT IHRER SICHERHEITS-STRATEGIE DIE FORTENTWICKLUNG DES UNTERNEHMENS

Die vielfältigen Gefahren- und Bedrohungslagen für Geschäftsbereiche fordern heutzutage von allen Unternehmen, das Thema „Sicherheit“ als Managementaufgabe zu begreifen. Daher sollte „Sicherheit“ als strategischer Partner der Führungs- und Leitungsebenen angesehen werden, indem vorausschauend sowie „Hand in Hand“ agiert wird.

Schutzanforderungen unterliegen ebenso einem stetigen Wandel wie die damit verbundenen Aufgaben und Maßnahmen. Eine neue Gefahren- und Bedrohungslage kann zu vollkommen veränderten und bisher eher weniger berücksichtigten Schadensszenarien führen, mit denen Sicherheitsverantwortliche umzugehen wissen müssen. Das Sicherheitsmanagement ist ein komplexer Prozess von materiellen, konzeptionellen und menschlichen Ressourcen, welches stets bauliche, (informations-) technische, personelle und organisatorische Sicherheitsmaßnahmen betrachtet.

SICHERHEITSRESSOURCEN VERSUS KOSTENSENKUNG

Nach dem wirtschaftlichen Credo eines Unternehmens wird es immer um Kostensenkung, effizientere Ressourcennutzung, schlankere Strukturen und das Outsourcing von einzelnen (Teil-) Bereichen gehen. Dies führt allerdings im Umkehrschluss sehr häufig zu immer stärker begrenzten Sicherheitsressourcen. Dem sollten Sie rechtzeitig entgegensteuern, indem Sie vorausschauend agieren und auf künftige Risiken und Gefährdungen frühzeitig hinweisen, z. B. bei der Erschließung neuer Märkte, der Planung von Bauprojekten, Unternehmensübernahmen/-integrationen, Vergabe/Einkauf von Fremddienstleistungen u. Ä. Der Ansatz eines gut strukturierten und auf alle Unternehmensbereiche ausgeweiteten Sicherheitsmanagements hilft Ihnen dabei, auch bei immer knapper werdenden Ressourcen die potentiellen Risiken und Gefährdungen rechtzeitig zu identifizieren, zu analysieren, zu bewerten und zu behandeln. Somit können Sie die Führungs- und Leitungsebenen nicht nur im Alltag, sondern auch in der konzeptionellen Phase von neuen Projekten adäquat unterstützen. Doch dies funktioniert nur, wenn es eine enge Verzahnung innerhalb der Abteilungen gibt, die mit Sicherheitsaufgaben im Unternehmen betraut sind, wie z. B. IT, Datenschutz, Compliance, Arbeitssicherheit etc.

Sie und Ihr Arbeitgeber sollten in der Lage sein, Sicherheitsrisiken stets kalkulier- und steuerbar zu halten. Wenn Sie in diesem Zusammenhang konkrete Argumente zur Abwehr von sicherheitsspezifischen Risiken und Gefährdungen für die Führungsetage bereithalten, wird man Sie als strategischer Partner wahrnehmen, dessen persönliches Credo eine sichere und nachhaltige Fortentwicklung des Unternehmens ist.

- Erschließung neuer Märkte
- Vergabe/Einkauf wichtiger Fremddienstleistungen
- Sicherheitsvorfälle
- (Neu-) Bauprojekte
- Unternehmensübernahmen/-integrationen
- Planung/Begleitung von Veranstaltungen und Messeauftritten

„NUR EIN GANZHEITLICHES SICHERHEITSMANAGEMENTSYSTEM KANN FÜHRUNGS- UND LEITUNGSEBENEN IN IHRER VERANTWORTUNG FÜR EINEN SICHEREN GESCHÄFTSBETRIEB UND DER DAMIT EINHERGEHENDEN FÜRSORGEPFLICHT DES ARBEITGEBERS UNTERSTÜTZEN.

EINE SICHERHEITSORGANISATION ALS INTEGRALEN BESTANDTEIL IM UNTERNEHMEN AUFBAUEN

„Sicherheit ist ein dynamischer Prozess, kein statischer Zustand!“ Demzufolge muss Sicherheit integrativ mit einem systematischen Ansatz und Vorgehen gesteuert werden, um strukturiert alle Themen- und Geschäftsbereiche abzudecken. Nur so lassen sich vorab definierte Schutzziele angemessen schützen. Um sich überhaupt zum Schutz des Unternehmens konkrete Gedanken machen zu können, benötigt es eine funktionierende Sicherheitsorganisation. Das Ziel dieser Sicherheitsorganisation – und dem damit verbundenen Aufbau eines Sicherheitsmanagementsystems – ist die Erlangung eines einheitlichen Sicherheitsniveaus und die Verankerung von Sicherheit in der Unternehmenskultur.

Ein funktionierendes und nachhaltiges Sicherheitsmanagementsystem muss in die existierenden Strukturen und Gegebenheiten der Organisation und Kultur eingebettet werden. Sicherheit lässt sich grundsätzlich nicht aufzwängen oder überstülpen, sie muss stets den individuellen Rahmenbedingungen und dem Kontext eines Unternehmens angepasst werden und in die Organisationsstruktur übernommen werden. Wichtig ist, dass sich die oberste Leitungsebene ihrer Verantwortung für (Unternehmens-) Sicherheit bewusst ist und hinter den Sicherheitszielen sowie den daraus resultierenden Sicherheitsmaßnahmen steht. Denn diese gewährleisten die Fortführung der Geschäftsprozesse, auch wenn insbesondere dieser Umstand vielen nicht auf Anhieb bewusst ist. Sicherheitsprozesse müssen von „oben“ initiiert, gesteuert und letztlich kontrolliert werden. Um dieser Aufgabe gerecht zu werden, ist die Benennung eines Sicherheitsverantwortlichen ein erster und unabdingbarer Schritt.

> DIE SICHERHEITSORGANISATION MUSS ALS FUNDAMENTALER BESTANDTEIL IM UNTERNEHMEN EINGEBUNDEN WERDEN. “

ERNENNUNG EINES SICHERHEITSVERANTWORTLICHEN

Sicherheit kann nicht in einem einzelnen Geschäftsbereich realisiert werden, sondern muss als integrativer Bestandteil aller unternehmerischen Prozesse betrachtet werden, damit der Werteschutz keine Lücken aufweist. Daher ist es unabdingbar, einen zentralen Ansprechpartner und Koordinator im Unternehmen zu definieren und diesen Funktionsträger mit entsprechenden Ressourcen auszustatten – sowohl personell mit entsprechenden Weisungsbefugnissen als auch monetär mit angemessenen finanziellen Möglichkeiten. Dem Sicherheitsverantwortlichen im Unternehmen (auch Corporate Security Officer, Sicherheitsbeauftragter, Leiter Corporate Security oder Sicherheitsmanager genannt) obliegt die konkrete Ausgestaltung der Sicherheitsorganisation im Unternehmen. Die Zuständigkeit erstreckt sich auf die Verantwortung für alle durch die oberste Leitungsebene definierten Themengebiete sowie die entsprechenden Schnittstellenkoordinationen und die Etablierung von Sicherheitsmaßnahmen mit nicht innerhalb der Organisationsstruktur integrierten Fachgebieten, wie z. B. IT, Datenschutz, Compliance, Arbeitssicherheit etc. sowie bereichsübergreifenden Prozessen, wie z. B. Mitarbeiterschulungen, Sicherheitsvorfallmanagement, Bewerberprüfungen/Einstellungsvorgaben etc. Hierzu werden klare Verantwortlichkeiten, Kompetenzen, Aufgaben sowie Dokumentations- und Berichterstattungsintervalle definiert.

Um den Stellenwert von „Sicherheit im Unternehmen“ abzubilden und dies auch tief in die Unternehmenskultur (Sensibilität gegenüber Sicherheitsrisiken, Eigeninitiative beim Umgang mit Sicherheitslücken, Schutz des unternehmerischen Know-hows, Umgang mit betriebsfremden Personen, Einhaltung von Sicherheitsmeldungen an die verantwortlichen Stellen im Unternehmen etc.) zu verankern, ist eine offizielle Ernennung und Integration des Sicherheitsverantwortlichen in die Aufbauorganisation des Unternehmens (Organigramm) erforderlich und dringend ratsam.

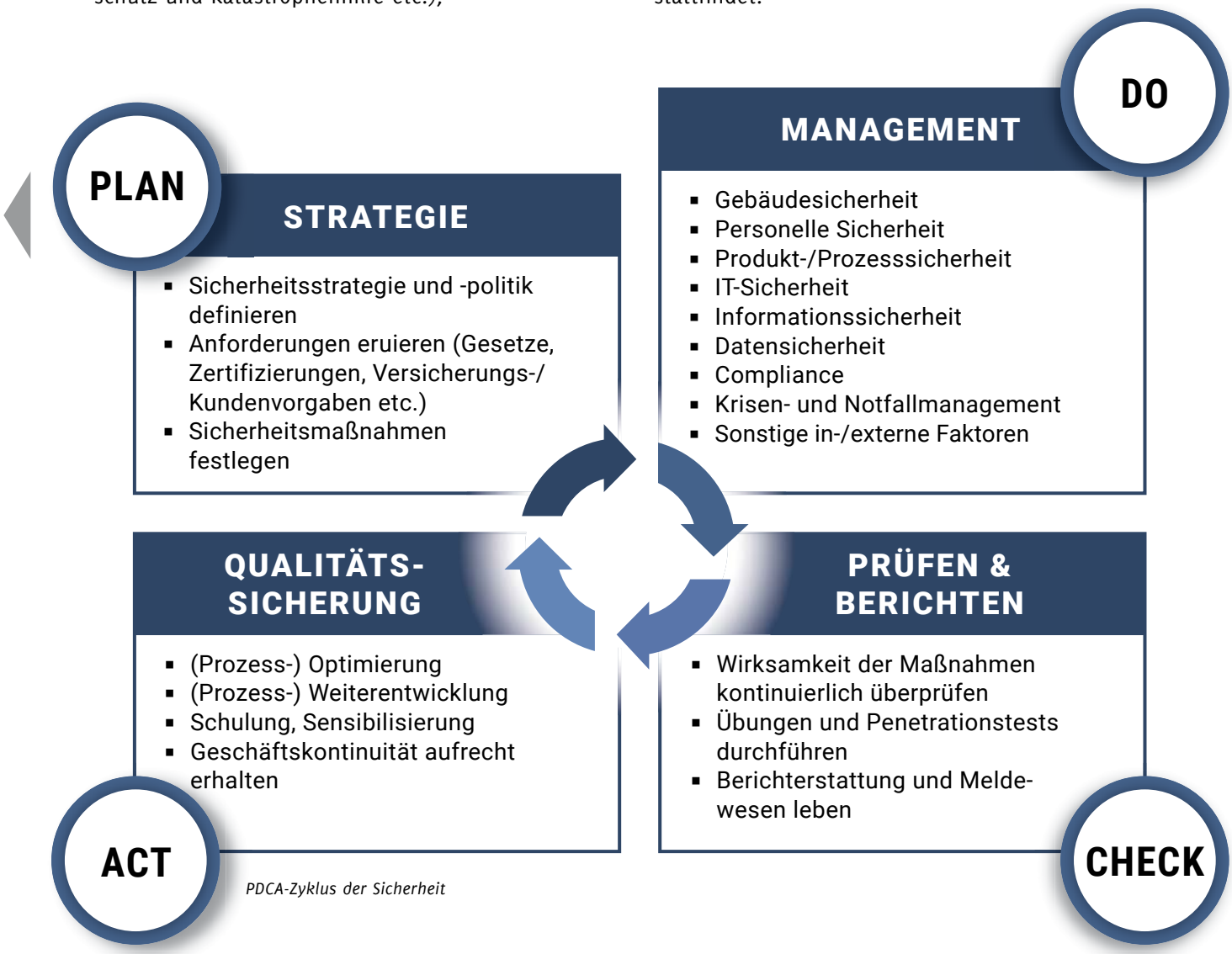
AUFGABEN EINER SICHERHEITSORGANISATION

Die Aufgaben einer Sicherheitsorganisation und somit eines Sicherheitsverantwortlichen unterliegen aufgrund von sich stets verändernden Risiko- und Bedrohungslagen oder etwaigen Sicherheitsvorkommnissen einem dynamischen Wandel.

Zu den Hauptaufgaben einer Sicherheitsorganisation zählen:

- das Erstellen einer Sicherheitsrichtlinie und Sicherheitsstrategie,
- die Beratung der Führungs- und Leitungsebenen in Sicherheitsfragen,
- das Erstellen von regelmäßigen Sicherheitsreports für die Führungs- und Leitungsebenen,
- die Leitung von spezialisierten und technischen Sicherheitsdienstleistungen und Dienstleistern,
- die Weiterentwicklung der Sicherheit im Unternehmen (Aufbau eines in- und externen Netzwerks),
- das Vorleben von Sicherheit und der Integration im Unternehmen (Security Awareness/Marketing),
- die Aktualisierung stetiger Sicherheitslagebilder unter Einbeziehung verschiedenster Quellen (Landespolizei, Bundeskriminalamt, Verfassungsschutz, Bundesamt für Informationssicherheit, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe etc.),
- der kontinuierliche partnerschaftliche Austausch mit anderen Fachbereichen, Prozessverantwortlichen und Schnittstellen im Unternehmen,
- die interne Unterstützungsleistung bei diversen Zertifizierungsprozessen (AEO, C-TPAT, bekannter Versender, BSI IT-Grundschutz, ISO 27001, ISO 28000, Food Defense etc.),
- das Erkennen, Bewerten und Eindämmen sicherheitsrelevanter Risiken und Gefährdungen sowie
- die Definition von Maßnahmen zur Behandlung von Sicherheitsrisiken und
- das Durchführen von regelmäßigen Sicherheitstests und -audits.

Diese Hauptaufgaben müssen dann in allen für die Sicherheitsorganisation definierten Themengebieten geleistet werden. Dies erfolgt automatisch nach dem sog. PDCA-Zyklus, bei dem jede definierte Strategie bzw. Maßnahme hinterfragt wird und somit eine kontinuierliche Verbesserung und permanente Weiterentwicklung stattfindet.



PDCA-Zyklus der Sicherheit

Die Sicherheitsorganisation übernimmt zusätzlich noch weitere unterstützende Funktionen für andere Geschäftsbereiche, wie z. B. die strategische Steuerung bei sicherheitsrelevanten Fragestellungen (z. B. der Erschließung neuer Märkte, der Planung von (Neu-) Bauprojekten, etwaigen Unternehmensübernahmen/-integrationen, der Vergabe und dem Einkauf wichtiger Fremddienstleistungen, der (sicheren) Planung und Begleitung von Veranstaltungen und Messeauftritten etc.). Dazu zählt auch die entsprechende Unterstützung der Geschäftsbereiche in der Anwendung und im Umgang mit Sicherheitsvorkehrungen/-maßnahmen. Nicht nur neue Rahmenbedingungen z. B. aufgrund von veränderten Risiko- und Bedrohungslagen oder etwaigen Sicherheitsvorkommnissen, auch operationelle Fragestellungen und künftige unternehmerische Herausforderungen sollten in regelmäßigen Sitzungen aller Fachbereiche mit den jeweiligen Schnittstellenkoordinatoren und ggf. weiteren fachkundigen Personen stattfinden. Hierbei können aktuelle Themen, Herausforderungen und/oder Optimierungen gemeinsam besprochen und angegangen werden.

IN 10 SCHRITTEN EINE SICHERHEITSORGANISATION AUFBAUEN

Aufbau einer Sicherheitsorganisation und somit eines erfolgreichen und wirksamen Sicherheitsmanagementsystems:

1. Sicherheitsverantwortlichen benennen
2. Risiko- und Gefährdungsanalyse erstellen, Schutzziele definieren
3. Sicherheitsstrategie entwickeln und an den Schutzzielen des Unternehmens ausrichten
4. Sicherheitsleitlinie/Sicherheitsrichtlinie erstellen (Schutzziele, Definitionen, Verantwortlichkeiten, Informations- und Berichtspflichten, Kontrollmaßnahmen etc.)
5. Sicherheitsorganisation aufbauen (Ansprechpartner, Zuständigkeiten, Verantwortlichkeiten, Aufgabenbereiche, Schnittstellen etc.) und mit Ressourcen ausstatten (personell und finanziell)
6. Sicherheitskonzept erstellen und konkrete Sicherheitsvorkehrungen/-maßnahmen umsetzen
7. Überprüfung der Sicherheitsvorkehrungen/-maßnahmen anhand des PDCA-Zyklus betreiben
8. Regelmäßige fachübergreifende Besprechungen und Berichterstattung an die oberste Leitungsebene
9. Qualitätssicherung betreiben (Audits, Penetrations- und Schwachstellentests, Test von sicherheitstechnischen Komponenten, Krisen- und Notfallmanagementübungen etc.)
10. Anpassung von Sicherheitskonzepten und ggf. der Sicherheitsorganisation bei sich verändernden Rahmenbedingungen

Mit der Einbindung der Sicherheitsorganisation als fundamentaler Bestandteil können die komplexen Prozesse der Sicherheit und die damit einhergehenden materiellen, konzeptionellen und menschlichen Ressourcen ideal gesteuert werden. Nur dadurch ist eine vorausschauende Planung von Sicherheitsmaßnahmen und -vorkehrungen auf strategischer und organisatorischer Ebene für alle Bereiche und Prozesse möglich.

KRISENSTABSARBEIT – WICHTIGE AUFGABEN IM EREIGNISFALL

Außergewöhnliche unternehmenskritische Ereignisse können jederzeit und in unterschiedlichster Ausprägung eintreten. Beim Eintritt eines kritischen Ereignisses können nicht nur technische Anlagen und die Funktionsfähigkeit des Unternehmens bedroht sein, sondern ggf. auch Menschenleben. Daher ist es essentiell, dass sich ein Krisenstab seiner Aufgaben und Verantwortung im Ereignisfall stets bewusst ist, um die Schadens- und Ereignisbewältigung angemessen und strukturiert anzugehen.

> EIN KRISENSTAB PLANT, KOORDINIERT, VERANLASST UND ÜBERWACHT ALLE AKTIVITÄTEN DER SCHADENS- UND EREIGNISBEWÄLTIGUNG UND STEUERT DIE BEREITSTELLUNG RELEVANTER INFORMATIONEN UND RESSOURCEN.

Der Krisenstab ist eine besondere (provisorisch zusammengesetzte) Gruppe von Vertretern unterschiedlichster Bereiche innerhalb der Aufbauorganisation in Not- und Krisenfällen, die aufgrund von besonderen Ereignissen situationsbedingt einberufen wird. Dieses zentrale Krisenreaktionsinstrument wird nur dann eingesetzt, wenn ein Vorfall hinreichend gravierend erscheint, um diese besondere vom Alltag losgelöste Aufbauorganisation einzuberufen.

KRISENSTABSMITGLIEDER DEFINIEREN

Vertreter im Krisenstab sollten stressresistente Personen sein, die aus den von einer Krise betroffenen sowie an deren Behebung beteiligten Bereichen stammen und über die notwendige Expertise verfügen, wie z. B. Vertreter aus

- Betriebsleitung, Geschäftsführung, Vorstand,
- Niederlassungsleitung,
- Facility Management, Haustechnik,
- Sicherheitsabteilung,
- IT, Datenschutz, Compliance, Arbeitssicherheit etc.,
- Rechtsabteilung,
- Personalabteilung,
- Pressestelle, Kommunikationsabteilung, Öffentlichkeitsarbeit und
- ggf. weitere für die Ereignisbewältigung benötigte Fachstellen.

Im Anschluss der Ereignisbewältigung kehren die Mitglieder des Krisenstabs wieder in ihre ursprüngliche Rollen- und Aufgabenverteilung im Unternehmen zurück.

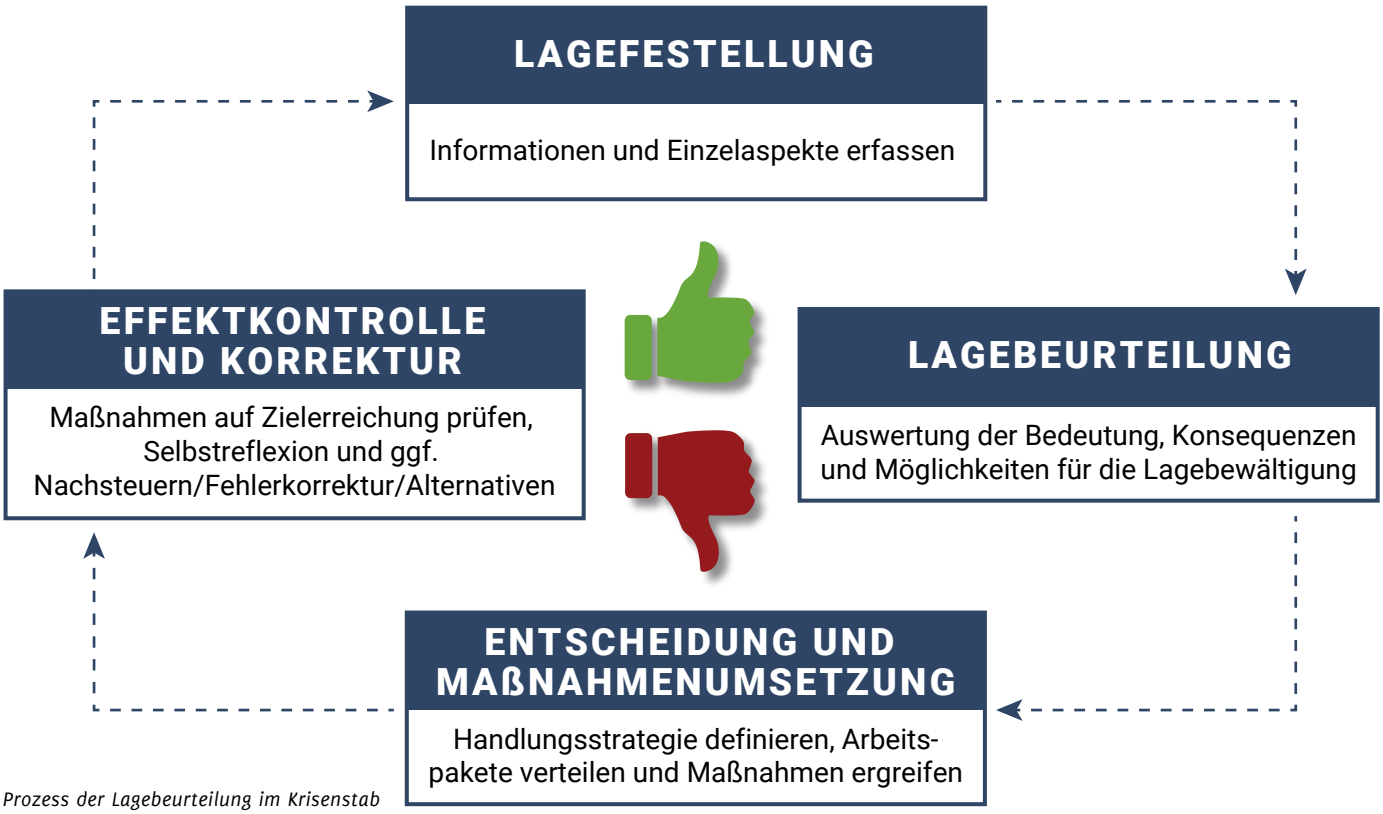
Die personelle Stärke und Zusammensetzung des Krisenstabs ist nicht in jedem Fall identisch, sondern hängt maßgeblich vom Ereignis ab (IT-Ausfall, Brand, Gefahrstoffaustritt, Wasserschaden, Produktionsanlagenausfall, Arbeitsunfall mit tödlichem Ausgang etc.). Alle Fachberater sowie deren individuelle ereignisspezifische Funktion und Verantwortlichkeit im Krisenstab sollten bereits im Vorfeld in entsprechenden Alarmierungsplänen für alle Tages- und Nachtzeiten inkl. Aufgabenzuweisung und Vertreterregelungen definiert werden. Der Krisenstab sollte als Kooperationseinheit agieren, da Hierarchiestrukturen während der Krisenstabsarbeit stark abgeflacht sind, was u. a. eine offene Kommunikation untereinander fördert. Idealerweise unter einem führungserfahrenen und allein verantwortlichen Krisenstabsleiter. Nur dadurch ist sichergestellt, dass auch unter hohem Druck Entscheidungen schnell getroffen und mit vereinten Kräften umgesetzt werden können. Sollte diese Funktion nicht von der obersten Leitungsebene gestellt werden, ist es wichtig, dass der Krisenstabsleiter die notwendigen Entscheidungskompetenzen innehat.

AUFGABEN UND ARBEITSWEISE DES KRISENSTABS

Der Krisenstab tritt zusammen, um die Lage aus den unterschiedlichsten Perspektiven zu beurteilen und Sofortmaßnahmen einzuleiten. Das Ziel der Krisenstabsarbeit stellt hierbei die Rettung von Menschenleben sowie den Schutz von Umwelt und Sachgütern dar. Das unternehmerische Ziel, also die zeitnahe Fortführung der Geschäftstätigkeit, sollte dennoch nicht aus den Augen verloren werden.

Die Aufgabe der Krisenstabsmitglieder besteht darin, den Krisenstabsleiter bei der Beurteilung der Lage zu beraten, Entscheidungen vorzubereiten und die Ausführungen zu koordinieren und zu überwachen. Sie stellen bildlich gesprochen „Hand und Kopf des Entscheiders“ dar. Dies geschieht mit Hilfe eines sog. Lagebeurteilungsprozesses. Jede Information wird dabei systematisch erfasst, die Bedeutung für die Lage eruiert und daraus logische Schlüsse gezogen, um anschließend konkrete Maßnahmen zu definieren, deren Erfolg wiederum kontrolliert werden muss. Dieser Prozess sollte stetig und bis zum Ende durchdacht und umgesetzt werden, damit keine Einzelaspekte ins Leere laufen und alle Maßnahmen auf Plausibilität geprüft werden können.

IN UNSEREM DOWNLOADBEREICH HABEN WIR IHNEN EINE „CHECKLISTE FÜR DIE KRISENSTABSARBEIT“ THEMATISCH GEGLIEDERT ZUR VERFÜGUNG GESTELLT.



Prozess der Lagebeurteilung im Krisenstab

Die getroffenen Maßnahmen beziehen sich in der ersten Ereignisphase vorwiegend auf den Kontakt zu den Blaulichtorganisationen, die Informationsbeschaffung, die Bereitstellung von Hilfsmitteln und Räumlichkeiten sowie die interne und externe (Krisen-) Kommunikation. Erst im weiteren Verlauf kommen die Fortführung und der Wiederanlauf der Geschäftsprozesse, als sog. Business Continuity Management (betriebliches Kontinuitätsmanagement) bezeichnet, hinzu.

EINE SINNVOLLE PERSONELLE ZUSAMMENSETZUNG, EIN PROFESSIONELLES INFORMATIONS- UND WEISUNGSMANAGEMENT SOWIE EINE SACH- UND FACHGERECHTE ENTSCHEIDUNGSFINDUNG SIND DAS A UND O DER KRISENSTABSARBEIT.

Zu den wesentlichen Aufgaben der Krisenstabsarbeit zählt es:

- sich umfassend über die aktuelle Lage zu informieren und zusätzliche Lageinformationen als (Gesamt-) Lagebild kontinuierlich fortzuschreiben
- den Informationsfluss in den Krisenstab hinein und aus dem Krisenstab heraus zu strukturieren
- vorbereitete Notfallpläne auszuführen/anzuweisen sowie weitere Maßnahmen zu veranlassen, zu koordinieren und zu überwachen
- aktuelle Informationen für Entscheidungsträger innerhalb des Unternehmens und der Blaulichtorganisationen bereitzuhalten
- die interne und externe (Krisen-) Kommunikation zu koordinieren bzw. zu übernehmen
- die Entsendung von Verbindungspersonen zu koordinieren und zu veranlassen
- ggf. benötigte Betreuungsflächen für Blaulichtorganisationen bereitzustellen
- eine gerichtsfeste Dokumentation der Krisenstabsarbeit (Beteiligte, getroffene Entscheidungen etc.) zu erstellen

Auch die adäquate Nachbereitung einer bewältigten Krise sollte dringend bedacht werden. Alle getroffenen Entscheidungen und durchgeführten Maßnahmen sowie etwaige Defizite und aufgetretene Problemstellungen während der Krisenstabsarbeit sollten im Nachgang detailliert betrachtet und ausgewertet werden, um für zukünftige Ereignisse noch besser aufgestellt zu sein.

Kein Unternehmen sollte sich von einem unternehmenskritischen Ereignisfall überraschen oder gar überrumpeln lassen. Für den Umgang mit außergewöhnlichen Lagen/Situationen ist es stets besser, bereits im Vorfeld eine entsprechende Aufbau- und Ablauforganisation inkl. Aufgabenverteilung definiert zu haben, die unterschiedlichsten (Notfall-/Krisen-) Szenarien in regelmäßigen Abständen zu betrachten und die Krisenstabsarbeit im Idealfall auch regelmäßig anhand von Krisenstabsübungen zu trainieren. Nur dadurch ist der Krisenstab bestmöglich auf die Lagebeurteilung und Bewältigung eines Schadensereignisses vorbereitet.

WICHTIG IST, DASS DER KRISENSTAB IN UNTERSCHIEDLICHEN KONSTELLATIONEN MÖGLICHE SCHADENSEREIGNISSE PERIODISCH ZU VERSCHIEDENEN TAGES- UND NACHTZEITEN ÜBT, UM DADURCH SEINE HANDLUNGSFÄHIGKEIT AUCH UNTER ERSCHWERTEN/VERÄNDERTEN RAHMENBEDINGUNGEN ZU ÜBERPRÜFEN.

WAS SIE IM HINBLICK AUF DIE EU-DATENSCHUTZ-GRUNDVERORDNUNG BEACHTEN MÜSSEN

Die technologischen Fortschritte der vergangenen Jahrzehnte haben eine Überarbeitung der Datenschutzrichtlinien auf EU-Ebene unumgänglich gemacht. Heutzutage müssen z. B. Themen rund um Industrie 4.0, Big Data, Künstliche Intelligenz und Robotik in die Gesamtbetrachtung mit einfließen. Ziel der neuen EU-Datenschutz-Grundverordnung (EU-DSGVO) ist es, den Umgang mit Daten europaweit einheitlich zu gestalten. Welche Neuerungen und Änderungen ggf. Auswirkungen auf deutsche Unternehmen haben und was Sie in diesem Zusammenhang tun sollten, um den neuen Vorgaben der Datenschutzpraxis gerecht zu werden, erläutern wir Ihnen in diesem Artikel.

Die am 25. Mai 2018 in Kraft getretene EU-DSGVO (herausgegeben im Jahr 2016 mit einer 2-jährigen Übergangsfrist) löst die aktuell gültige Datenschutzrichtline aus dem Jahr 1995 ab und ist zu unmittelbar geltendem Recht in allen Mitgliedstaaten der EU geworden. Die Bundesregierung hat mit dem Bundesdatenschutzgesetz neu (BDSG neu) darauf reagiert und darin die Möglichkeit der Präzisierung oder Ergänzung von Regelungen (Öffnungsklausel) wahrgenommen und festgeschrieben.

Für jeden Verbraucher und Betroffenen von Datenerhebungen sind es erst einmal positive Neuerungen, denn der Schutz der Erhebung personenbezogener Daten wird erheblich gestärkt.

WELCHE UNTERNEHMEN MÜSSEN SICH ANGESPROCHEN FÜHLEN?

Relevant ist die neue EU-DSGVO für alle, die Mitarbeiter beschäftigen, Kunden, Lieferanten oder Webseitenbesucher haben und/oder einen Onlinehandel betreiben – also quasi für die überwiegende Mehrzahl von Unternehmen. Neuerungen kommen insbesondere in den Bereichen Arbeitnehmerdatenschutz, Webseitenbetrieb sowie Onlinehandel zum Tragen.

Leider fehlen in vielen Unternehmen grundlegende organisatorische Voraussetzungen für den Datenschutz. Mehr als 50 % der Unternehmen haben z. B. kein sog. Verfahrensverzeichnis, in welchem die internen (Datenschutz-) Prozesse für die Verarbeitung personenbezogener Daten dokumentiert sind. Aber kein Grund zur Panik: Unternehmen, die sich bisher an die Vorgaben aus dem Bundesdatenschutzgesetz (BDSG) gehalten haben, haben auch zukünftig nicht viel zu befürchten.

WELCHE RISIKEN KÖNNEN ENTSTEHEN?

Die Abmahnung von Verstößen gegen den Datenschutz ist in Deutschland ein „lukratives Geschäft“ und die hohen Bußgelder – von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Unternehmensumsatzes des vorangegangenen Geschäftsjahres – verleiten künftig umso mehr dazu, genauer hinzuschauen. Daher sollte sich jedes Unternehmen – gleich welcher Branche und Größenordnung – mit der neuen EU-DSGVO auseinandersetzen und adäquate Maßnahmen einleiten und weiterentwickeln, um den Änderungen gerecht zu werden und am Ende auch etwaigen Bußgeldzahlungen zu entgehen.

BENENNUNG EINES DATENSCHUTZ-BEAUFTRAGTEN IM UNTERNEHMEN

Bisher kam dem Datenschutzbeauftragten lediglich die Aufgabe der Datenkonformität zu. Künftig müssen die Maßnahmen der Datenschutzstrategie aber auch kontinuierlich überwacht werden. Dies hat ein wachsendes Aufgabenfeld zur Folge, was jedoch wiederum zu einer Aufwertung der Position des Datenschutzbeauftragten führen kann.

> „EINE REPRÄSENTATIVE UMFRAGE DES DIGITALVERBANDES BITKOM HAT ERGEBEN, DASS SICH ERST 1/3 DER DEUTSCHEN UNTERNEHMEN MIT DEM THEMA EU-DSGVO AUSEINANDERGESETZT HAT.

Alle öffentlichen Stellen und alle Unternehmen, deren Kerntätigkeit sich auf die Handhabung von Personendaten bezieht, müssen einen Datenschutzbeauftragten benennen, sofern dies nicht bereits in der Vergangenheit geschehen ist. Wenn in einem Betrieb mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, muss ebenfalls ein Datenschutzbeauftragter benannt werden.

DIE BEWAHRUNG DES IM GRUNDRECHT FESTGELEGTEN RECHTS AUF INFORMATIONELLE SELBSTBESTIMMUNG SOLL DER DATENSCHUTZ BEWERKSTELLIGEN.

DIE GRUNDLAGE DER EU-DSGVO SIND DIE FOLGENDEN 5 DATENSCHUTZGRUNDPRINZIPIEN

Diese Grundprinzipien bilden die Grundlage für alle Anforderungen an die Datensicherheit im Unternehmen.

1. VERBOT MIT ERLAUBNISVORBEHALT: Jede Verarbeitung personenbezogener Daten bzw. Daten mit Personenbezug ist grundsätzlich verboten, es sei denn, sie ist erlaubt.
2. ZWECKBINDUNG: Zu Beginn der Erhebung von Daten müssen die Zwecke ausformuliert und die zukünftige Verwendung der Daten dokumentiert werden.

   Ein Beispiel: Vertragsdaten, z. B. durch einen Kaufvertrag, dürfen nicht für Werbezwecke verwendet werden, da dies ein anderer Zweck ist. Nachträgliche Zweckänderungen sind nur unter bestimmten Voraussetzungen zulässig.
3. DATENMINIMIERUNG: Unternehmen dürfen so wenig wie möglich und so viel wie nötig an Daten erheben. Datensammlung ist nur für die Ausführung des Erhebungszwecks erlaubt.
4. TRANSPARENZ: Es muss verständliche Datenschutzerklärungen geben. Die Nachvollziehbarkeit der Datenerhebung und Verwendung durch die Unternehmen muss auf Anfrage mitgeteilt werden.
5. VERTRAULICHKEIT: Es müssen angemessene technische und organisatorische Schutzmaßnahmen getroffen werden, um einem Datendiebstahl, einer unbefugten Verarbeitung oder Veränderung von Daten sowie der Vernichtung von Daten vorzubeugen.

DATENSCHUTZ ≠ DATENSICHERHEIT
DATENSCHUTZ IST DER SCHUTZ PERSONENBEZOGENER DATEN ALS TEILBEREICH DER DATENSICHERHEIT, DIE DER SICHERUNG JEDWEDER DATEN DIENT.

WOMIT SOLLTE MAN BEGINNEN?

Vielleicht kennen Sie ja den Spruch „Einen Elefanten verspeist man häppchenweise“. Als erstes sollte das vorhandene Datenmaterial klassifiziert werden. Welche Art von Daten, insbesondere personenbezogene Daten, werden wo im Unternehmen vorgehalten? Erst dann können Sie sich explizit mit den rechtlichen Vorgaben befassen. Bei der Bearbeitung dieser Thematik sollte die oberste Leitungsebene stetig und kontinuierlich informiert werden.

ZUSAMMENFASSUNG DER ALLGEMEINEN DATENSICHERHEIT AUS DER EU-DSGVO

Die folgenden Punkte sind Gegenstand der neuen EU-DSGVO, mit denen Sie sich vertraut machen sollten, um Ihre neue Datensicherheitsstrategie zu definieren. Hinterfragen Sie hierzu stets alle Arbeits-, Datenverarbeitungs- und organisatorischen Prozesse sowie Verträge im Unternehmen.

DATENSCHUTZ-FOLGEABSCHÄTZUNG: Unternehmen sind verpflichtet, Risikoabschätzungen in Bezug auf die Datenverarbeitung und die Betroffenenrechte vorzunehmen. Sie müssen außerdem festhalten, welche Schutzmaßnahmen zur Risikominimierung unternommen werden. Die Datenschutz-Folgeabschätzung gilt auch für den Einsatz neuer Technologien.

MELDEPFLICHTEN: Datenpannen, Sicherheitsvorfälle und Datenschutzverstöße müssen innerhalb von 72 Stunden nach Bekanntwerden an die zuständige Aufsichtsbehörde und den Betroffenen selbst gemeldet werden, wenn dies zu einem (hohen) Risiko führt. Auch an Inhalt und Dokumentation dieser Meldung werden Anforderungen gestellt. Wichtig: Die entsprechende Aufsichtsbehörde befindet sich in dem Land/Bundesland, in welchem das Unternehmen seine wichtigsten Entscheidungen zur Datenverarbeitung trifft.

ARBEITNEHMERDATEN: Auf den Prüfstand kommt auch, wie ein Unternehmen die Daten seiner Arbeitnehmer im Hinblick auf die 5 Datenschutzgrundprinzipien bearbeitet (siehe Seite 11).

VERANTWORTLICHKEIT UND BUSSGELDER: Grundsätzlich gilt die Umkehr der Beweislast bei Verstößen. Unternehmen müssen also selbst nachweisen, dass sie ihrer Datenschutzverpflichtung nachgekommen sind.

BEACHTEN SIE UNBEDINGT DIE ÄNDERUNGEN ZU DOKUMENTATIONSPFLICHTEN, ERLAUBNISGRUNDLAGEN, SPEICHERUNG, AUSKUNFTSRECHTEN UND ZUM RECHT AUF LÖSCHUNG VON DATEN.

Dies klingt sehr komplex, aber es bedeutet im Grunde lediglich eine explizite Hinterfragung diverser Datenverarbeitungsprozesse im Unternehmen. Neben den Abteilungen, die dieses Thema bearbeiten, sind die Auswirkungen natürlich für das gesamte Unternehmen relevant.

Stecken Sie nicht den Kopf in den Sand! Setzen Sie sich gemeinsam mit ihrem Datenschutzbeauftragten, der Compliance- und Rechtsabteilung sowie der IT-Abteilung mit dem Thema auseinander, um so den neuen Vorgaben gerecht zu werden.

BESONDERHEITEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

DOKUMENTATIONSPFLICHT: Unternehmen sind verpflichtet, die umgesetzten Datenschutzstrategien durch eine hausinterne Dokumentation zu belegen (Rechenschaftspflicht von Unternehmen – Accountability). Aufsichtsbehörden können jederzeit die Vorlage eines entsprechenden Verzeichnisses verlangen (→ welche Daten werden zu welchem Zweck erhoben, auf welche Weise gespeichert und wann wieder gelöscht?).

PRIVACY BY DESIGN: Unternehmen müssen bereits beim (technischen) Aufbau der Arbeitsabläufe mit Personenbezug den Datenschutz berücksichtigen. Produkte und Prozesse sollten daher stets so konzipiert sein, dass sie mit möglichst wenig personenbezogenen Daten auskommen.

PRIVACY BY DEFAULT: Bei technischen Geräten muss grundsätzlich die datenschutzfreundlichste Variante voreingestellt sein. Somit müssen Verbraucher keine komplizierten Beschränkungen der Datenverarbeitung erwirken.

EINWILLIGUNG: Individuen müssen der Nutzung ihrer persönlichen Daten in den meisten Fällen durch aktive Bestätigung ausdrücklich zustimmen (Anklicken oder Unterschreiben). Die Einwilligungserklärung muss verständlich formuliert und grundsätzlich widerrufbar sein.

LÖSCHUNG VON DATEN: Erlischt die Verarbeitungsbefugnis aufgrund des fehlenden Zwecks (weil die Einwilligung widerrufen oder der Vertrag erfüllt wurde), müssen die Daten gelöscht werden.

UM SIE DABEI TATKRÄFTIG ZU UNTERSTÜTZEN, HABEN WIR IHNEN ONLINE DIVERSE HILFESTELLUNGEN ZUSAMMENGESTELLT.

Leider gibt es bei diesem Thema keine Musterlösung, da jedes Unternehmen durch sein individuelles Geschäftsmodell eigene, unterschiedliche Datenverarbeitungsprozesse durchführt.

VORGABEN, DIE JEDES UNTERNEHMEN BERÜCKSICHTIGEN SOLLTE:

- ☐ Benennen Sie einen Datenschutz-beauftragten (wenn erforderlich)
- ☐ Passen Sie alle Datenschutz-erklärungen (Informationspflicht) an die neuen Regelungen an
- ☐ Prüfen Sie die Einwilligungserklärung zur Datennutzung (aktive Bestätigung)
- ☐ Beachten Sie das Kopplungsverbot (Freiwilligkeit der Datennutzung)
- ☐ Passen Sie Auftragsverarbeitungen an die Änderungen an (Haftung, Dokumentation)
- ☐ Etablieren Sie Dokumentationsprozesse (Dokumentationspflicht) für den Umgang mit personenbezogenen Daten
- ☐ Erstellen Sie ein Verzeichnis der Verarbeitungs-tätigkeiten/Datenflüsse in gängigen und online übertragbaren Formaten (bzgl. Auskunftsgesuch)
- ☐ Prüfen Sie die technischen Schutzvorkehrungen (Krypto-Konzept, Anonymisierung, Pseudonymisierung etc.) und ein entsprechendes Backup mit der Technik- und IT-Abteilung sowie dem Datenschutzbeauftragten
- ☐ Passen Sie Ihre Betriebsvereinbarungen und ggf. diverse andere Unterlagen/Anweisungen an die neuen Vorgaben der EU-DSGVO an
- ☐ Kanalisieren Sie die Kommunikationsrouten für Kundenanfragen zum Datenschutz insbesondere bei Widersprüchen zur Datennutzung
- ☐ Klären Sie mit externen Dienstleistern, die ggf. personenbezogene Daten für Sie verwalten, ob die EU-DSGVO bei diesen outgesourcten Tätigkeiten Anwendung findet
- ☐ Etablieren Sie einen Prozess bei Datenpannen, Sicherheitsvorfällen und Datenschutzverstößen
- ☐ Schulen Sie Ihre Mitarbeiter zielgruppengerecht im Hinblick auf die neuen Prozesse
- ☐ Behalten Sie stets den Überblick über Neuerungen, Gesetzesänderungen und Fortbildungsmöglichkeiten

MELDUNG VON IT-STÖRUNGEN: EFFEKTIVES VERFAHREN ZUR PRAKTISCHEN ANWENDUNG

Ausfälle der Informations- und Kommunikationstechnik können je nach Unternehmensbranche gravierende oder teils existenzbedrohende Folgeschäden für den Geschäftsbetrieb mit sich bringen. Doch wie klassifiziert man derartige Störungen und welche „internen Störungen“ sollten ggf. gemeldet werden?

Globale Netzwerke und Lieferketten sowie ineinandergreifende Produktionsprozesse machen uns enorm abhängig von einem störungsfreien Betrieb. Störungen können unterschiedlichste Ursachen haben, z. B. durch Beeinträchtigungen der Stromversorgung, Hardware- oder Softwarefehler oder aber Hackerangriffe, Sabotageakte oder anderweitige kriminelle Einwirkungen.

MELDEVERPFLICHTUNGEN VON IT-STÖRUNGEN

Daher ist es umso wichtiger, dass die Informationen von Angriffen Dritter mit kriminellem Hintergrund zusammengeführt und allen zugänglich gemacht werden. Denn mit derartigen Informationen hat jedes Unternehmen die Möglichkeit, seine IT-Systeme gegenüber den neuesten bekanntgewordenen Bedrohungen zu schützen und ggf. systemseitig nachzurüsten. Doch aus Angst vor einer Verbreitung werden IT-Störungen oftmals totgeschwiegen oder vertuscht.

Für deutsche Unternehmen gibt es keine gesetzliche Verpflichtung zur Meldung von IT-Störungen. Lediglich das neue IT-Sicherheitsgesetz verpflichtet Betreiber Kritischer Infrastrukturen (KRITIS) zur Meldung von außergewöhnlichen Störungen und Ausfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI). Mit dem Meldeformular des BSI oder auch bei der Meldestelle der Allianz für Cyber-Sicherheit können Betroffene freiwillige und anonymisierte Meldungen abgeben. Dies ist insbesondere unter dem Kontext gewünscht und auch sinnvoll, dass jede Meldung einen Beitrag zum IT-Lagebild liefert und somit in aktuelle Warnmeldungen einfließen kann.

DAS ENTSPRECHENDE MELDEFORMULAR FINDEN SIE IM DOWNLOADBEREICH ZU DIESER AUSGABE.

ARTEN VON IT-STÖRUNGEN SINNVOLL EINTEILEN

Das BSI teilt IT-Störungen in 3 Kategorien der Beeinträchtigung ein, an denen auch Sie sich im Unternehmen orientieren können.

Meldekriterien für IT-Störungen nach BSI

GEWÖHNLICHE IT-STÖRUNGEN

- SPAM
- Phishing
- Schadprogramme
- Technische Defekte
- Bereits bekannte Sicherheitslücken

AUSSERGEWÖHNLICHE IT-STÖRUNGEN

- Gezielte IT-Angriffe
- Spear Phishing (gezielter E-Mail Betrug)
- Unbekannte Schadprogramme
- Unerwartete technische Defekte
- Neue Sicherheitslücken
- Neue Angriffswege
- APT-Angriffe (Fremde im Firmennetzwerk)
- DOS-Angriffe (Überlastung)

Beispiele von IT-Störungen

Als gewöhnliche Störungen bezeichnet das BSI Störungen, die mit technischen und organisatorischen Maßnahmen nach dem heutigen technischen Standard abgewehrt werden können, ohne nennenswerte Probleme zu verursachen oder bei denen kein erhöhter Ressourcenaufwand von Nöten ist.

Außergewöhnliche Störungen sind demnach IT-Störungen, die nicht mit den gängigen Techniken abgewehrt wurden, sondern mit erheblichem Ressourcenaufwand behoben werden müssen (IT-Experten, Krisenstab etc.).

Stimmen Sie sich mit der IT-Abteilung ab, ob es in ihrem Unternehmen ein IT-Störungsmanagementsystem gibt, und ob eine derartige Einteilung bereits vorgenommen wurde. Diese Informationen können Sie dann wiederum in ihr Krisen- und Notfallmanagement einfließen lassen. Denn Ziel bei einem Ausfall ist es immer, die Geschäftskontinuität schnellstmöglich wiederherzustellen, um den betriebswirtschaftlichen Schaden zu minimieren.

©PHOTOMORPHIC PTE. LTD.

NUTZEN SIE E-LEARNING-TRAININGS FÜR DEN AUFBAU EINER „MENSCHLICHEN FIREWALL“

Bauliche und technische Sicherheitsvorkehrungen und -maßnahmen allein betrachtet sind keineswegs ausreichend, um ein gewisses Maß an Sicherheit zu gewährleisten. Denn der Faktor „Mensch“ bildet nach wie vor das schwächste Glied der Kette und bleibt ein beliebtes Angriffsziel für Kriminelle. Daher ist es essentiell, Mitarbeiter nachhaltig zu sensibilisieren und mit auf die „Reise der Sicherheit“ zu nehmen.

Hierfür ist es zum Einen notwendig, Mitarbeitern das „Wieso“ und „Weshalb“ von Sicherheitsvorkehrungen und -maßnahmen sowie ggf. damit einhergehende alltägliche Einschränkungen zu erläutert, um ein gewisses Grundverständnis zu bilden. Und zum Anderen werden Mitarbeiter durch die Wissensvermittlung von Risiken und Gefährdungen dahingehend sensibilisiert, dass sie zukünftig genauer auf verdächtige Situationen und Ereignisse reagieren und ihr persönliches Sicherheitsbewusstsein und Verhalten stärken.

> **DURCH DIE VERSTÄNDLICHE VERMITTLUNG VON RISIKEN UND GEFÄHRDUNGEN LASSEN SICH POSITIVE VERHALTENSÄNDERUNGEN HERBEIFÜHREN!**

DER RISIKOFAKTOR MENSCH

Viele Mitarbeiter kennen die vielfältigen Risiken und Gefährdungen gar nicht, denen sie und ihr Unternehmen innerhalb der Arbeitswelt ausgesetzt sind. Dies führt dazu, dass

- Sicherheitsmaßnahmen nicht verstanden oder als lästig empfunden und entsprechend umgangen werden,
- eine gewisse Sorglosigkeit im Umgang mit Daten und Informationen herrscht,
- sich auf technische Schutzmechanismen zu 100 % verlassen wird und
- keine persönliche Eigenverantwortlichkeit für Sicherheit gesehen wird.

Diese mangelnde Kenntnis lässt sich vielerorts bereits im Flurgespräch ganz einfach herausfinden, indem gezielt z. B. nach der Kenntnis über Social Engineering, CEO-Fraud oder dergleichen gefragt wird. Die Mehrzahl der Befragten wird mit den Begriffen und was sich dahinter verbirgt, kaum etwas anfangen können.

ABHILFE SCHAFFEN

Durch Erkenntnis und Übung lassen sich Verhaltensänderungen herbeiführen. Daher bieten sich kurze und innovative E-Learning-Trainings als „on the job“-Schulung an, um in kurzer Zeit und mit geringem Aufwand einen hohen Wissenstransfer zu erzielen. Die Möglichkeit des zeit- und ortsunabhängigen Lernens im eigenen Lerntempo, ohne Reisekosten, ohne Personalausfälle sowie die einfache Integration in den Alltag machen E-Learning-Trainings zu einer attraktiven Lösung für modernen Wissenstransfer.

E-LEARNING BIETET IHNEN VIELE VORTEILE:

- zeit- und ortsunabhängiges Lernen (24/7)
- spart Reisekosten
- ist umweltschonend
- berücksichtigt das individuelle Lerntempo
- ist in den Arbeitsalltag integrierbar
- bedient sich einer interaktiven Wissensvermittlung
- kann über jeden internetfähigen PC oder Tablet durchgeführt werden
- u. v. m.

Geben Sie Mitarbeitern das notwendige Rüstzeug an die Hand, um potentiell sicherheitskritische Situationen selbstständig erkennen und angemessen reagieren zu können.

Natürlich bildet dies nur die Basis der Mitarbeitersensibilisierung, da hierbei unternehmensspezifische Sicherheitsmaßnahmen nicht erläutert werden. Dies kann jedoch mit kurzen Impulsvorträgen, Newslettern, thematischen Bausteinen im Intranet oder der Mitarbeiterzeitung etc. erreicht werden.

AUSZUG DER THEMENVIELFALT DER AM MARKT VERFÜGBAREN E-LEARNING-TRAININGS

UNTERNEHMENSSICHERHEIT/WIRTSCHAFTSSCHUTZ

- Unternehmenssicherheit
- Clear-Desk am Arbeitsplatz
- Datenschutz und Datensicherheit
- Compliance
- Anti-Korruption
- Social Engineering
- Reisesicherheit im Ausland
- Gefahrenwahrnehmung
- Besucher- und Fremdfirmenmanagement
- Umgang mit Bombendrohungen, verdächtigen Postsendungen und Gegenständen

NOTFALL-, KRISEN- UND KATASTROPHENVORSORGE

- Notfall- und Krisenvorsorge
- Hygienemaßnahmen im Pandemiefall
- Richtiges Verhalten in Not- und Krisensituationen
- Vorbereitung, Verhalten und Selbsthilfe bei einem langanhaltenden Stromausfall

INFORMATIONS- UND IT-SICHERHEIT

- IT-Sicherheit
- Risiken sozialer Medien
- Passwortsicherheit
- WLAN sicher nutzen (VPN)
- Gefahrenquellen im Internet
- Sicheres Verhalten im Internet
- Grundbegriffe der Informationssicherheit
- Klassifizieren von Informationen
- Sicheres Vernichten von Informationen
- Gefahren mobiler Endgeräte und Datenträger

GEWALTPRÄVENTION

- Bedrohungsmanagement an Arbeitsplätzen mit Publikumsverkehr
- Richtiges Verhalten bei Gefahren- und Bedrohungslagen an Arbeitsplätzen mit Publikumsverkehr

SONDERTHEMEN

- AEO-Sicherheitsunterweisung
- ISPS-Code-Unterweisung gemäß SOLAS XI-2
- Luftsicherheitsschulungen gemäß DVO (EU) 2015/1998

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.

SICHERHEITSMESSE

SICHERHEITSEXPO VOM 27. - 28. JUNI 2018 IN MÜNCHEN

Die SicherheitsExpo München ist eine Fachmesse, die sich zum Ziel gesetzt hat, Sicherheitstechnik für Unternehmen und Privatpersonen zum Schutz vor Innen- und Außentätern zu demonstrieren.

Die neuesten Entwicklungen und zukunftsweisende Technologien der Sicherheitstechnik, unter anderem NFC (Nahfeldkommunikation/Micropayment), RFID (Kontaktlose Sender-Empfänger-Systeme), Biometrie und Identity-Management sowie Zutrittskontrolle, Videoüberwachung, Leitstellen und Mobilfunk werden auf der SicherheitsExpo 2018 vorgestellt.

Weitere Messeschwerpunkte sind:

- Alarmanlagen
- Brand- und Explosionsschutz
- Freilandsicherung
- Gebäudesicherheit
- IT- und Kommunikationssicherheit
- KFZ-Sicherungssysteme
- Videotechnik

Parallel zur Messe finden an beiden Messetagen Foren mit interessanten Fachvorträgen rund um den Einsatz von Sicherheitstechnik gerade im Zeitalter der Digitalisierung und Industrie 4.0 statt.

SICHERHEITS EXPO MÜNCHEN

VERBAND

ASW BUNDESVERBAND (ALLIANZ FÜR SICHERHEIT IN DER WIRTSCHAFT E. V.)

1993 wurde die Arbeitsgemeinschaft für Sicherheit in der Wirtschaft gegründet, welche sich in den vergangenen Jahren umstrukturiert hat und seit 2015 den neuen Namen ASW Bundesverband (Allianz für Sicherheit in der Wirtschaft e. V.) trägt. Der ASW ist ein Zusammenschluss regionaler Branchenverbände und vertritt als Bundesverband die Interessen der deutschen Wirtschaft in Sicherheitsfragen.

Sicherheitsthemen werden vom ASW als aktiver Dialogpartner mit Behörden, der Politik und Nichtregierungsorganisationen auf nationaler und europäischer Ebene mitgestaltet. Kernbestandteil ist, dass Sicherheit ein Designmerkmal ist und als integraler Bestandteil aller unternehmerischen Prozesse wahrgenommen wird. Dafür werden die Kommunikationskanäle zwischen Behörden und Unternehmen geöffnet und gepflegt, denn frühzeitiges Wissen bedeutet nachhaltige Sicherheit für deutsche Unternehmen.

Eine hohe fachliche Spezialisierung erreicht der ASW durch die Gründung einzelner Arbeitskreise und Kompetenz-Center zu den Themen:

- Wirtschaftsschutz und Spionageabwehr
- Cyber-Security
- Logistiksicherheit
- Personelle Sicherheit
- Anti-Fraud-Management
- Lage- und Reisesicherheit
- Aus- und Weiterbildung, Veranstaltungen

Diese Arbeitskreise beschäftigen sich eingehend mit der Betrachtung von Risiken bezüglich möglicher Abwehrmaßnahmen und Sensibilisierungsstrategien für die deutsche Wirtschaft.

Der ASW informiert auf seiner Webseite u. a. zu aktuellen Problemfeldern und stellt kostenfrei Leitfäden und Leitblätter zu verschiedenen Sicherheitsthemen sowie Informationen rund um relevante Bedrohungsfelder zur Verfügung.

ZU DEN AUTOREN

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

IMPRESSUM

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

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.