SICHERHEIT. DAS FACHMAGAZIN.

SICHERHEIT AUF DEN PUNKT GEBRACHT.

EXKLUSIV Seite 9 und 18

2 Experteninterviews zu den Themen „Desinformation“ und „Veranstaltungssicherheit“

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.

SICHERHEIT. DAS FACHMAGAZIN.

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

DOWNLOADS

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

SECURITY-SERVICE-CENTER

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

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

KOSTENFREI & UNVERBINDLICH

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

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

Wie finanziert sich SICHERHEIT. Das Fachmagazin.?

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

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

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

UNSERE THEMEN

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

E-PAPER

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

Ihre Vorteile:

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

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

NUTZEN SIE DIE ATTRAKTIVEN ANGEBOTE DES „EUROPEAN CYBER SECURITY MONTH 2018 (ECSM)“

Der „European Cyber Security Month“ ist eine europaweite Sensibilisierungskampagne, die Veranstaltungen und Aktionen rund um die Themen der Cyber-Sicherheit anbietet. Seit 2012 findet diese europaweite Aktion für den umsichtigen und verantwortungsvollen Umgang im Cyber-Raum statt.

Federführend ist die europäische IT-Sicherheitsbehörde (ENISA). In Deutschland koordiniert das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Aktionsmonat.

Die Ziele der Initiatoren des ECSM sind:

- die Schaffung eines allgemeinen Bewusstseins für Cyber-, Netz- und Informationssicherheit
- die Förderung einer sichereren Nutzung des Internets
- die Aufmerksamkeit und das Interesse in Bezug auf Informationssicherheit durch politische und mediale Koordination

In diesem Jahr findet der Aktionszeitraum vom 1. bis 31. Oktober mit wechselnden Wochenthemen statt:

1. bis 7. Oktober
IT-Basisschutz leicht gemacht

8. bis 14. Oktober
Digitales Leben - Sicherheit vermitteln

15. bis 21. Oktober
Schutz vor Onlinebetrug

22. bis 31. Oktober
IoT und Smart Devices - mit Sicherheit digital und smart

ANGEBOTE DES ECSM

Allein im vergangenen Jahr gab es 530 Partneraktionen, die kostenfreie oder vergünstigte Checks, Webinare, Veranstaltungen, E-Learning-Schulungen, Videos, Live-Hacks, persönliche Beratungen und Vergünstigungen auf Produkte angeboten haben. Die Zielgruppen sind breit gestreut von Privatpersonen, Unternehmen über Institutionen und Behörden bis hin zu Fachexperten.

Unter folgendem Link können Sie einen Blick in die Aktionen des ECSM 2018 werfen. Eventuell ist ja auch für Ihre Kolleginnen und Kollegen ein passendes Angebot dabei, das zur Stärkung der Sicherheitssensibilität im Unternehmen beiträgt.

www.cybersecuritymonth.eu

VERHALTENSEMPFEHLUNGEN BEI ENTFÜHRUNGEN UND GEISELNAHMEN

Entführungen und Geiselnahmen finden sich in allen Epochen der Zeitgeschichte wieder, da Geiseln als Verhandlungsmasse dienen, um materielle oder auch immaterielle Zwecke durchzusetzen. Für gefährdete Personenkreise ist nicht nur ein angemessenes Gefahrenbewusstsein essentiell, sondern auch das richtige Verhalten im Entführungsfall.

Eine Entführung ist immer mit Zwang verbunden und liegt im polizeitaktischen Sinne vor, wenn Täter Personen/Opfer ohne deren Einwilligung zur Durchsetzung ihrer Ziele an einen unbekannten Ort verbringen und einsperren oder an dem vorhandenen Ort (Geiselnahme) festhalten. Derartige Delikte werden im deutschen Strafgesetzbuch in Abschnitt 18 unter Straftaten gegen die persönliche Freiheit (Freiheitsberaubung) geführt.

FORDERUNGEN GEGEN LEBENDE GEISELN

Überwiegend dienen Entführungen der Durchsetzung materieller, gelegentlich auch immaterieller Ziele wie soziale, politische oder religiös motivierte Forderungen. Gerade bei den materiellen Forderungen sind Repräsentanten des Geldes oder deren Familienangehörige besonders lukrative Ziele. Aber auch Auslandsreisende oder Entsandte (Expatriate) sollten dieses Risiko nicht unterschätzen, wie die jüngste Vergangenheit zeigt. Der Islamische Staat (IS) machte vor allem durch seine überaus brutalen Videos von Enthauptungen mehrerer Geiseln von sich reden. Opfer einer Entführung oder Geiselnahme kann man entweder zufällig oder gezielt werden. Gerade bei gezielten Entführungen gehen die Täter geplant und strukturiert vor, indem das Opfer sorgfältig ausgewählt und im Vorfeld eingehend observiert wird.

DIE ENTFÜHRUNG

Eine Entführung oder Geiselnahme bedeutet eine schwere physische und psychische Ausnahmesituation für das Opfer. Wie tragfähig das Opfer während der Gefangenschaft ist, ist auch davon abhängig, unter welchen äußeren Bedingungen die Geiselhaft erfolgt.

Hierbei spielen folgende Faktoren eine wichtige Rolle:

DER ABLAUF

- Verletzungen
- Transportstrapazen
- Hygienische Verhältnisse
- Kommunikation/Erklärungen
- Licht/Dunkelheit
- Art/Anzahl Versteck(e)
- Dauer

DER/DIE TÄTER

- Gewaltbereitschaft
- Folter
- Planungstreue
- Professionalität
- Kalkulierbarkeit

DIE GEISEL

- Physische Belastbarkeit
- Psychische Belastbarkeit
- Lebenssituation
- Liquidität der Familie

Die Reaktionen und das Verhalten von Geiseln ist willkürlich und von Zweifel, Furcht, Panik bis hin zu Wut und Überempfindlichkeit geprägt.

DER ÜBERFALL

In dieser risikobehafteten Phase erleben die Täter alles Unerwartete als Angriff und wenden oftmals Gewalt an, ohne das Opfer jedoch zu töten. Als Opfer sollte man sich

defensiv, passiv und kooperativ verhalten, da Flucht in den meisten Fällen zwecklos ist und das Leben kosten kann. Nicht auffallen, sich dem Täter nicht widersetzen und keine Anwendung von Gewalt sind die Grundprinzipien in der ersten Phase. Versuchen die Entführer mit Ihnen zu kommunizieren, vermeiden Sie Blickkontakt und antworten Sie ehrlich auf Fragen, um sich nicht in Widersprüche zu verstricken.

Von Anfang an geht es darum, den Schock des Kontrollverlustes durch die Entführung zu mildern und den eigenen Handlungsspielraum nach und nach auszudehnen. Ihre Reaktion auf das Geschehen wird zunächst aus Furcht, Schock und einem Gefühl der Desorientierung bestehen. Verinnerlichen Sie sich die Tatsache des Ereignisses, realisieren Sie die Situation und nehmen Sie sich dieser an, denn nur so können die eigenen Ängste abgebaut werden. Über die Zeit wird sich die Situation stabilisieren.

OPTIMISMUS HILFT BEIM ÜBERLEBEN

Für Ihr Überleben ist es von entscheidender Bedeutung, dass Sie optimistisch bleiben. Lassen Sie sich nicht hängen, machen Sie sich immer wieder bewusst, dass dort draußen andere Menschen an Ihrer Befreiung arbeiten. Ihre Entführer wollen in der Regel ebenfalls, dass Sie am Leben bleiben, denn tot nützen Sie ihnen nichts mehr. Sie sind ein Tauschgegenstand, ein Mittel zum Zweck. Ausnahmen hiervon sind Entführungen, bei denen Geiseln durch eine medienwirksame Inszenierung ihres Todes für die terroristische Propaganda instrumentalisiert werden. Eine der wichtigsten Voraussetzungen für Ihr Überleben im Entführungsfall ist Selbstrespekt. Zeigen Sie gegenüber Ihren Entführern nach Möglichkeit weder Traurigkeit noch Schwäche, auch wenn es gerade zu Beginn einer solchen Gefangenschaft hart ist, sich an den Kontrollverlust und die ungewohnten Umstände zu gewöhnen. Dies wird mit der Zeit einfacher.

VERHALTENSREGELN IM ENTFÜHRUNGSFALL

1. GEWINNEN SIE SO VIEL KONTROLLE WIE MÖGLICH ZURÜCK. Dies umfasst Ihren Geist ebenso wie Ihren Körper. Kooperieren Sie und befolgen Sie die Anweisungen der Entführer, aber ziehen Sie innerlich klare Grenzen in Bezug auf Ihre persönlichen Werte und Einstellungen, sodass Ihre eigene Integrität gewahrt bleibt. Machen Sie sich klar, dass nicht Sie persönlich gemeint sind, sondern dass Sie als Mittel für einen bestimmten Zweck dienen.

2. BESCHÄFTIGEN SIE IHR GEHIRN, UM PANIK ZU VERMEIDEN. Bestimmen Sie, was Sie denken, indem Sie sich selbst immer wieder neue Aufgaben stellen: Prägen Sie sich bereits zu Beginn der Entführung die Fahrtroute ein, schätzen Sie Zeitdauer und Zeitintervalle, versuchen Sie, Geräusche wahrzunehmen und einzuordnen. Dies hilft nicht allein, Ihre Panik zu kontrollieren, sondern kann den Sicherheitsbehörden später auch bei der Aufklärung helfen. Dasselbe gilt bei der Ankunft am Ort Ihrer Gefangenschaft: Prägen Sie sich alle Merkmale ein, von der Bodenbeschaffenheit bis hin zu Geräuschen und Gerüchen. Es geht um Orientierung.

3. TRAINIEREN SIE IHREN KÖRPER. Tägliche Übungen verbessern Ihren körperlichen Zustand. Zudem helfen sie gegen die allgegenwärtige Langeweile der Gefangenschaft und wirken sich positiv auf Ihren mentalen Zustand aus. Damit Sie in Form bleiben, müssen Sie regelmäßig essen. Lehnen Sie das Essen nicht ab, das Ihnen die Entführer geben. Sie brauchen Energie, um zu überleben. Die Angst, die Entführer hätten das Essen vergiftet, ist unbegründet, denn es gäbe für sie leichtere Möglichkeiten, Sie zu töten.

4. ACHTEN SIE AUF IHRE PERSÖNLICHE HYGIENE. Entwickeln Sie Routinen, um den eigenen Körper zu reinigen, soweit die Umstände dies erlauben. Eine über längere Zeit unterlassene Körperhygiene kann in extremen Klimaverhältnissen wie Wüsten oder Urwäldern fatale Folgen haben. Zudem ist Körperpflege Ausdruck Ihres Selbstrespekts und dient der Abgrenzung: Sie wollen nicht aussehen wie Ihre Geiselnehmer. Tragen Sie, sofern es Ihnen erlaubt ist, weiterhin Ihre eigene Kleidung als Ausdruck Ihrer eigenen Persönlichkeit.

5. BAUEN SIE EINE PERSÖNLICHE BEZIEHUNG ZU IHREN ENTFÜHRERN AUF - IN MAßEN. Ihr Ziel sollte eine kontrollierte Kooperation sein. Bewahren Sie zu Anfang Distanz und gewinnen Sie zunächst einen Eindruck von Ihren Geiselnehmern. Versuchen Sie, die unterschiedlichen Persönlichkeiten und Charaktere einzuschätzen. Sobald Sie diesbezüglich etwas Klarheit haben, etablieren Sie vorsichtig und gezielt den Kontakt zu ausgewählten Geiselnehmern.

Gelingt Ihnen das, können Sie eventuell Ihren Handlungsspielraum erhöhen, erhalten mehr Essen, dürfen häufiger zur Toilette gehen oder können Ihren persönlichen Komfort auf andere Weise steigern. Außerdem fällt es (psychisch gesunden) Menschen deutlich schwerer, diejenigen zu töten, zu denen sie eine persönliche Beziehung aufgebaut haben.

ENTFÜHRER UND ENTFÜHRTE: GEFÄHRLICHE NÄHE

Bei alledem ist dennoch höchste Vorsicht geboten: Geisel und Geiselnehmer werden durch die extreme Situation und die damit verbundenen emotionalen Belastungen ungewollt zusammengeschweißt. Die Grenzen zwischen beiden Parteien können gerade bei länger andauernden Entführungssituationen verschwimmen. So kann es passieren, dass Geiseln ein positives emotionales Verhältnis zu ihren Entführern aufbauen und Sympathie und Verständnis für deren Sache entwickeln.
Dieses als »Stockholm-Syndrom« bekannte psychologische Phänomen kann dazu führen, dass die Geiseln mit ihren Geiselnehmern kooperieren oder diese gar gegenüber Polizei und Sicherheitskräften zu schützen versuchen.

DIESE UND WEITERE TIPPS, DIE WIR IHNEN IN UNSEREM DOWNLOAD-BEREICH ZUR VERFÜGUNG GESTELLT HABEN, SOLLTEN SIE IN DIE UNTERNEHMERISCHEN INFORMATIONEN EINFLIESSEN LASSEN, UM POTENTIELL GEFÄHRDETEN PERSONEN ODER REISENDEN EINEN WEGWEISER AN DIE HAND ZU GEBEN.

DIE FREILASSUNG

Zwischen Zielerfüllung und der Freilassung können Stunden, Tage, Wochen oder gar Monate vergehen. Die Umstände der Freilassung sind so individuell wie die Entführung selbst. Von der Freisetzung auf einer Straße, den Hinweis auf das Versteck bis hin zu neuen Forderungen ist alles möglich.

Im Anschluss an eine überstandene Entführung empfiehlt sich in jedem Fall eine psychologische Behandlung, um die extreme Situation bestmöglich zu verarbeiten und Folgewirkungen möglichst zu mildern.

Die hier aufgeführten Handlungsempfehlungen sind in leicht gekürzter Fassung dem Buch **„Terrorismus - wie wir uns schützen können"** von **Florian Peil** entnommen (Murmann Publishers).

VERBREITUNG VON DESINFORMATION: SCHADEN OHNE EINBRUCH

Die Macht der Medien ist seit jeher unbestritten. Begrifflichkeiten wie „Desinformation“ oder „Fake News“ sind im medialen Kontext jedoch relativ neu anzutreffen. Dennoch gab es gefälschte oder gezielt fehlgeleitete Informationen in den Medien schon immer. Für Unternehmen und Organisationen ist es daher wichtig, sich mit dem Phänomen „Desinformation“ und den Möglichkeiten der Aufdeckung und Eindämmung frühzeitig auseinanderzusetzen.

Gefälschte oder verfälschte Informationen, die im Internet oder in anderen Medien verbreitet werden, gezielte Hetze gegen Unternehmen, Organisationen oder Einzelpersonen und somit das Streuen von Gerüchten, üble Nachrede oder gezielte Propaganda sind das Ergebnis von Desinformation. Falschmeldungen, die nicht aus dem Bereich des satirischen Journalismus stammen, werden zur gesellschaftlichen, politischen und/oder wirtschaftlichen Stimmungsmache genutzt, oder um einen monetären Gewinn zu erzielen, die politische Meinungsbildung in eine bestimmte Richtung zu lenken bis hin zur Destabilisierung von demokratischer Meinungsbildung und von ganzen Staaten.

VERBREITUNG VON DESINFORMATIONEN

Soziale Netzwerke und Nachrichtenportale sind mittlerweile zu wichtigen Plattformen der gesellschaftlichen, politischen und wirtschaftlichen Kommunikation geworden. Um auf diesen Plattformen gezielt Desinformationen zu verbreiten, benötigt man geringe IT-Kenntnisse. Es müssen auch keine Systeme gehackt werden oder ein unmittelbarer persönlicher Kontakt mit dem Ziel bzw. der Zielperson bestehen. Die Erstellung von Desinformationen ist heutzutage binnen weniger Minuten mit Hilfe frei verfügbarer Software im Internet auch für den Laien möglich.

Gerade für Unternehmen und Organisationen besteht die Gefahr dahingehend, dass gezielt die öffentliche Wahrnehmung oder die Diskreditierung bestimmter Produkte beeinflusst bzw. nachhaltig geschädigt werden kann. In jedem Fall lassen sich durch derartige Manipulationen durchaus nennenswerte Wettbewerbervorteile in Bezug auf die Marktsituation herstellen.

Daher kommt es immer mehr zu gezielt eingesetzten Desinformationskampagnen, die durch sogenannte „malicious social bots“ initiiert, verbreitet und verstärkt werden. „Bots“ kennt man beispielsweise aus Computerspielen als virtuelle Gegner oder Ersatz für spieleseitige Akteure, die automatisiert eine gewisse Rolle einnehmen. Im Bereich der Informationsverbreitung sind „Bots“ nichts anderes als Computerprogramme, die automatisiert gewisse vorab definierte Aufgaben/Abläufe erledigen sollen, wie beispielsweise Begriffe in sozialen Netzwerken liken, Inhalte mit der Community teilen, Kommentare verfassen oder einzelnen Nutzern folgen. Die Erstellung eines eigenen „Bots“ ist heutzutage binnen weniger Minuten mit Hilfe frei verfügbarer Software im Internet auch für den Laien möglich. Effektiv wird das Ganze erst, wenn „Bots“ zusammen als Schwarm agieren (sogenannte „Bot-Netze“) und somit das Meinungsbild gezielt und strukturiert durch die massenhafte Schwarmverbreitung beeinflussen. Darüber hinaus gibt es aber auch durchaus reale Menschen (sogenannte „Trolle“), die dafür bezahlt werden, im Internet negative oder mitunter abwertende Kommentare zu verfassen oder aber positive Bewertungen abzugeben, um Produkte, Dienstleistungen oder Meinungen zu loben.

ANGRIFFSZIELE	→ DESINFORMATION
Reputation des Unternehmens	Produkte werden im Tierversuch getestet, Produkte stammen aus Kinderarbeit ...
Kreditwürdigkeit	Gravierende technische Probleme in der Produktion, Eröffnung eines Insolvenzverfahrens ...
Ruf als Arbeitgeber	Menschenunwürdige Arbeitsbedingungen, Verstöße gegen Arbeitsschutzgesetze ...
Diskreditierung der Qualität	Produktverunreinigungen, Tote/Verletzte durch Produktbenutzung ...
Mitarbeiterdemotivation	Veröffentlichung fiktiver Gehaltslisten, Standortschließungen und Stellenabbau ...
Compliance-Vorwürfe	Bestechungsvorwürfe, Schmiergeldskandal ...

DIE HERAUSFORDERUNG LIEGT IN DER FRÜHERKENNUNG

Die Herausforderung bei der frühzeitigen Erkennung von Desinformationen ist, dass man nicht genau weiß, wonach man eigentlich suchen soll. Es ist lediglich bekannt, dass das Phänomen „Desinformation“ für das eigene Unternehmen oder einzelne Unternehmensvertreter sowie ggf. Kunden und Geschäftspartner mitunter gefährlich werden könnte.

VISUALISIERUNG DER NETZE

Wichtig ist, einen solchen Angriff bereits in der frühen Phase der Aufmerksamkeitslenkung zu erkennen. Rein stichwortbasierte Suchhilfen scheiden jedoch in den meisten Fällen aus, denn diese zielen primär auf die alltäglichen Informationen ab. Wichtig ist, bereits in der Früherkennung zu filtern: also nicht im bereits gefestigten Google-Ranking zu suchen, sondern in sozialen Netzwerken, Blogs oder vermeintlichen Produkttests oder Produktbewertungen.

Die Möglichkeiten der Analyse sollten im Idealfall von IT-Spezialisten eruiert werden, um sich den neuen Herausforderungen überhaupt adäquat stellen zu können. Algorithmen können dabei unterstützen, aus dem Meer an Informationen die wesentlichen Informationen herauszufiltern, übereinanderzulegen und zu analysieren. Die daraus resultierenden Rechercheergebnisse sollten im Anschluss von einer geeigneten Stelle im Unternehmen (im Idealfall der Kommunikationsabteilung in Zusammenarbeit mit der Sicherheitsabteilung bzw. einem Sicherheitsverantwortlichen) durchgeführt werden.

WENN SIE NICHT HANDELN, WERDEN SIE BEHANDELT! “

DEFINITION „DESINFORMATION“

Desinformation steht für alle nachweislichen Formen der falschen, ungenauen oder irreführenden Darstellungsform, die entworfen, dargestellt und präsentiert werden mit dem Ziel, absichtlich öffentlichen oder wirtschaftlichen Schaden anzurichten oder einen monetären Gewinn zu erzielen.

UMFRAGEN ZUFOLGE WIRD DIE BEDROHUNG DURCH DIE VERBREITUNG VON „FAKE NEWS“ IN DEN KOMMENDEN JAHREN ALS SEHR HOCH EINGESCHÄTZT. NICHT ZULETZT BEDINGT DURCH DIE RASANT WACHSENDE DIGITALISIERUNG UND DIE NUTZUNG NEUER MEDIENFORMATE. DAS MEISTE VERTRAUEN IN NACHRICHTENQUELLEN WIRD LAUT DEN UMFRAGEERGEBNISSEN DEM RADIO, TV UND PRINTMEDIEN ENTGEGENGEBRACHT, DA MAN HIER AUF DIE SORGFÄLTIGE JOURNALISTISCHE RECHERCHE VERTRAUT. AM WENIGSTEN VERTRAUEN WIRD ONLINENACHRICHTENQUELLEN UND VIDEOPORTALEN ZUGESPROCHEN, OBWOHL HIER DER VERBREITUNGSFAKTOR WESENTLICH HÖHER UND SCHNELLER IST.

3 SCHRITTE ZUR EFFEKTIVEN VORBEUGUNG UND VERTEIDIGUNG

1. EINE EFFEKTIVE VORBEUGUNG UNTERSTÜTZT BEI DER WIRKSAMEN BEKÄMPFUNG

- Die beste Verteidigung ist immer ein kritischer Verstand.
- Die Sensibilisierung von Mitarbeitern steht besonders im Vordergrund, denn umso weniger vertrauliche Informationen nach Außen gelangen, desto weniger Angriffspunkte gibt es.
- Ein präventiver Austausch mit Sicherheitsbehörden (Landeskriminalamt, Verfassungsschutz etc.) zu aktuellen Vorkommnissen oder Kriminalitätsphänomenen kann weitere relevante Erkenntnisse liefern.
- Presse- und Medienkontakte sind immer hilfreich, um im Ereignisfall die notwendige Glaubwürdigkeit zu besitzen und etwaigen „Fake News“ gemeinsam entgegenzusteuern.
- Auch der umgekehrte Weg ist hilfreich, denn Presse- und Medienvertreter suchen bei kursierenden Informationen i. d. R. zuerst den direkten Kontakt zum Betroffenen.
- Definition von Zuständigkeiten und Verantwortlichkeiten (z. B. Kommunikationsabteilung in Zusammenarbeit mit der Sicherheitsabteilung bzw. einem Sicherheitsverantwortlichen) bis hin zu einem Leitfaden für den „Ernstfall“.
- Erstellung eines Reputationslagebildes aller Unternehmensbereiche (Arbeitgeberbild, Kreditfähigkeit, Produkt/-e, Vertrieb, Qualität, Service etc.).

2. MEDIENBEOBACHTUNG UND MEDIENFILTERUNG SIND DAS A UND O

- Automatisierte Analyse von länder- und sprachenübergreifenden Informationen als eine Art „Frühwarnsystem“ (z. B. mittels Google Alerts, Software-Tools, externen Dienstleistern etc.).
- (Desinformations-)Filterung nach Inhalt, Kontext und Quelle.
- Schaffung einer unternehmensweiten Ausrichtung im Bereich der Früherkennung und Weiterleitung von Falschmeldungen.
- Strukturierte Informationsteilung im Unternehmen sowie ggf. mit Lieferanten, Geschäftspartnern und Kunden.

3. GEGENMASSNAHMEN EINLEITEN UND ZUKÜNFTIGE ABWEHRSTRATEGIEN ENTWICKELN

- Möglichkeiten geeigneter Gegenmaßnahmen eruieren.
- Prüfung juristischer Handlungsspielräume und Möglichkeiten.
- Einbeziehung intern betroffener Abteilungen in die Kommunikationsstrategie.
- Zeitnahe Reaktion am Ursprungsort der (Des-)Information.
- Je nach Schwere bzw. öffentlicher Gewichtung der (Des-)Information: breite Stellungnahme in den Medien betreiben.
- Angreifer und artverwandte Akteure ermitteln und Abwehrstrategien entwickeln.

Zumindest für größere Unternehmen wäre der Einsatz von speziell in Datenjournalismus ausgebildetem Personal denkbar. Denn neben der Tätigkeit im Marketing, in der PR und insbesondere bezüglich des Social-Media-Auftritts könnten sie für das Unternehmen sehr nützlich sein, da Desinformationskampagnen frühzeitiger erkannt werden könnten.

Mit freundlicher Unterstützung von Dr. Michael Kreutzer (Fraunhofer SIT)

INTERVIEW MIT DR. MICHAEL KREUTZER

Forschungsleiter des Forschungsprojektes „DORIAN - Desinformation aufdecken und bekämpfen“ - am Fraunhofer-Institut für Sichere Informationstechnologie

DORIAN

Das vom Bundesministerium geförderte Forschungsprojekt „DORIAN - Desinformation aufdecken und bekämpfen“ - erarbeitet einen Katalog möglicher technischer, politisch-normativer und soziokultureller sowie organisatorischer Empfehlungen zur Bekämpfung von Desinformation im Internet. Neben diesen Empfehlungen, die sich an die Medien, Politik, Bürger und die Wissenschaft richten, werden auch mögliche technische Lösungen zur Erkennung und Bekämpfung von Desinformation und Meinungsmanipulation ›››

››› im Internet aufgezeigt und deren mögliche Wirkung auf Nutzer und deren Akzeptanz überprüft. Insbesondere die Weiterentwicklung der Rechtsordnung, die Mediendidaktik und der weitere Forschungsbedarf stehen im Mittelpunkt des Projektes DORIAN. Projektpartner sind das Fraunhofer-Institut für Sichere Informationstechnologie SIT Darmstadt, die Hochschule der Medien Stuttgart, die Universität Duisburg-Essen und die Universität Kassel.

GIBT ES AUS IHRER SICHT UNTERSCHIEDE IN DER WORTBEDEUTUNG VON DESINFORMATION, „FAKE NEWS“ ODER FALSCHMELDUNG?

Bei einer Falschmeldung steckt in der Regel keine böse Absicht dahinter. Sie ist vielfach auf journalistische Fehler zurückzuführen, die diverse Ursachen haben können, wie beispielsweise Zeitdruck. Als Modebegriff wird „Fake News“ aktuell von verschiedenen für alle denkbaren, unliebsamen Meldungen genutzt. Die europäische Kommission definiert Desinformationen als „nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können“.

WIE SCHÄTZEN SIE DAS ENTDECKUNGSRISIKO VON „FAKE NEWS“ EIN?

Eine einzelne Nachricht, Kommentierung oder über soziale Medien geteilte Information kann mittels journalistischer Recherchemethoden recht leicht als Desinformation überführt werden. Es gibt sogar eine hohe Übereinstimmung von Desinformationsstrategien selbst bei verschiedenen Verursachern. Typisch sind beispielsweise Negativität von Meldungen und die Beschreibung eines großen Schadens.

GIBT ES KONKRETE BEISPIELE AUS DER WIRTSCHAFT, BEI DENEN DIE VERBREITUNG VON DESINFORMATIONEN ZU WIRTSCHAFTLICHEN SCHÄDEN GEFÜHRT HAT?

CEO-Fraud kann beispielsweise als gezielter Angriff mit Methoden der Desinformation angesehen werden: Beim CEO-Fraud sammeln die Täter alle ihnen öffentlich zugänglichen Informationen über das Unternehmen und nehmen teilweise auch Kontakt mit einzelnen Personen aus dem Zielunternehmen auf. Mit Hilfe dieses Wissens veranlassen sie eine Person aus dem Unternehmen durch plausibel anmutende Dringlichkeit von oberster Ebene zum Transfer eines größeren Geldbetrages ins Ausland.

KÖNNEN SIE SCHON ÜBER KONKRETE FORSCHUNGSERGEBNISSE BERICHTEN?

Erste Zwischenergebnisse stimmen uns optimistisch, dass wir mit Hilfe von diversen Methoden vor allem des maschinellen Lernens themenspezifische Desinformation vorfiltern können und sich damit die Rechercheergebnisse von Menschen sehr gut verbessern lassen. Hierzu trainieren wir die Erkennungsleistung der Maschine, indem wir sie mit Inhalten und deren sprachlichen Eigenschaften füttern, die wir als Desinformation mittels journalistischer Recherchemethoden identifiziert haben. Im Idealfall kann der Rechner später mit hoher Zuverlässigkeit diese Eigenschaften bei neu präsentierten Texten wiedererkennen und die Desinformationstexte entlarven. Da die Maschine sehr schnell arbeitet, kann sie potentielle Kandidaten für Desinformation aus einer großen Datenmenge in kurzer Zeit herausfiltern.

IM ENDEFFEKT KANN MAN NICHTS GEGEN EINE FALSCHE INFORMATION ANRICHTEN, AUSSER DIESE MÖGLICHST IM KEIM ZU ERSTICKEN UND MIT EINEM EFFEKTIVEN KOMMUNIKATIONSKONZEPT GEGENZUSTEUERN…!

Das sind sicher zwei wirksame Vorgehensweisen. Damit die Desinformation nicht auf fruchtbaren Boden fällt, kann eine solide, breit angelegte Medienbildung helfen, unseriöse Quellen zu erkennen. Die Stärkung seriöser und faktenbasierter Berichterstattung und die weitere Erforschung der Mechanismen von Desinformationskampagnen ermöglicht, diese offenlegen und „entzaubern“ zu können.

WIE SOLLTE IHRER MEINUNG NACH AUF EINE DESINFORMATION REAGIERT WERDEN? GIBT ES GEMESSENE ERFAHRUNGSWERTE, WAS AM EFFEKTIVSTEN IST? OFFENSIVE KOMMUNIKATION ODER KLASSISCHE GEGENDARSTELLUNG MIT ODER OHNE BEZUG ZUM ANGRIFF?

Das ist ein aktueller Forschungsgegenstand bei uns. Was wir bereits auch schon von anderen Forschungsgruppen wissen: Die faktenbasierte Darstellung sollte möglichst übersichtlich und klar sein - der Bezug zur manipulativen Botschaft sollte hierbei so gewählt werden, dass er diese nicht noch verstärkt. Dies bedeutet insbesondere, dass die falsche Botschaft nicht an prominenter Stelle in der richtigstellenden Kommunikation wiederholt wird und sich damit „einbrennt“. Zur klar verständlichen Vermittlung von Fakten eignen sich insbesondere leicht zu erfassende graphische Darstellungen.

GAB ES WÄHREND DER BISHERIGEN FORSCHUNGSDAUER ASPEKTE, DIE SIE PERSÖNLICH SCHOCKIERT HABEN, ODER DIE SIE NICHT FÜR MÖGLICH GEHALTEN HÄTTEN?

Der Grad an Negativität, Skandalisierung und teilweise Brutalität der Darstellung der erfassten Desinformationen war für mehrere Mitarbeitende aufwühlend. Umso wichtiger erscheint uns hier die Möglichkeit der maschinenunterstützten Vorverarbeitung, so dass sich verantwortliche Personen zunächst nur mit den wahrscheinlich relevantesten Desinformationen zu befassen brauchen.

VIELEN DANK FÜR DIE INTERESSANTEN EINBLICKE.

ALARMIERUNGS- UND MELDEKETTEN IM EREIGNISFALL

Eine zügige innerbetriebliche Alarmierung gemäß der im Notfall-/Krisenplan festgelegten Alarmierungs- und Meldewege ist eine der wichtigsten Grundlagen für das zeitnahe Tätigwerden der besonderen Aufbau- und Ablauforganisation im Ereignisfall. Wie man einen derartigen Alarmierungsplan aufbauen, strukturieren und beschreiben kann, erläutern wir Ihnen nachfolgend.

Im Ereignisfall ist ein zügiger, strukturierter und ressourcenschonender Informationsfluss für die erfolgreiche Ereignisbewältigung entscheidend. Daher ist die Festlegung von Prozessen und Verfahren für die Alarmierung, Meldung und Eskalation von Ereignissen von entscheidender Bedeutung.

ERKENNEN SIE DIE NOTWENDIGKEIT

Grundsätzlich ist das Thema Krisen- und Notfallmanagement Teil der Fürsorge- und Sorgfaltspflicht eines jeden Arbeitgebers. Und somit im Sinne der Organisationshaftung stets „Chefsache“. Doch ohne Grundkenntnisse und eine gezielte Vorbereitung auf den Ereignisfall wird es schwer, in Notfällen und Krisen richtig zu reagieren und rechtzeitig mögliche Auswirkungen und Folgen abzuschätzen. Ein gut aufgestelltes Unternehmen sollte daher über ein Notfall- und Krisenmanagementsystem verfügen, welches nicht nur den klassischen Brand beinhaltet, sondern auch als Managementorgan für viele andere (Sonder-)Fälle, wie z. B. Versorgungs- und Gebäudeausfälle, Naturereignisse, medizinische Notfälle, CBRN-Gefahren (CBRN: Chemisch-Biologisch-Radioaktiv-Nuklear), Pandemien, Streiks, Demonstrationen, Kriminalität, Amoklagen, Terrorismus etc., herangezogen werden kann.

FESTLEGEN DER ALARMIERUNGS-, MELDE- UND ESKALATIONSSTUFEN

Legen Sie für ihr Unternehmen einen gut durchdachten Alarmierungsplan fest, aus dem eindeutig hervorgeht,

WER? → WANN? → WEN?

verständigt. Bedenken Sie dabei auch stets die Zeiten außerhalb der regulären Kernarbeitszeit (nachts, Wochenende, feiertags).

1 WOHER KANN EINE EREIGNISMELDUNG KOMMEN?

Überlegen Sie sich, über welche Kanäle Sie eine Ereignismeldung erhalten können. Durch

- interne oder externe Stellen,
- technische Sicherheitssysteme (Brandmeldeanlagen etc.),
- Behörden oder andere Unternehmen (Bekennerschreiben, nachrichtendienstliche Erkenntnisse etc.) oder gar durch
- die Öffentlichkeit (Nachbarschaft, Presse- und Medienberichte etc.).

Diese Meldungen laufen an unterschiedlichen Stellen im Unternehmen auf und müssen gezielt weiterbearbeitet werden.

2 WIE ERFOLGT DIE MELDUNGSWEITERLEITUNG?

Im Idealfall laufen derartige Meldungen an einer zentralen Stelle 24/7 auf (Schichtdienstleitung, Rufbereitschaft, externe Notruf- und Serviceleitstelle etc.). Dies können je nach Ereignisfall ggf. auch unterschiedliche Stellen sein, sofern die betriebliche Organisation dies erfordert. Wichtig ist, dass allen Mitarbeitern dieser erste Anlaufpunkt bekannt ist.

Die entgegennehmende Stelle muss in der Lage sein, das Ereignis auf Plausibilität zu überprüfen und die Information anschließend entweder an die zuständige Fachabteilung oder direkt an einen (Notfall-/Krisen-)Beauftragten oder ggf. den Leiter des Krisenstabs weiterzuleiten.

Derartige Meldungen sollten stets schriftlich erfasst werden und deutlich als Tatsache oder Vermutung gekennzeichnet sein. Folgende Angaben sind notwendig:

- Wer meldet (Person, Stelle, Informationsherkunft)?
- Ursache/Auslöser?
- Ereignisort? Betroffene Bereiche?
- Erwartete Auswirkungen?

Von der zentralen Stelle werden erste Sofortmaßnahmen eingeleitet, wie z. B. bei Gefahr im Verzug die entsprechenden Rettungskräfte zu alarmieren (Polizei unter 110 oder Feuerwehr/Rettungsdienst unter 112), eine Gebäuderäumung auszulösen und die Meldung in die vordefinierte Meldekette gemäß Alarmierungsplan einzuspeisen.

3 ALARMIERUNG DER IN- UND EXTERNEN FACHABTEILUNGEN IM EREIGNISFALL

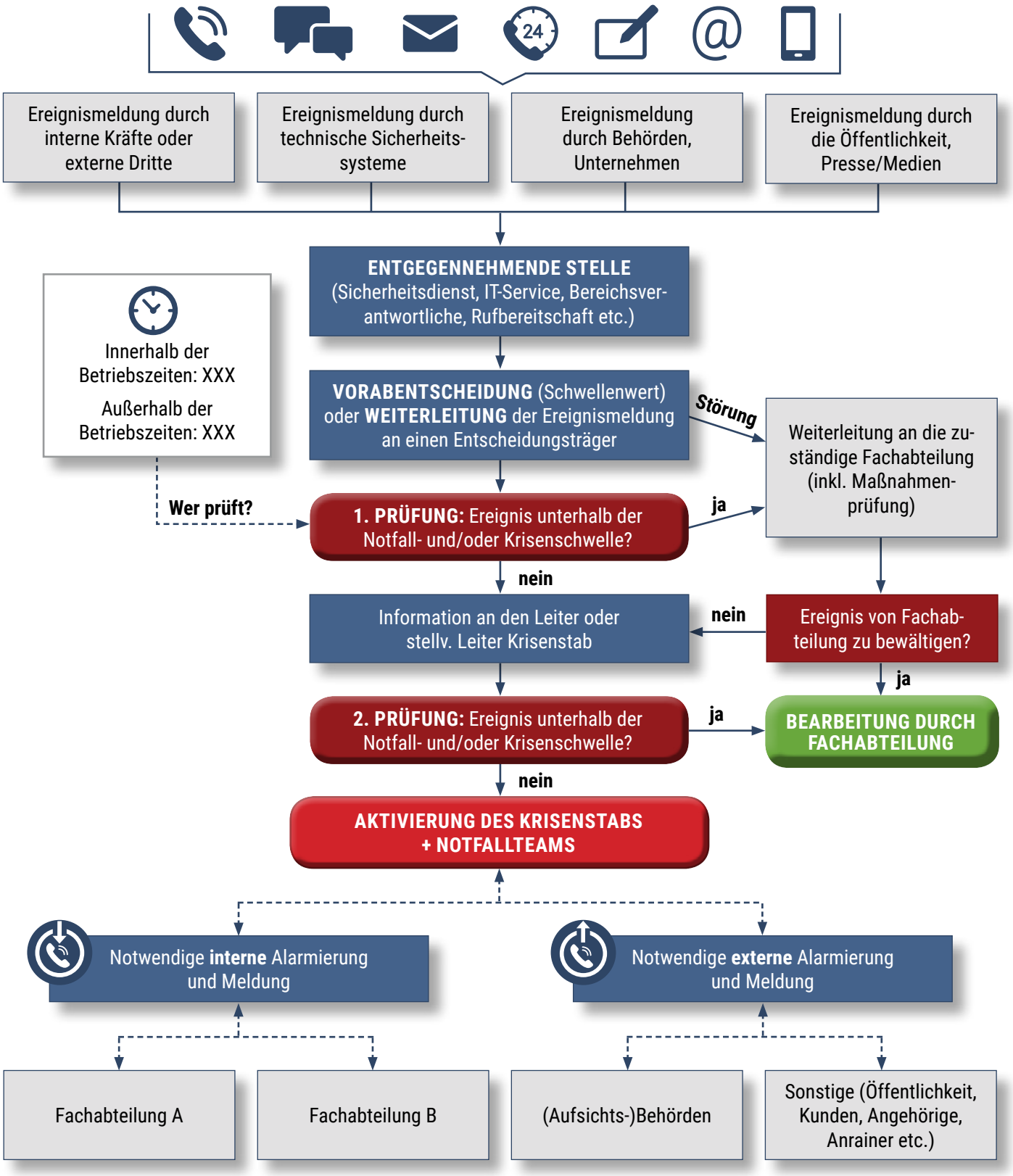
Sobald ein Ereignis einen gewissen Schwellenwert (Eskalationsstufe) übersteigt oder von der Stelle, die die Meldung entgegennimmt nicht final überprüft bzw. bearbeitet werden kann, wird die Meldung an die internen Entscheidungsinstanzen (Fachabteilungen, den (Notfall-/Krisen-)Beauftragten oder den Leiter des Krisenstabs) weitergeleitet. Diese prüfen anschließend, ob sich das Ereignis über die Fachabteilung im allgemeinen Arbeitsalltag bewältigen lässt oder ob es ein Ereignis größeren Ausmaßes ist, bei dem die entsprechende „besondere“ Aufbau- und Ablauforganisation des Unternehmens (Krisenstab) zum Tragen kommen sollte.

SCHWELLENWERTE / ESKALATIONSSTUFEN

STÖRUNG: Kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur geringem Schaden.

NOTFALL: Länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden.

KRISE: Im Wesentlichen auf das Unternehmen begrenzter verschärfter Notfall, der die Existenz des Unternehmens bedroht oder die Gesundheit oder das Leben von Personen beeinträchtigt.



Beispielhafte Meldekette im Alarmierungsfall

Die bis hierhin notwendigen Anrufe sind im normalen Arbeitsalltag noch zu bewältigen. Spätestens wenn der Krisenstab mit internen und externen Fachabteilungen einberufen wird, sollte dies jedoch von einer Stelle erledigt werden, die nicht zur konkreten Ereignisbewältigung benötigt wird. Natürlich auch, um wichtige Telefonleitungen nicht zu blockieren. Sie können an dieser Stelle beispielsweise - sofern vorhanden - eine Leitstelle/Leitwarte, eine Assistenz ›››

››› oder einen Verwaltungsmitarbeiter aktiv einbinden. Oder Sie arbeiten mit externen Dienstleistern zusammen, die derartige Meldungen steuern können (SaaS-Systeme - siehe nachfolgenden Artikel).

Definieren Sie für sich im Unternehmen ganz konkret, wie die Alarmierungs- und Meldewege sowie die einzelnen Eskalationsstufen zu den unterschiedlichsten Zeiten und bei den unterschiedlichsten Ereignissen aussehen könnten. Denn im Ereignisfall steht einzig und allein die Ereignisbewältigung im Vordergrund, die im Idealfall nicht durch zeitraubende (Fehl-)Alarmierungen beeinträchtigt werden sollte. Einen vorhanden Alarmierungsplan (inkl. Telefonnummern) sollten Sie stets auf dem aktuellsten Stand halten und in regelmäßigen Übungen einer entsprechenden Praxistauglichkeit unterziehen.

ALARMIERUNG IM KRISENFALL: SAAS-SYSTEME KÖNNTEN AUCH FÜR SIE EINE GUTE ALTERNATIVE SEIN

In Ereignissituationen und Krisenmomenten kommt es darauf an, dass verschiedene Personengruppen ihres Unternehmens schnellstmöglich mit den unterschiedlichsten Informationen versorgt oder lokationsbasiert alarmiert werden. Hierfür bieten SaaS-Systeme optimale und kostengünstige Lösungen an.

Wie läuft derzeit bei Ihnen im Unternehmen die Alarmierung im Ereignisfall? Ist es die Sekretärin, die Meldeketten abtelefoniert oder bedienen sie sich eines externen Dienstleisters?
Um im Ereignisfall schnell handeln zu können, muss das Fachpersonal und das Management umgehend alarmiert werden. Hierfür nutzen viele Unternehmen inzwischen die Vorteile moderner Telekommunikation. Das bedeutet: softwarebasierte Lösungen anstelle von Callcentern.

WAS BEDEUTET „SAAS“?

„Software as a Service“ (SaaS) ist ein Teilbereich des Cloud-Computings. Die Software und die IT-Infrastruktur werden bei einem externen IT-Dienstleister betrieben und von Ihnen als Dienstleistung genutzt. Somit schonen Sie interne Ressourcen und die Software kann auch unter höchstem Zeitdruck effizient für Sie arbeiten. Aufgrund der neuesten Datenschutzänderungen müssen Sie derartige Anbieter sorgfältig auswählen, da Mitarbeiter- und ggf. Kunden-/Fremdfirmendaten nicht mehr auf den eigenen Rechnern liegen. Besonderes Augenmerk muss hierbei auf der Auftragsdatenverarbeitung liegen, die vertraglich entsprechend geregelt sein muss.

ALARMIERUNGSBEISPIELE

Ein „Abklingeln“ der benötigten Personen und eine zügige und auf das Wesentliche beschränkte Informationsweitergabe sind im Alarmierungsfall essentiell, um das Ereignis best- und schnellstmöglich bewältigen zu können. Solche Systeme können zum Einsatz kommen bei:

- Einberufung des Krisenstabs mit einer entsprechenden Rückmeldeinformation ("Komme." / "Komme nicht." etc.)
- Wichtigen Informationen an die Führungsetage
- Einleitung standortübergreifender Telefonkonferenzen
- Benachrichtigungen an Techniker, Behörden und Medien
- Einrichtung von Info-Hotlines für Kunden, Geschäftspartner, Mitarbeiter, Bürger etc.

Dies alles sind Abläufe, die im Ereignisfall automatisiert ablaufen sollten, um Ressourcen und Zeit zu sparen.

DER VORTEIL FÜR UNTERNEHMEN

In erster Linie handelt es sich dabei um ein System, dass Ihnen im Ereignisfall auf Knopfdruck Hilfe leistet und

- unabhängig von der Infrastruktur ihres Unternehmens funktioniert,
- webbasiert ist und daher zügig implementiert werden kann sowie flexibel einsetzbar ist,
- eines geringen Investments bedarf und
- Individualisierungen zulässt (Definition von Nutzergruppen oder Alarmunterscheidungen etc.).

Neben der klassischen Alarmierungs- und Informationsweitergabe können auch weitere Möglichkeiten dieser Systeme die Bewältigung eines Ereignisses erleichtern:

- Aufgabenmanagement und Media-Monitoring
- Austausch von Dokumenten in Echtzeit
- Entwarnung
- Ereignisdokumentation

Diese Art von SaaS-Systemen können Sie aber nicht nur als Alarmierungs- und Informationsplattform im Ereignisfall nutzen, sondern auch im täglichen Geschäft für gezielte Kunden- oder Mitarbeiterinformationen verwenden. Beispielsweise zur Einsatzplanung, Terminbestätigung, Bestellabwicklung oder zur Information über Produktionsfortschritte.
Machen Sie sich darüber Gedanken, wie Sie außerhalb der Bürozeiten den Krisenstab alarmieren und ihre Kollegen informieren. Vielleicht sind derartige Alarmierungssysteme genau die richtige Lösung für ihr Unternehmen.

VERANSTALTUNGSSICHERHEIT MIT STRUKTUR UND PLAN

Jede Veranstaltung verfolgt einen konkreten Zweck, wie z. B. Verkauf, Unterhaltung, Erziehung oder Kultur. Dabei steht vor allem die Freude am geselligen Miteinander für die Besucher im Vordergrund, um aus einem Event eine gelungene Veranstaltung zu machen. Doch für den Veranstalter ist eine sichere und gelungene Veranstaltung mit einem hohen Planungs- und Organisationsaufwand verbunden – insbesondere im Hinblick auf die Sicherheitsorganisation und -konzeption.

> **„VON EINER VERANSTALTUNG IST DIE REDE, WENN AN EINEM ZEITLICH BEGRENZTEN UND ORGANISIERTEN TREFFEN EINE GRUPPE VON MENSCHEN TEILNIMMT. DIE VERANSTALTUNG HAT EINEN DEFINIERTEN ZWECK UND FINDET AN EINEM ODER MEHREREN VORDEFINIERTEN ORTEN STATT.**

Mit der Funktion als Veranstaltungsleiter (natürliche Person und nicht Unternehmen XY) bzw. Betreiber einer Versammlungsstätte sind nicht nur Rechte, sondern vor allem auch Pflichten verbunden. Diese ergeben sich u. a. aus dem Genehmigungsbescheid und der Risikobeurteilung. Vor jeder größeren Veranstaltung (Kongress, Messe, Tagung, Event etc.) empfiehlt es sich, sowohl rechtliche Vorgaben zu prüfen wie auch eine Risikobewertung durchzuführen, um der Verantwortung der behörden- und veranstalterseitigen sicherheitsrechtlichen Einschätzung gerecht zu werden. Diese Vorgaben, Risiken und Auflagen sollten in einem Sicherheitskonzept schriftlich festgehalten werden, um auf mögliche Gefahren- und Schadensereignisse gut vorbereitet zu sein - denn wer kennt die Veranstaltung besser als der Veranstalter?

Eine gesetzlich geregelte Verantwortung zur Erstellung von Sicherheitskonzepten außerhalb des § 43 Muster-Versammlungsstättenverordnung (MVStättV0), die für Versammlungsstätten mit mehr als 5.000 Besuchern oder bei besonderen Veranstaltungen gilt, gibt es nicht. Allerdings ergibt sich für den Veranstalter aus zivilrechtlichen Haftungsansprüchen (Organisationshaftung) eine Notwendigkeit zur Erstellung eines Sicherheitskonzepts, wenn die Veranstaltung in einer nicht genehmigten Versammlungsstätte stattfindet. Die behördliche Forderung nach einem Sicherheitskonzept kann sich auch durch das Überschreiten einer tolerierbaren Risikoschwelle ergeben.

Weitere rechtliche Vorgaben sind in den jeweiligen Landesgesetzen geregelt (Straßen- und Wegerecht, Baurecht, Ordnungsrecht, Immissionsschutz etc.). Daher sollte sich jedes Unternehmen bei Veranstaltungen, bei denen mehrere Personen teilnehmen, über die Sicherheitsaspekte Gedanken machen.

PLANUNGSSICHERHEIT DURCH EINEN BEHÖRDLICHEN GENEHMIGUNGSBESCHEID

Um Veranstaltungen auf einer soliden Grundlage aufzubauen, sollte die Genehmigungsbehörde (i. d. R. das Ordnungsamt) zeitnah über die geplante Veranstaltung und das Grobkonzept informiert werden, da diese ggf. weitere nützliche Informationen, Fristen und Hinweise zur Verfügung stellen kann, was wiederum zu mehr Planungssicherheit führt.

FOLGENDE PUNKTE SOLLTEN DURCH DEN VERANSTALTER IN EINER ENTWURFSFORM DER GENEHMIGUNGSBEHÖRDE SCHLÜSSIG DARGESTELLT WERDEN:

- ☐ Art und Ort (Größe und Lage) der Veranstaltung
- ☐ Zusatzflächen (Abstellflächen, Parkplätze etc.)
- ☐ Datum und Zeitraum der Durchführung (inklusive Auf-/Abbauzeiten)
- ☐ Parallelveranstaltungen, sofern bekannt (ggf. mit Einflüssen auf die eigene Veranstaltung)
- ☐ Zutrittsregelungen (Kartenverkauf etc.)
- ☐ Begehbarkeit der Veranstaltungsfläche
- ☐ Besucherzahl (gesamt und zeitgleich) sowie Alter und Besucherstruktur
- ☐ Besucheranreise (PKW, ÖPNV, Fahrrad etc.)
- ☐ VIPs und deren ggf. individuelle Schutzbedürftigkeit
- ☐ Wetterrisiken der Veranstaltung (auch im Hinblick auf An-/Abreise)
- ☐ Mögliche Störungen durch Zuschauerverhalten oder Dritte (kriminelle Handlungen)
- ☐ Erfahrungshintergrund des Veranstalters im Allgemeinen und konkret auf die Veranstaltung bezogen
- ☐ Ablaufplan (Höhepunkte)
- ☐ Geplante Anordnung (Bühne, Fahrgeschäfte, Stände, Toiletten etc.)
- ☐ Verwendung von Pyrotechnik und/oder Durchführung feuergefährlicher Handlungen
- ☐ eingesetzter Ordnungsdienst (Sicherheitsdienst)
- ☐ eingesetzter Sanitätsdienst
- ☐ ggf. weitere Veranstaltungsdienstleister

Die zuständige Behörde teilt die Veranstaltung daraufhin in eine entsprechende Risikoklasse ein und leitet daraus mögliche Auflagen ab, die mit dem Genehmigungsbescheid einhergehen. Ein Genehmigungsbescheid ist erforderlich und ersetzt nicht das abgestimmte Sicherheitskonzept, welches seitens der Behörden lediglich auf Plausibilität und Schlüssigkeit hin geprüft wird.

RISIKOBEURTEILUNG DER VERANSTALTUNG

Eine Risikobeurteilung umfasst alle Aspekte der Veranstaltungsplanung, um etwaige Schadensfälle und deren Eintrittswahrscheinlichkeit eingehend zu betrachten. Risikoquellen werden identifiziert, analysiert und bewertet, um Schutzmaßnahmen formulieren zu können, welche die nicht tolerierbaren Risiken angemessen bewältigen sollen.

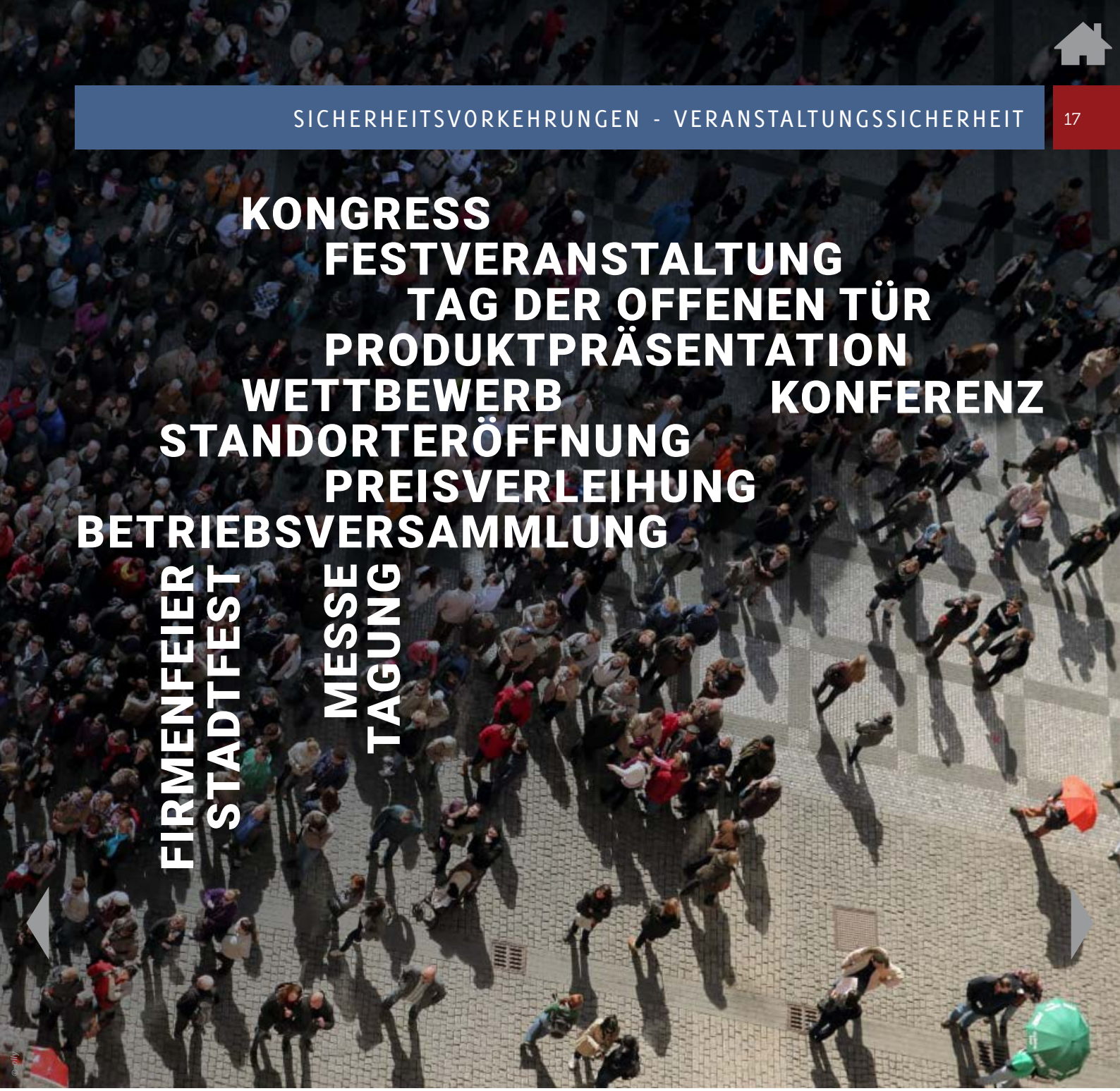
Dabei ist eine vollumfängliche Betrachtung der Risiken nur schwer möglich. Daher sollte die angedachte Veranstaltung in dem Organisations-/Planungsstab systematisch durchgesprochen werden, um alle Erfahrungen und das Fachwissen jedes Einzelnen einzubinden. Bei der Risikobeurteilung gilt es Standardgefährdungen ebenso zu betrachten wie individuell durch die Art der Veranstaltung bedingte Risiken.

Zu den Standardgefährdungen zählen:

- Wetter (Hitze, Kälte, Sturm, Hagel, Starkregen, Schnee, Glatteis etc.)
- gefährdete Orte (Einlass, Auslass, Bühne, Backstage-Bereich etc.)
- Besucherverhalten (Überwinden von Absperrungen, Gedränge, Erklettern von Aufbauten, Kriminalitätsdelikte, Emotionen etc.)
- Besucherstruktur (Anzahl an nicht selbstrettungsfähigen Personen etc.)
- Sanitätsbereich (Konsumverhalten, vermisste Personen, Massenerkrankungen etc.)
- Brandgefährdungen (Technik, Pyrotechnik, Gasflaschen etc.)
- technische Gefährdungen (Stromausfall, Austritt von Gefahrstoffen, Bauteile etc.)
- besucherrelevante Infrastruktur (Ver- und Entsorgungsausfälle, Versorgungsknappheit von Getränken, An- und Abreisekomplikationen etc.)
- VIPs (Demonstrationen, Gegenveranstaltungen, Emotionen, An-/Abreise etc.)

Die daraus resultierenden Risiken und Schutzmaßnahmen werden als Szenarien mit entsprechenden Gegenmaßnahmen und Verantwortlichkeiten niedergeschrieben.

Die Risikobeurteilung bildet einen Teil des Sicherheitskonzeptes einer Veranstaltung ab, welches mit den für



Sicherheit und Ordnung zuständigen Behörden (Ordnungsamt, Polizei, Feuerwehr und Rettungsdienst, ggf. Bauamt) in jedem Fall abgestimmt werden sollte.

Nur wenn Sie sich im Vorfeld einer Veranstaltung mit den möglichen Risiken und Gefährdungsszenarien vertraut machen, können Sie rechtzeitig Gegenmaßnahmen ergreifen, so dass einer gelungenen und sicheren Veranstaltung nichts im Wege steht.

JEDER VERANSTALTUNGSLEITER MUSS SICH BEREITS WÄHREND DER PLANUNGSPHASE EINGEHEND GEDANKEN ÜBER DIE SICHERHEIT VON PERSONEN, SACHWERTEN UND DER UMWELT MACHEN. DAHER EMPFIEHLT SICH STETS DIE ERSTELLUNG EINES SICHERHEITSKONZEPTES, WELCHES AUF GRUNDLAGE EINER VORAB DURCHGEFÜHRTEN RISIKOBEURTEILUNG ERSTELLT WIRD.

IN UNSEREM DOWNLOADBEREICH FINDEN SIE EINE KOSTENFREIE VORLAGE EINER „INHALTSÜBERSICHT VERANSTALTUNGS-SICHERHEITSKONZEPT“ SOWIE WEITERE NÜTZLICHE LITERATUR ZUM THEMA „VERANSTALTUNGSSICHERHEIT“, U. A. DIE ERGEBNISSE DES FORSCHUNGSPROJEKTES „BASIGO - BAUSTEINE FÜR DIE SICHERHEIT VON GROSSVERANSTALTUNGEN“, AUS DEM BAUSTEINE AUCH IM ARTIKEL VERSCHRIFTLICHT WURDEN.

INTERVIEW MIT DENNIS VOSTEEN ZUM THEMA „SICHERHEIT AUF VERANSTALTUNGEN“

ZUR PERSON: Dennis Vosteen ist ausgebildeter Zugführer von Einsatzeinheiten, Rettungssanitäter und Feuerwehrmann und derzeit als Sicherheitsberater bei der PSC Private Security Company GmbH in München tätig. Als wissenschaftlicher Mitarbeiter hat er bei der Branddirektion München am Forschungsprojekt „BaSiGo - Bausteine für die Sicherheit von Großveranstaltungen“ mitgearbeitet und ist einer der Hauptautoren des Standardwerks „Veranstaltungssicherheit“, das vom Bayerischen Innenministerium zur Anwendung empfohlen ist.

BEI VERANSTALTUNGEN EGAL WELCHER ART GILT NACH AUFFASSUNG DES BUNDESGERICHTSHOFS: „DIE SICHERHEIT DER BESUCHER HAT ABSOLUTEN VORRANG VOR WIRTSCHAFTLICHEN INTERESSEN DES VERANSTALTERS“. WER MUSS SICH BEI EINER VERANSTALTUNG UM SICHERHEITSASPEKTE KÜMMERN?

Grundlegend ist jeder Veranstalter für die eigene Veranstaltung verantwortlich. Hierzu gehört natürlich - unabhängig von der Größe der Veranstaltung - das Thema Sicherheit. Veranstalter kann eine natürliche oder eine juristische Person sein. Handelt es sich um eine juristische Person wie ein Unternehmen oder einen Verein, muss festgelegt werden, welche natürliche Person den Veranstalter vertritt. Die Vorstandsvorsitzende oder der Sachbearbeiter werden dann explizit als Veranstaltungsleitung benannt. Die Veranstaltungsleitung übernimmt die Rechte und Pflichten für die Veranstaltung. Eine Veranstaltungsleitung kann auch extern vergeben werden. Es muss jedoch bedacht werden, dass diese immer erster Ansprechpartner der Behörden bei Fragen in Bezug auf die Veranstaltung ist und ggf. nicht von Anfang an in der Ideen-, Planungs- und Umsetzungsphase eingebunden war. Dies kann zu Wissensverlusten führen. Neben der Sicherheit ist der Veranstalter ebenfalls verpflichtet, den Arbeitsschutz für seine Mitarbeiterinnen und Mitarbeiter sicherzustellen bzw. auf dessen Einhaltung bei Subunternehmen zu achten.

Sollte die Veranstaltung in einer baulichen Anlage stattfinden, ist der Betreiber dieser Anlage für die Sicherheit mitverantwortlich. Insbesondere ist der Betreiber in seiner Örtlichkeit für die notwendigen Anlagen, Einrichtungen oder Vorrichtungen verantwortlich und muss intervenieren, wenn diese nicht betriebsfähig sind oder Betriebsvorschriften nicht eingehalten werden. Allerdings kann diese Betreiberverantwortung an den Veranstalter abgegeben werden.

Letztlich sind die Besucherinnen und Besucher für ihre eigene Sicherheit verantwortlich. Sie sollten beispielsweise bei hohen Temperaturen ausreichend (alkoholfreie) Getränke zu sich nehmen, sich der Witterung entsprechend kleiden oder auf einem Volksfest festes Schuhwerk den Flipflops vorziehen. Der Veranstalter kann dieses Verhalten in Besucherinformationen beeinflussen, indem er darauf hinweist (Einladungen, Ankündigungen, Auftritte in sozialen Netzwerken, Aushang von „Veranstaltungsregeln“ etc.), sollte aber grundsätzlich mit arglosen Besuchern rechnen.

UNFÄLLE UND SICHERHEITSRELEVANTE EREIGNISSE KANN ES BEI JEDER ART UND GRÖSSE VON VERANSTALTUNGEN GEBEN. IST ES DAHER NICHT ESSENTIELL, DASS SICH ALLE DIE FRAGE NACH SICHERHEITSASPEKTEN IM BEREICH DER ABWEHR VON DURCH ÄUSSERE EINWIRKUNG VERURSACHTE GEFAHREN STELLEN?

Grundsätzlich sollte jeder Mensch im alltäglichen Leben auf seine eigene Sicherheit achten und in der Lage sein, anderen Menschen zu helfen, beispielsweise bei einem Unfall. Bei einer Veranstaltung bleibt diese Verantwortung dennoch beim Veranstalter: Der Veranstalter muss dafür sorgen, dass alle Menschen die Veranstaltung sicher erleben können und sich im Notfall schnell selbst retten können. Sollte die Selbstrettungsfähigkeit nicht mehr vorhanden sein, muss der Veranstalter dafür Sorge tragen, dass einer betroffenen Person geholfen wird.

Wichtig für den Veranstalter ist daher die richtige Auswahl von Dienstleistern, die auch entsprechende Erfahrungswerte mit der Veranstaltungsgröße haben sollten.

Darüber hinaus kann sich ein Veranstalter das Leben stark erleichtern, wenn er frühzeitig mit den beteiligten Akteuren plant. Es bleibt dann genug Zeit, Probleme gemeinsam anzugehen und die einzelnen Akteure wissen, an wen sie sich bei sicherheitsrelevanten Fragestellungen wenden können.

ZIELT DIESE SICHERHEIT AUF DEN EINZELNEN ODER DIE GESAMTHEIT AB?

Sicherheit bezieht sich immer auf die Gesamtheit der anwesenden Personen - es gibt keine Besucher 1. und 2. Klasse oder einen Unterschied zwischen Besuchern und Mitarbeitern. Dennoch kann der Veranstalter - ggf. in Abstimmung mit den Genehmigungsbehörden - für sich definieren, was tolerierbar ist. Bei einem Stehempfang eines mittelständischen Handwerksunternehmens mit 50 Personen bedarf es in der Regel keines Sanitätsdienstes. Sollte ein

Besucher medizinische Hilfe benötigen, kann dies durch Ersthelfer und Erste-Hilfe-Material (z. B. KFZ-Verbandskasten) sichergestellt werden. Das Eintreffen des Rettungsdienstes kann allerdings - je nach Region - bis zu 15 Minuten dauern. Ist dies tolerierbar? In der Regel schon. Handelt es sich jedoch um einen Stehempfang der Vorstandsvorsitzenden der im DAX vertretenen Unternehmen, sollte aufgrund der möglichen Auswirkungen schnell qualifiziertes Personal anwesend und somit vor Ort sein.

Ebenfalls muss die Außenwirkung betrachtet werden: Kommt bei einem Volksfest an einem Abend mehrmals der Rettungsdienst, um Patienten abzuholen, wird dies allgemein als normal angesehen. Sollte es sich um eine Unternehmensfeier in der gleichen Größe und mit Kindern handeln, ist die öffentliche Bewertung anders.

Letztlich muss jeder Veranstalter - losgelöst von eventuellen Auflagen einer Behörde - Kosten und Nutzen abwägen. Oftmals sind die Kosten allerdings gar nicht so hoch wie befürchtet und die negativen Auswirkungen bei Schadenseintritt sehr viel höher.

WIE VIEL VERANSTALTUNGSSICHERHEIT IST AUS IHRER SICHT SINNVOLL?

Das Ziel muss immer sein, Veranstaltungen zu ermöglichen, anstatt sie zu verhindern. Ermöglichen bedeutet, dass die Menschen die Veranstaltung „sicher“ erleben können. Gefährdungen dürfen nicht ignoriert werden und im Fall der Fälle muss diesen zielgerichtet begegnet werden können. Die beste Form zu ermitteln, was „sinnvoll“ ist, ist eine Gefährdungsanalyse durchzuführen. Ein großes Wort, aber im Prinzip bedeutet es nur „Was kann passieren?“ und „Wie wahrscheinlich ist das Risiko, dass es eintritt?“.

In einem zweiten Schritt müssen dann die Fragen gestellt werden „Was sind die Auswirkungen, wenn es passiert?“ und „Wie reagiere ich, wenn es passiert?“.

Gerade für eine Gefährdungsanalyse und ein daraus folgendes Sicherheitskonzept kann ein externes Beratungsunternehmen unterstützend tätig werden. Allerdings gibt es eine Vielzahl an Anbietern mit unterschiedlichsten Ausbildungen und Erfahrungswerten. Es sollte daher unbedingt auf die Referenzen sowie die Erfahrungswerte und das Ausbildungsprofil der Berater des Unternehmens geachtet werden.

WELCHE GEFAHREN UND ENTWICKLUNGEN SEHEN SIE KÜNFTIG FÜR VERANSTALTUNGEN?

Die Sicherheit von Veranstaltungen ist ein Thema von allgemeingesellschaftlicher Relevanz - nahezu jeder Mensch besucht jedes Jahr die unterschiedlichsten Veranstaltungen. Das Gefühl des gemeinsamen Erlebens ist ein Trend, so dass immer neue Ideen für Veranstaltungen entstehen. Die Geschehnisse bei der Loveparade in Duisburg haben das Thema Veranstaltungssicherheit auf die politische Agenda und durch die Medien in das Bewusstsein der Bevölkerung gerückt - in der Folge konnten bereits viele Verbesserungen erreicht werden.

Als Gefahr sehe ich, dass zum einen die Geschehnisse von Duisburg in Vergessenheit geraten könnten und dem Thema Sicherheit nicht mehr die notwendige Aufmerksamkeit zuteilwird. Zum anderen, dass das Thema Sicherheit immer nur für Großveranstaltungen gesehen wird. Genauso wichtig sind aber die Veranstaltungen mit weniger Personen, die aber natürlich nicht den Aufwand und Umfang einer Großveranstaltung erfordern.

WELCHER SICHERHEITSRELEVANTEN FRAGESTELLUNG GILT ES SICH VOR VERANSTALTUNGSBEGINN ZU STELLEN?

Die wichtigste Frage am Beginn aller sicherheitsrelevanten Überlegungen ist: „Wer macht was wann und warum?“ oder anders gesagt: Am Anfang ist es immer das Wichtigste, die Aufgaben und Zuständigkeiten klar zu benennen und dies zu kommunizieren - am besten schriftlich. Begrifflichkeiten müssen darüber hinaus klar definiert werden - es soll schließlich jeder wissen, was die Aufgaben des „chief security supervisor on duty“ sind oder was mit dem „Ausgang Nord 1“ oder den „Feuerlöschgerätschaften am Schuppen 5“ gemeint ist.

HAND AUFS HERZ: SICHERHEIT SOLLTE ALSO BEI JEDER ART VON VERANSTALTUNG GRUNDSÄTZLICH BEDACHT WERDEN.

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.

MESSE

SECURITY ESSEN
WELTLEITMESSE FÜR ZIVILE SICHERHEIT

Vom 25.09. - 28.09.2018 laden 1.000 Aussteller aus 45 Nationen in die nach Themen aufgebauten Messehallen (Zutritt, Mechatronik und Systeme, Dienstleistungen, Video, Brand und Einbruch, Perimeter sowie Cyber-Sicherheit und Wirtschaftsschutz) nach Essen ein.

Die Messe Essen sucht alle 2 Jahre Antworten auf aktuelle Herausforderungen und Fragestellungen aus Wirtschaft und Gesellschaft an die Sicherheitsbranche - von neuen Lösungen der Smart Home Security und der Digitalisierung über intelligente Drohnensysteme bis hin zu innovativen Konzepten zur Veranstaltungssicherheit.

Im Rahmen der SECURITY findet u. a. die Cyber-Security-Konferenz statt, die die Digitalisierung in den Vordergrund rückt. Weitere Bestandteile des Rahmenprogramms sind das „Public Security Forum“, in dem Live-Szenarien für den Schutz des öffentlichen Raumes gezeigt werden und der Gesprächskreis Innere Sicherheit mit Teilnehmern aus Polizei, Wissenschaft, Justiz, Politik, Kommunen und der Sicherheitswirtschaft.

Somit erhalten Sie neben den Messeständen auch die Möglichkeit, sich thematisch mit dem Thema Sicherheit auseinanderzusetzen.

TOOL

ERKENNEN SIE SICHERHEITSPROBLEME UND -LÜCKEN AUF WEBSEITEN IM SCHNELLTEST

Über 90 % der Cyberangriffe erfolgen auf Sicherheitslücken in der Standardsoftware. Untersuchen Sie ihre Webseite(n) regelmäßig auf Schwachstellen? Der Siweco Check ermöglicht es Ihnen, kostenfrei ihre Webseiten auf potentielle Schwachstellen zu überprüfen und somit Sicherheitslücken rechtzeitig aufzudecken, bevor diese zum Ziel von Angriffen werden können. Siweco ist ein durch die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministerium für Wirtschaft und Energie (BMWi) gefördertes Gemeinschaftsprojekt von eco – dem Verband der Internetwirtschaft e. V. sowie der Ruhr-Universität Bochum mit Unterstützung des CMS Garden e. V. und dem Bochumer IT-Security Startup „Hackmanit“.

Registrieren Sie sich kostenfrei auf der Webseite und lassen Sie täglich bis zu 25 Domains automatisch prüfen! Sie erhalten zusätzlich Sicherheitshinweise und Informationen zu Sicherheitslücken und weitere Hilfs- und Informationsangebote, die auch mit wenig Hintergrundwissen einen hohen Nutzwert haben.

SIWECOS
Auf der sicheren Seite

SIWECO (Sichere Webseiten und Content) hat sich zum Ziel gesetzt, die Webseitensicherheit kleiner und mittelständischer Unternehmen langfristig zu erhöhen.

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.