AUSGABE 29

SICHERHEIT. DAS FACHMAGAZIN.

SICHERHEIT AUF DEN PUNKT GEBRACHT.

SIUS Consulting

KOMPETENZPARTNER

Ihre Softwarelösung für modernes Notfall- und Krisenmanagement

Unsere webbasierte Software „Notfall- und Krisenmanager“ bietet Ihnen die perfekte Grundlage für den schnellen und einfachen Aufbau eines Notfall- und Krisenmanagements oder die digitale Transformation Ihres bestehenden Notfall- und Krisenmanagementsystems.

NOTFALL- UND KRISENMANAGER

- **Keine Installation erforderlich.**
- **In wenigen Minuten startklar.**
- **Made & hosted in Germany.**

www.NKM-Software.de

HINWEISTELEFON: IHRE ANLAUFSTELLE GEGEN EXTREMISMUS, TERRORISMUS UND SPIONAGE

>>> So handeln Sie richtig bei Verdachtsfällen <<<

Das Bundesamt für Verfassungsschutz ist gesetzlich beauftragt, Extremismus und Terrorismus zu bekämpfen sowie Spionage aufzudecken. Der Umgang mit Verdachtsfällen in diesen sensiblen Bereichen erfordert Besonnenheit, strukturierte Abläufe und eine enge Kooperation mit den zuständigen Behörden.

Durch Pre-Employment Checks, Hinweisgebersysteme und die zunehmende Sensibilisierung für Themen wie Extremismus, Terrorismus und Spionage steigt die Aufmerksamkeit innerhalb der Bevölkerung und bei Kollegen.

Doch wie sollte man sich verhalten, wenn man beunruhigende Beobachtungen oder Auffälligkeiten wahrnimmt?

Was tun, wenn die Situation nicht eigenständig beurteilt oder der Sachverhalt mit einer fachlich versierten Stelle geklärt werden soll?

IN SOLCHEN FÄLLEN KÖNNEN SIE SICH VERTRAULICH AN DIE ZUSTÄNDIGEN SICHERHEITSBEHÖRDEN WENDEN:

Das Bundesamt für Verfassungsschutz (BfV) für Verdachtsfälle im Bereich **Extremismus** und **Spionage**.

Das Bundeskriminalamt (BKA) oder die Polizei für akute Verdachtsfälle im Bereich **Terrorismus**.

> DER UMGANG MIT VERDACHTSFÄLLEN IN DEN BEREICHEN TERRORISMUS, EXTREMISMUS UND SPIONAGE VERLANGT EINEN PROFESSIONELLEN UND RECHTLICH EINWANDFREIEN ANSATZ.

Unterstützen Sie die Sicherheitsbehörden und nehmen Sie vertraulich Kontakt auf, wenn Sie:

- Kenntnis von Planungen von Gewalt- oder Sabotageakten oder Terroranschlägen haben.
- Personen kennen, die sich an solchen Planungen beteiligen.
- beobachten, dass in Ihrer Umgebung für Terror und Gewalt geworben wird.
- wahrnehmen, dass sich Personen in Ihrem Umfeld radikalisieren.
- hierzulande oder bei einer Auslandsreise von Unbekannten angesprochen und Informationen verlangt werden.
- oder Ihre Angehörigen von einem Nachrichten- oder Sicherheitsdienst unter Druck gesetzt werden.
- Kenntnis von Spionagetätigkeiten gegen Deutschland haben.

Wichtig ist, dass – sofern keine Gefahr im Verzug besteht – bestehende interne Meldewege eingehalten werden. Verdachtsmomente sollten dabei stets datenschutzkonform und auf der Grundlage objektiver Fakten dokumentiert werden.

> **HINWEISE ZUR ABWEHR VON SPIONAGE ODER TERRORISMUS KÖNNEN DAZU BEITRAGEN, LEBEN ZU SCHÜTZEN UND DIE SICHERHEIT DEUTSCHLANDS ZU STÄRKEN.**

Grundsätzlich ist ein diskreter Umgang mit Sachverhalten und Informationen erforderlich. Verdächtigte Personen dürfen keinesfalls eigenmächtig mit dem Verdacht konfrontiert werden, da dies sowohl rechtliche Konsequenzen nach sich ziehen als auch künftige Ermittlungen erheblich behindern kann. Achten Sie darauf, den rechtlichen Rahmen einzuhalten, Maßnahmen verhältnismäßig zu gestalten und die Grundrechte aller Beteiligten zu respektieren.

! VIELE BEHÖRDEN BIETEN UNTERNEHMEN UND INSTITUTIONEN PRÄVENTIONSPROGRAMME SOWIE BERATUNGSLEISTUNGEN ZUM PROFESSIONELLEN UMGANG MIT EXTREMISMUS, TERRORISMUS UND SPIONAGE AN.

DAS BUNDESAMT FÜR VERFASSUNGSSCHUTZ (BFV) HAT EIN HINWEISTELEFON EINGERICHTET, ÜBER DAS SIE ENTSPRECHENDE MELDUNGEN ABGEBEN KÖNNEN.

0228 / 99 792 6000 oder
030 / 18 792 6000

hinweise@bfv.bund.de

BANALE STOLPERSTEINE: WARUM KRISENSTÄBE BEREITS ZU BEGINN SCHEITERN

> DIESES BEISPIEL ZEIGT DEUTLICH: MANGELNDE VORBEREITUNG IST NICHT NUR ÄRGERLICH, SONDERN KANN SCHWERWIEGENDE KONSEQUENZEN HABEN.

Ein Krisenereignis wird häufig aus unterschiedlichsten Quellen erkannt: durch technische Anlagen, persönliche, telefonische oder schriftliche Übermittlung oder durch eigenes Erleben. Diese Meldung muss aufgenommen, als Krisenereignis außerhalb des regulären Alltags erkannt und an die zuständigen Stellen weitergeleitet werden. Im Rahmen der Eskalation sollte dann ein Entscheidungsträger die Einberufung des Krisenstabs veranlassen. Anschließend werden die Krisenstabsmitglieder alarmiert, die sich persönlich oder hybrid in den dafür definierten Räumlichkeiten versammeln.

DOCH BIS ZU DIESEM PUNKT SCHEITERN VIELE BETRIEBE, WEIL DIE ZUGRUNDE LIEGENDEN PROZESSE OFT NICHT KLAR, TRANSPARENT ODER DURCHGÄNGIG DEFINIERT SIND.

Eine detaillierte Analyse dieser Unzulänglichkeiten würde jedoch den Rahmen dieses Artikels sprengen. Stattdessen soll hier der Fokus auf die typischen Fehler gelegt werden, die während der folgenden ersten Schritte der Krisenstabsarbeit auftreten.

Ein lebhaftes Praxisbeispiel:

WENN DER KRISENSTAB BEREITS AM ANFANG SCHEITERT

Der COO, Herr Meyer, sitzt gemütlich zu Hause, als sein Handy klingelt. Ein Vorfall hat sich ereignet, und nach einer holprigen Telefonkette, die quer durch das Unternehmen ging, wird ihm die Entscheidung überlassen: Der Krisenstab muss einberufen werden. Herr Meyer löst über eine spezielle App die Alarmierung des Krisenstabs aus und macht sich gegen 21:20 Uhr auf den Weg zur Firma – nur fünf Minuten entfernt. Doch schon hier beginnt das Chaos.

Am Werkstor angekommen, prallt er gegen die Realität: Nach 20:00 Uhr ist der Zutritt nur der Geschäftsführung gestattet. Der externe Sicherheitsdienst wurde nicht über das Eintreffen des Krisenstabs informiert. Nach mehreren Telefonaten öffnet sich endlich das Tor.

Im Gebäude scheitert Herr Meyer erneut: Seine Zugangskarte funktioniert in dem Gebäudebereich nicht. Glücklicherweise hilft ihm die Reinigungskraft weiter. Doch was ihn im Raum erwartet, ist alles andere als eine professionelle Arbeitsumgebung: Ein kleiner, stickiger Raum mit Platz für maximal acht Personen. Auf dem Tisch stehen noch die schmutzigen Kaffeetassen des letzten Meetings. Die Fenster sind bei 2 °C Außentemperatur weit geöffnet, und von technischer oder organisatorischer Ausstattung fehlt jede Spur. Weder Stifte noch Blöcke, kein Flipchart, kein Monitor. Im Flur gibt es zwar einen Schrank, der angeblich Equipment enthält, doch niemand hat den passenden Schlüssel dafür.

Nach und nach trudeln die Krisenstabsmitglieder ein. Einige plaudern über erste Informationen, die sie aufgeschnappt haben, andere sitzen schweigend da und wirken unsicher. Es herrscht Unruhe, bis die Assistentin der Geschäftsführung fragt: *„Wie machen wir jetzt weiter?“* Ratlose Gesichter. Rollen müssen definiert werden – klar, aber welche? Leitung, Kommunikation, HR und IT sind klar. Doch was ist mit der Dokumentation? *„Das sollten wir festhalten.“*, wirft jemand ein. *„Aber womit? Papier? Laptop? Gibt es ein Protokollschema?“* Keiner weiß es genau. Und so verstreichen die nächsten Minuten mit improvisierten Versuchen, eine Struktur zu schaffen.

Vielleicht wirkt dieses Szenario wie eine Komödie, aber genau solche Situationen passieren in Unternehmen, die ihre Notfall- und Krisenprozesse weder klar definiert noch regelmäßig geübt haben. Jede verschwendete Minute kann entscheidend sein – sei es für die Schadensminimierung, die Wiederaufnahme des Geschäftsbetriebs oder die Reputation.

> ES GEHT NICHT IMMER UM LEBEN UND TOD, ABER JEDE SEKUNDE, IN DER EIN KRISENSTAB SICH „VOR DIE LAGE BRINGEN“ KÖNNTE, ZÄHLT.

Schon kleine Versäumnisse können die Arbeit des Krisenstabs erheblich behindern. Die Grundlagen – von der Definition eines Krisenstabsraums bis zur klaren Rollenverteilung – sollten nicht nur theoretisch vorhanden, sondern auch praktisch erprobt und allen Beteiligten bekannt sein. Regelmäßige Übungen und Checklisten können helfen, Schwachstellen frühzeitig zu erkennen und abzustellen, bevor eine echte Krise eintritt.

1. DER KRISENSTABSRAUM

Der Krisenstabsraum ist die Grundlage effektiver Zusammenarbeit. Doch bereits hier treten die ersten Probleme auf:

- **Wurde der Raum überhaupt definiert?** Idealerweise existiert auch eine Ausweichfläche, falls der vorgesehene Raum nicht verfügbar ist.
- **Ist der Raum allen Krisenstabsmitgliedern bekannt?** Wurde die Information bei der Alarmierung klar kommuniziert?
- **Zufahrts- und Zutrittsberechtigung:** Haben alle alarmierten Mitglieder 24/7 Zugang zu den Räumlichkeiten?
- **Kapazität des Raums:** Ist der Krisenstabsraum für die Anzahl der Personen geeignet?
- **Grundausstattung:** Gibt es eine Grundausstattung wie Stifte, Blöcke, ein Flipchart oder ein Whiteboard (inklusive Stiften)? Ist eine Videokonferenzmöglichkeit vorhanden?
- **Räumliche Bedingungen:** Können Temperatur und Licht an die Bedürfnisse der Krisenstabsmitglieder angepasst werden?

2. VERANTWORTLICHKEIT UND ZUSTÄNDIGKEITEN

Wenn der Krisenstab sich nach und nach im Raum einfindet, sollte die Rollenverteilung klar sein. Häufig mangelt es jedoch an Transparenz in diesem Bereich:

- **Kenntnis der Rollen:** Wissen alle Mitglieder, welche Rolle sie im Krisenstab einnehmen?
- **Besetzung von Rollen:** Sind alle erforderlichen Rollen besetzt, oder muss eine Nachalarmierung erfolgen?
- **Doppelte Besetzung:** Gibt es Rollen, bei denen aufgrund eines hohen Arbeitsaufwands eine doppelte Besetzung sinnvoll wäre?
- **Nicht benötigte Personen:** Sind Personen anwesend, die derzeit keine Rolle haben und stattdessen für eine spätere Zweitbesetzung eingeplant werden könnten?
- **Klarheit über Zuständigkeiten:** Ist jedem bewusst, welche Verantwortlichkeiten mit seiner Rolle verbunden sind und welche Rolle die anderen Mitglieder im Raum innehaben? >>>

3. ARBEITSBEREITSCHAFT UND ARBEITSAUSSTATTUNG

Sobald die Rollen verteilt sind, sollte der Krisenstab arbeitsfähig sein. Doch auch hier gibt es oft vermeidbare Probleme:

- **Hilfsmittel und Dokumente:** Sind alle notwendigen Unterlagen, Checklisten und Ressourcen physisch oder digital verfügbar? Fehlen Links, Passwörter oder Schlüssel? Und werden diese Hilfsmittel und Dokumente überhaupt eingesetzt, oder bleiben sie ungenutzt, obwohl sie bereitstehen?
- **Sitzordnung:** Passt die Sitzordnung zu den definierten Rollen? Gibt es Personen, die aufgrund ihrer Aufgaben eine ruhigere Ecke benötigen oder nahe bei einer anderen Person sitzen sollten?
- **Störfaktoren:** Gibt es ausreichend „Ruhe“ im Raum? Oder werden die Mitglieder durch ständigen Personenverkehr, neugierige Blicke von außen oder die sichtbare Präsenz des Ereignisses abgelenkt?

4. LAGEERFASSUNG

Bis zu diesem Punkt sind seit dem Ereignis zahlreiche Minuten bis hin zu einer halben Stunde vergangen – eine wertvolle Zeit, in der kaum etwas zur tatsächlichen Lagebewältigung unternommen wurde. Der Anfang jeder Krise ist natürlich geprägt von der sogenannten „Chaosphase“, in der Unsicherheiten, Informationsmangel und Unklarheit dominieren. Der Begriff „Chaos“ bezieht sich hier weniger auf die Arbeit des Krisenstabs als vielmehr auf die unübersichtliche Informationslage.

Ein zentraler Schritt in der Lagebewältigung ist die erste Lageeinschätzung bzw. Lageerfassung.

- **Kommunikation im Krisenstab:** Reden alle Mitglieder geordnet, oder sprechen sie durcheinander? Sind die Informationsquellen und Inhalte klar definiert? Wird die Frage „Wo stehen wir?“ zu Beginn gestellt?
- **Umgang mit ersten Informationen:** Werden die anfänglichen Informationen kritisch hinterfragt? Ist allen bewusst, dass diese oft ungenau, spekulativ oder vermischt mit Annahmen und Erstmaßnahmen sind?
- **Visualisierung der Informationen:** Werden die vorhandenen Informationen übersichtlich und visuell dargestellt, sodass eine Fortschreibung der Lage möglich ist? Gibt es dafür geeignete Hilfsmittel wie Whiteboards, Flipcharts oder digitale Tools? Wer übernimmt das?
- **Dokumentation:** Werden alle verfügbaren Informationen, Entscheidungsgrundlagen und Maßnahmen systematisch dokumentiert? Ist klar, wer diese Aufgabe übernimmt?
- **Priorisierung:** Werden entscheidende Informationen identifiziert/eingeholt oder wird die Zeit mit unwichtigen Details verschwendet?
- **Kommunikationswege:** Ist definiert, wer welche Informationen weiterleitet? Sind die Kommunikationskanäle innerhalb des Stabs, ins Unternehmen und nach außen klar und für alle zugänglich?

> **DIE LAGEBEWÄLTIGUNG IN EINER KRISE HÄNGT MASSGEBLICH VON DER FÄHIGKEIT DES KRISENSTABS AB, STRUKTUR INS CHAOS ZU BRINGEN.**

jamulart - stock.adobe.com

Es wäre fatal zu glauben, man könne dies „einfach so“ souverän aus dem Ärmel schütteln. Oder, um es anders zu sagen: Ein Feuerwehrmann weiß zwar grundsätzlich, wie ein Feuer gelöscht wird, aber ohne die richtige Ausrüstung, Struktur und Übung wird selbst das einfachste Szenario zur Herausforderung.

Erst ab diesem Punkt beginnt die eigentliche Bewältigung eines Notfalls oder einer Krise im Rahmen der Stabsarbeit – ein Prozess, der weit mehr Herausforderungen birgt als die hier skizzierten ersten Minuten.

DIE LEHRE AUS DER GESCHICHTE

Ein funktionierender Krisenstab braucht mehr als nur gute Absichten. Ohne klare Prozesse, eine verlässliche Infrastruktur und ein geschultes Team endet die Krise schnell im Chaos. Nur wer Notfall- und Krisenmanagement ganzheitlich betrachtet und alle Aspekte – von der Alarmierung bis zur Nachbereitung – systematisch plant, kann die skizzierten Situationen vermeiden und Ereignisse souverän bewältigen.

*Beispiel einer Softwarelösung im Notfall- und Krisenmanagement: **Der „Notfall- und Krisenmanager“ von SIUS Consulting®***

DIGITALISIERUNG IM NOTFALL- UND KRISENMANAGEMENT: WO GEHT DIE REISE HIN?

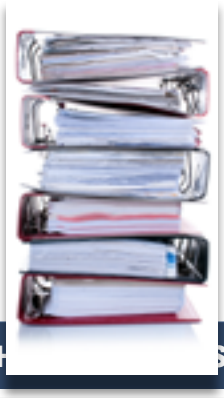
Unternehmen, Behörden und Organisationen müssen sich in einer zunehmend komplexeren Welt auf unterschiedlichste Notfall- und Krisenszenarien vorbereiten. Dabei stehen stets drei Schutzziele im Vordergrund: der Schutz von Leben, der Umwelt und von Sachwerten. Um diese Aufgaben zu bewältigen, setzen viele Betriebe auf moderne Softwarelösungen, die den gesamten Prozess des Notfall- und Krisenmanagements – von der Vorbereitung über die Bewältigung bis hin zur Auswertung – digital unterstützen und abbilden.

Im Ernstfall zählt jede Minute. Alarm- und Meldewege müssen funktionieren, Entscheidungsprozesse greifen, und relevante Informationen sollten für alle Beteiligten möglichst schnell verfügbar sein. Ob Naturkatastrophen, großflächige Stromausfälle oder Cyberangriffe – Notfälle und Krisen können in unterschiedlichsten Formen auftreten und erfordern flexible, gut aufeinander abgestimmte Gegenmaßnahmen. Dabei sind an vielen Ereignisfällen nicht nur interne Teams, sondern auch (Aufsichts-)Behörden sowie weitere interne und externe Stakeholder beteiligt. Eine lückenlose Dokumentation sämtlicher Schritte und Entscheidungen ist daher unverzichtbar. Um Menschenleben zu schützen, Umweltschäden zu begrenzen und Sachwerte zu erhalten, müssen Informationen in Echtzeit verfügbar sein und kompetent bewertet werden.

STATUS QUO IM NOTFALL- UND KRISENMANAGEMENT

Trotz der offensichtlichen Relevanz wird Krisenmanagement in vielen Organisationen immer noch stiefmütterlich behandelt. Der Notfall- und Krisenmanagement-Beauftragte kämpft oft allein an vorderster Front, erhält wenig bis keine Zuarbeit und sieht sich einer Flut von Aufgaben gegenüber, die von der Organisation kaum ernsthaft unterstützt werden. Dokumente werden erstellt, aber selten gelesen, geschweige denn gelebt. Die Kenntnisse über vorhandene Ressourcen und Möglichkeiten sind oft erschreckend begrenzt, und anstatt ein strategisches, ganzheitliches Krisenmanagement auf Managementebene zu etablieren, vergraben sich viele in abteilungsbezogenen Notfallplänen. Das führt dazu, dass im Ernstfall weder Übersicht noch klare Entscheidungswege vorhanden sind – ein Pulverfass, das nur darauf wartet, zu explodieren.

> „WER WÜHLT SCHON GERNE IN PAPIER, WENN ER MIT EINER INTUITIVEN SOFTWARE ARBEITEN KANN, DIE ALLES ÜBERSICHTLICH UND GRIFFBEREIT BIETET?



KLASSISCH[...]SIERTE) SYSTEME

DIGITALE SYSTEME

✅ VORTEILE ✅

HOHE AKZEPTANZ BEI „TRADITIONELLEN“ TEAMS
- niedrige Einstiegshürden durch intuitive Nutzung
- Notizen sind jederzeit möglich

UNABHÄNGIG VON TECHNOLOGIEN
- bei Strom- oder Internetausfällen weiterhin nutzbar
- Papierunterlagen sind leicht zu transportieren und ohne technische Voraussetzungen nutzbar

REDUZIERTE KOMPLEXITÄT
- keine Ablenkung durch Zusatzfunktionen
- Checklisten können als „klassische Listen“ bearbeitet werden
- Bedienungsfehler nahezu ausgeschlossen

KEINE ABHÄNGIGKEIT
- autarkes System ohne Dienstleisterabhängigkeit

EINGESPIELTE ABLÄUFE
- oft über Jahrzehnte erprobt
- Unterlagen können so verwendet werden, wie es der eigenen Arbeitsweise entspricht
- in Stresssituationen wirkt Papier beruhigender

ÜBERSICHTLICHKEIT UND SUCHE
- klare Übersicht/Struktur durch ein Dashboard
- schnelle Informationsfindung durch integrierte Suchfunktion

KOLLABORATION UND KOMMUNIKATION
- zentrale, skalierbare und flexible Datenhaltung
- ortsunabhängige Kommunikationsmöglichkeit

ECHTZEIT-INFORMATIONEN & SCHNELLE AKTUALISIERUNG
- Lageänderungen, Dokumentation und Aufgaben sind sofort für alle sichtbar

AUTOMATISIERTE DOKUMENTATION UND VERSIONIERUNG
- lückenlose Nachverfolgung aller Schritte und Änderungen

DATENINTEGRITÄT UND DATENSICHERHEIT
- Zugriffsrechte schützen vor unbefugten/unbemerkten Änderungen
- regelmäßige Datensicherung sowie automatische technische und inhaltliche Updates

ANALYSEN UND AUSWERTUNGEN
- Reportings und Ereignisdokumentation

❌ NACHTEILE ❌

EINGESCHRÄNKTE VERNETZUNG
- Informationsweitergabe in Echtzeit ist kaum möglich
- Daten bleiben oft isoliert, da keine Schnittstellen zu anderen Systemen bestehen

FEHLENDE AUTOMATISIERUNG
- Aufgabenverteilung und Protokollführung erfolgen manuell
- Analysen und Auswertungen müssen händisch erstellt werden

NACHHALTIGKEIT UND SICHERHEIT
- hoher Papierverbrauch steht in Widerspruch zu nachhaltigen Unternehmenszielen
- Zugriffsschutz nur bedingt möglich

UNÜBERSICHTLICHKEIT
- hoher Verwaltungsaufwand und steigende Unübersichtlichkeit bei der Verwaltung von Versionen
- Änderungen sind schwer nachvollziehbar
- Informationssuche ist zeitintensiv

AUFWENDIGE AKTUALISIERUNG
- Änderungen müssen manuell in allen Dokumenten eingepflegt werden
- eingeschränkte Nachverfolgbarkeit von Änderungen und Ergänzungen
- erhöhte Fehleranfälligkeit

KOMPLEXITÄT UND DATENMIGRATION
- Überforderung durch Funktionalität oder zu hohe fachliche Spezialisierung
- Bestehende Daten müssen übertragen werden

ABHÄNGIGKEIT VON IT-INFRASTRUKTUR
- Bei Strom-, Server- oder Internetausfällen kann der Zugriff blockiert sein

DATENSCHUTZ UND IT-SICHERHEIT
- Digitalisierung birgt Risiken (z. B. Cyberangriffe, Datenverlust)
- Erfüllung von Compliance- und Datenschutzanforderungen
- Erhöhter Schutzbedarf bei sensiblen Daten

EINGESCHRÄNKTE ANPASSUNGSMÖGLICHKEITEN
- Standardsoftware ist möglicherweise nicht flexibel genug

HÖHERE IMPLEMENTIERUNGSKOSTEN
- Lizenzen, Schulungen und ggf. neue Hardware können Initialinvestitionen erfordern

EINARBEITUNGSAUFWAND
- Notwendigkeit von Einführungsschulungen
- Akzeptanzprobleme nicht technikaffiner Mitarbeiter

Lesen Sie weiter auf der nächsten Seite. >>>

KERNFUNKTIONEN MODERNER SOFTWARELÖSUNGEN

Am Markt erhältliche Softwarelösungen bieten eine breite Palette an Funktionen, die helfen, Notfälle und Krisen systematisch zu bewältigen. Dabei decken sie den gesamten Managementkreislauf ab: Vorbereitung, Erkennung, Alarmierung, Bewältigung, Dokumentation und Analyse.

1. DIGITALES NOTFALL- UND KRISENHANDBUCH UND SZENARIENVERWALTUNG

- **Zentrale Ablage relevanter Dokumente:** In einer übersichtlichen Datenbank sind Notfallpläne, Krisenkommunikationspläne, Kontaktdaten und Checklisten (ggf. standortübergreifend) gebündelt.
- **Individuell anpassbare Handbücher:** Jeder Betrieb oder jede Organisation kann eigene Pläne und Prozesse hinterlegen und jederzeit aktualisieren.
- **Szenarienbasierte Module:** Bei bestimmten Vorfällen (z. B. Naturkatastrophe, Cyberangriff, Chemieunfall) werden automatisch passende Hilfsmittel und Prozesse vorgeschlagen.

2. ALARMIERUNG UND BENACHRICHTIGUNG

- **Mehrkanal-Alarmierung:** Automatische Benachrichtigung per E-Mail, SMS, App oder Telefon, um relevante Akteure schnell zu erreichen.
- **Eskalationsstufen und Rollenverteilung:** Das System erkennt, wenn eine Meldung unbeantwortet bleibt, und informiert im nächsten Schritt weitere Personen.
- **Schnittstellen zu externen Einrichtungen:** Möglichkeit, Meldungen an offizielle Warnsysteme, Rettungsleitstellen oder Behörden weiterzuleiten.

3. ECHTZEIT-LAGEBILDER UND DASHBOARDS

- **Visuelle Darstellung der Situation:** Einsatzorte, Wetterdaten, Sensormeldungen und weitere Faktoren werden in einer Lageübersicht zusammengeführt.
- **Priorisierung von Maßnahmen:** Anhand von Statusanzeigen und klar zugewiesenen Verantwortlichkeiten lassen sich offene, laufende und abgeschlossene Aufgaben effizient verfolgen.
- **Anbindung externer Datenquellen:** Einbindung von Geoinformationssystemen, um etwa Evakuierungszonen oder Störfallbereiche exakt darzustellen.

4. AUFGABEN- UND RESSOURCENMANAGEMENT

- **Transparente Aufgabenverteilung:** Beteiligte sehen Aufgaben und Fristen auf einen Blick.
- **Kontinuierliche Aktualisierung:** Neue Informationen oder geänderte Maßnahmen werden sofort sichtbar.
- **Ressourcenübersicht:** Verfügbarkeit von Personal, Betriebsmitteln, Schutzkleidung, Einsatzfahrzeugen oder externen Dienstleistern wird in Echtzeit sichtbar.

5. DOKUMENTATION UND REPORTING

- **Automatisierte Protokollierung:** Alle Maßnahmen werden mit Zeit- und Userstempel hinterlegt und lassen sich später detailliert nachvollziehen.
- **Revisionssichere Archivierung:** Das System erstellt nach Abschluss eines Vorfalls einen umfassenden Bericht mit allen relevanten Informationen.
- **Individuell anpassbare Auswertungen:** Von der kurzgefassten Lageübersicht bis zum umfangreichen Abschlussbericht ist vieles auf Knopfdruck verfügbar.

6. PLANSPIELE UND TRAININGS

- **Digitale Simulationen:** Verschiedene Notfall- und Krisenszenarien können realitätsnah durchgespielt werden, um Abläufe zu trainieren, Engpässe und Defizite aufzudecken und gewonnene Erkenntnisse gezielt in die Optimierung einfließen zu lassen.

AUSBLICK: WO GEHT DIE REISE HIN?

Die Digitalisierung im Notfall- und Krisenmanagement ist weit mehr als nur ein technischer „Nice-to-have"-Aspekt. Der Schutz von Leben, Umwelt und Sachwerten wird dadurch deutlich effektiver und ressourcenschonender, wenn Systeme richtig eingesetzt und die Anwender entsprechend geschult werden. Zwar weisen analoge Lösungen einige Vorzüge auf (z. B. Unabhängigkeit von IT), aber sie geraten bei komplexen und dynamischen Ereignisfällen an ihre Grenzen.

Die am Markt verfügbaren Softwarelösungen bieten eine beeindruckende Bandbreite an Funktionen – von digitalen Notfall- und Krisenhandbüchern über automatische Alarmierung und Echtzeit-Lagebilder bis hin zu Planspielen und automatisierter Dokumentation. Eine Investition in solche Technologien ist eine Investition in die Zukunftsfähigkeit des Unternehmens. Dennoch bleibt der Mensch der entscheidende Faktor: Erst durch gezielte Schulung, praktische Erfahrung und vorausschauendes Handeln können digitale Systeme ihr volles Potenzial entfalten und effektiv zum Krisenmanagement beitragen.

„ANGESICHTS DES STEIGENDEN ANSPRUCHS AN DAS NOTFALL- UND KRISENMANAGEMENT – ETWA DURCH ZUNEHMENDE BEDROHUNGEN ODER EXTERNE ANFORDERUNGEN – **GEWINNEN SOFTWARELÖSUNGEN IMMER MEHR AN BEDEUTUNG.**

PRE-EMPLOYMENT CHECKS: EIN WICHTIGER BESTANDTEIL MODERNER PERSONALAUSWAHLPROZESSE

In Zeiten steigender Compliance-Anforderungen und zunehmender Mobilität von Arbeitskräften gewinnen Pre-Employment Checks (PEC) immer mehr an Bedeutung. Diese Überprüfungen gewährleisten, dass Unternehmen fundierte Entscheidungen bei der Einstellung neuer Mitarbeiter treffen, potenzielle Risiken, die durch unzureichend geprüfte Bewerber entstehen könnten, minimieren und gleichzeitig rechtliche Anforderungen erfüllen.

Pre-Employment Checks sind strukturierte und rechtskonforme Überprüfungen von Bewerberangaben und -hintergründen, die vor einer finalen Einstellung durchgeführt werden. Dabei handelt es sich NICHT um das wahllose Durchforsten des Internets nach persönlichen Daten oder das Ausspähen des Privatlebens.

DEFINITION: EIN PRE-EMPLOYMENT CHECK (AUCH PRE-EMPLOYMENT SCREENING ODER BEWERBER BACKGROUND CHECK GENANNT) IST DIE LEGALE UND RECHTSKONFORME ÜBERPRÜFUNG VON BEWERBUNGSKANDIDATEN VOR DER EIGENTLICHEN EINSTELLUNG BZW. UNTERZEICHNUNG DES ARBEITS- BZW. ANSTELLUNGSVERTRAGS.

TYPISCHE BESTANDTEILE VON BACKGROUND-CHECKS

Das Ziel dieser Checks ist es, die Eignung eines Kandidaten für eine spezifische Position anhand objektiver Kriterien zu bewerten und potenzielle Risiken für das Unternehmen, wie beispielsweise wirtschaftskriminelle Handlungen, frühzeitig zu erkennen. Der Umfang der Überprüfungen variiert je nach Branche, Position und berechtigtem Interesse, das stets im Verhältnis zur Tätigkeit steht. So ist beispielsweise ein Führungszeugnis in sensiblen Bereichen wie dem Finanzsektor, Sicherheitsgewerbe oder bei Arbeiten mit schutzbedürftigen Personen legitim. Diese Überprüfungen müssen jedoch rechtskonform erfolgen und dürfen zum Teil nur mit dem ausdrücklichen Einverständnis des Bewerbers durchgeführt werden. >>>

TYPISCHE BESTANDTEILE EINES PEC

IDENTITÄTSPRÜFUNG
Überprüfung offizieller Dokumente wie Personalausweis oder Reisepass.

BERUFSQUALIFIKATIONEN
Validierung von Abschlüssen, Zertifikaten und beruflichen Lizenzen sowie das Überprüfen der Beschäftigungshistorie. Analysieren Sie auch, ob der Bewerber in Ländern tätig war, die als Hochrisikoregionen für Korruption oder Geldwäsche gelten.

REFERENZPRÜFUNG
Kontaktaufnahme mit früheren Arbeitgebern, Vorgesetzten, Kollegen oder anderen relevanten Referenzpersonen, um ein vollständigeres Bild zu erhalten.

STRAFRECHTLICHE VERGEHEN
Überprüfung, ob relevante Vorstrafen oder laufende Verfahren vorliegen, sofern dies für die Position erforderlich ist.

FINANZPRÜFUNG
Überprüfung der finanziellen Stabilität des Bewerbers, insbesondere bei Positionen mit hoher oder finanzieller Verantwortung, um potenzielle Risiken wie Unterschlagung oder Bestechlichkeit frühzeitig zu erkennen und zu minimieren.

SANKTIONS- UND WATCHLISTEN
Prüfung, ob der Bewerber auf internationalen Sanktionslisten (z. B. OFAC oder EU-Sanktionslisten) verzeichnet ist, sowie ein Abgleich mit Terrorlisten, um sicherzustellen, dass keine Verbindungen zu sicherheitsrelevanten Organisationen bestehen.

GESUNDHEITSCHECKS
Sicherstellung der Arbeitsfähigkeit, wenn gesetzlich oder betrieblich erforderlich.

ÜBERPRÜFUNG VON INTERESSENKONFLIKTEN
Prüfen Sie potenzielle Geschäftsbeziehungen oder persönliche Verbindungen des Bewerbers, die zu Interessenkonflikten im Unternehmen führen könnten. Vergewissern Sie sich, dass keine Beteiligungen an Wettbewerbern oder mögliche Einflussnahmen durch externe Parteien bestehen. Identifizieren Sie Verbindungen zu politisch exponierten Personen, die zu Risiken führen könnten.

Ergänzend kann eine Analyse öffentlich zugänglicher Informationen und Social-Media-Profile sinnvoll sein, um potenziell problematisches Verhalten oder widersprüchliche Angaben frühzeitig zu erkennen.

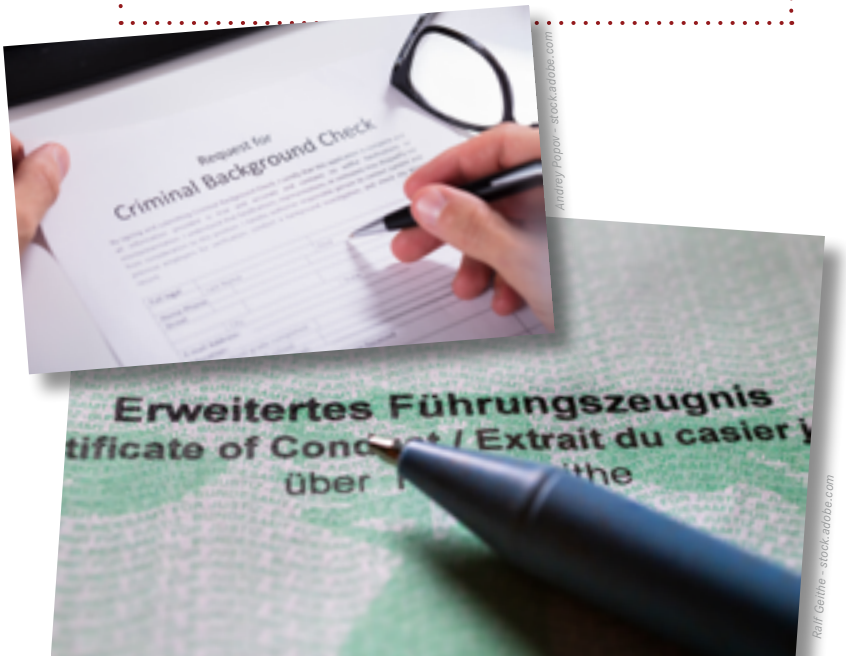
DIE BEDEUTUNG VON PRE-EMPLOYMENT CHECKS

Ein fehlerhafter oder unzureichender Einstellungsprozess kann für Unternehmen erhebliche Kosten und Risiken mit sich bringen. Background-Checks dienen dabei nicht nur der Risikominimierung, sondern auch der Stärkung von Vertrauen und dem Schutz der Unternehmensreputation. Sie bieten Schutz vor:

> **STUDIEN ZEIGEN, DASS BIS ZU 30 % DER BEWERBER FALSCHE ANGABEN IM LEBENSLAUF MACHEN.**

1. BETRUG: Falschangaben im Lebenslauf oder unerwünschte Verbindungen können frühzeitig erkannt werden.
2. RECHTSRISIKEN: In vielen Branchen sind bestimmte Überprüfungen gesetzlich vorgeschrieben.
3. REPUTATIONSSCHÄDEN: Die Anstellung eines Kandidaten mit kriminellem Hintergrund oder unzureichenden Qualifikationen kann dem Ruf eines Unternehmens erheblich schaden und das Vertrauen in die Marke schwächen.
4. KOSTEN DURCH FEHLBESETZUNGEN: Fehlentscheidungen bei der Personalauswahl können zu enormen Kosten führen.
5. SICHERHEITSLÜCKEN: Unternehmen möchten sicherstellen, dass neue Mitarbeiter nicht nur die erforderlichen Qualifikationen mitbringen, sondern auch ethische und professionelle Standards einhalten, um die Unternehmenskultur zu schützen und interne Sicherheitsrisiken zu minimieren.

In bestimmten Bereichen oder Branchen werden Pre-Employment Checks durch behördliche Überprüfungen ergänzt oder ersetzt. Beispiele hierfür sind Zuverlässigkeitsüberprüfungen in der Luftfahrt, Sicherheitsüberprüfungen nach dem Sicherheitsüberprüfungsgesetz (SÜG) für sicherheitskritische Tätigkeiten sowie Prüfungen im Rahmen des Wirtschaftsschutzes, etwa bei sensiblen Unternehmen der kritischen Infrastruktur.



EFFIZIENTE DURCHFÜHRUNG VON PRE-EMPLOYMENT CHECKS

Bei der Durchführung von Pre-Employment Checks ist es unerlässlich, diese transparent und datenschutzkonform zu gestalten. Neben den finanziellen Ressourcen sollten auch der zeitliche Aufwand und mögliche Auswirkungen auf den Rekrutierungsprozess einkalkuliert werden. Da solche Prüfungen zeitintensiv sein und den Einstellungsprozess verlängern können, greifen viele Unternehmen auf spezialisierte Dienstleister zurück. Diese Anbieter bieten effiziente Lösungen und entlasten Unternehmen durch ihre Expertise und zeitsparenden Verfahren.

Damit Pre-Employment Checks effizient und rechtssicher umgesetzt werden, sollten Unternehmen folgende Best Practices beachten:

- INFORMATION DES BEWERBERS: Bewerber sollten frühzeitig transparent über die erhobenen Daten, deren Zweck sowie gegebenenfalls erforderliche Einwilligungen informiert werden.
- STANDARDISIERTE PROZESSE: Einheitliche Richtlinien und standardisierte Abläufe sorgen für Konsistenz und Transparenz. Der Screening-Prozess sollte lückenlos dokumentiert werden, um den korrekten Umgang mit personenbezogenen Daten nachweisen zu können.
- SCHULUNG DER VERANTWORTLICHEN: Mitarbeiter der Personalabteilung sollten im Umgang mit sensiblen Daten und den rechtlichen Anforderungen geschult sein.
- TECHNOLOGISCHE UNTERSTÜTZUNG: Der Einsatz von datenschutzkonformen Softwarelösungen zur Automatisierung kann Zeit und Ressourcen sparen.

UMGANG MIT SCREENING-ERGEBNISSEN

Kandidaten sollte stets die Möglichkeit eingeräumt werden, zu negativen Screening-Ergebnissen Stellung zu nehmen. Dies ist ein Ausdruck von Respekt und Fairness im Umgang miteinander. Gewonnene Informationen können unvollständig, veraltet oder fehlerhaft sein, da nicht immer alle Fakten und Hintergründe bekannt sind. Ein klärendes Gespräch hilft, potenzielle Missverständnisse auszuräumen und verhindert, dass ein geeigneter Mitarbeiter aufgrund einer Fehleinschätzung übersehen wird.

Pre-Employment Checks sind mehr als nur ein Kontrollinstrument – sie bilden die Grundlage für eine verantwortungsvolle Personalauswahl und zeitgemäße Personalauswahlprozesse. Sie schützen Unternehmen vor finanziellen, rechtlichen und reputationsbezogenen Risiken und tragen dazu bei, die besten Talente zu gewinnen. Unternehmen, die auf transparente und strukturierte PECs setzen, legen den Grundstein für langfristigen Erfolg und nachhaltige Mitarbeiterbeziehungen. Gleichzeitig sichern sie ihre Wettbewerbsfähigkeit und stärken das Vertrauen von Mitarbeitern und Stakeholdern. Diese lassen sich aber auch ausweiten auf In-Employment Screenings während der Arbeitstätigkeit oder Background-Checks von externen Mitarbeitenden.

In unserem Downloadbereich stellen wir Ihnen ein informatives Merkblatt vom Bundesamt für Verfassungsschutz bereit.

„BACKGROUND-CHECKS UND IN- SOWIE PRE-EMPLOYMENT SCREENINGS SIND WEIT MEHR ALS NUR FORMALITÄTEN – SIE SIND EINE STRATEGISCHE MASSNAHME IM PERSONALMANAGEMENT.

ANSPRUCH VS. REALITÄT:

UNTERNEHMENSSICHERHEIT BRAUCHT EINEN PLATZ IM STRATEGISCHEN KONTEXT

In den Führungsetagen von Unternehmen finden sich klangvolle Titel wie CEO, CFO, COO, CIO, CTO, CMO, CHRO, CISO – und irgendwo dazwischen, sofern es ihn denn gibt, der CSO – der Chief Security Officer, also die Leitung der Unternehmenssicherheit. Doch gerade bei dieser Position stellt sich die Frage: Wird dieser Rolle die notwendige strategische Bedeutung zugemessen, oder bleibt sie ein zahnloser Tiger ohne echten Einfluss auf die Entscheidungsfindung des Unternehmens?

Ein Chief Security Officer sollte weit mehr sein als nur der „Kümmerer“ für Zutrittskontrollen, den Sicherheitsdienst oder die Erstellung von Notfallplänen. Er sollte eine zentrale Rolle spielen, wenn es um den Schutz von Mitarbeitern, der Arbeitsumgebung, Vermögenswerten und den Ruf des Unternehmens geht. Doch allzu oft wird die Unternehmenssicherheit nach wie vor nur als operative Funktion wahrgenommen – ein interner Dienstleister, der Maßnahmen umsetzt, anstatt eine treibende Kraft hinter strategischen Entscheidungen zu sein.

Die Aufgaben des CSO reichen von der Entwicklung und Implementierung umfassender Sicherheitsstrategien bis hin zur proaktiven Risikominimierung, um Mitarbeiter, Betriebsstätten, Vermögenswerte und den Ruf des Unternehmens zu schützen.

EIN PARADIGMENWECHSEL IST NOTWENDIG

Ein zentraler Grund für die mangelnde Wirksamkeit der Unternehmenssicherheit liegt in der fehlenden Integration in die obersten Entscheidungsprozesse. Die Leitung der Unternehmenssicherheit wird oft auf einen Abteilungsleiter-Status reduziert und in der Hierarchie unter Funktionen wie der IT-Leitung (CIO) oder dem Facility Management angesiedelt. Dies widerspricht dem Anspruch, Sicherheit als geschäftskritischen Faktor zu verstehen und zu behandeln.

> „Sicherheit ist weder IT, Arbeitsschutz noch Gebäudemanagement – sie ist eine eigenständige Disziplin mit strategischer Relevanz und zahlreichen Facetten.

Noch immer wird Sicherheit in vielen Unternehmen als rein technische Disziplin wahrgenommen. Der Fokus liegt auf Systemen und operativen Prozessen wie Videoüberwachung, Zutrittskontrollen oder der Leitung des Sicherheitsdienstes. Diese Sichtweise führt häufig dazu, dass Unternehmen auf die Schaffung einer eigenständigen Position verzichten – schließlich können „die paar Aufgaben“ auch von der Haustechnik, dem Facility Management oder der Arbeitssicherheit mit übernommen werden. Doch dieser Ansatz greift zu kurz. Sicherheit ist mehr:

1. Sie erfordert eine ganzheitliche Betrachtung technischer Komponenten im Zusammenspiel mit Prozessen, personellen Maßnahmen und spezifischen Sicherheitskonzepten, die sich durch das gesamte Unternehmen ziehen.
2. Sie umfasst strategische Fragestellungen wie die Antizipation von Risiken und die Schaffung einer Sicherheitskultur. Dazu zählen physische Sicherheitsmaßnahmen, Reisesicherheitsmaßnahmen, die Betrachtung von Bedrohungen aus dem Inneren sowie der Schutz von Lieferketten, Veranstaltungen und Führungspersönlichkeiten. Auch der Produktschutz und die Verankerung von Resilienz als Wettbewerbsvorteil spielen eine zentrale Rolle.
3. Und vor allem muss Sicherheit in den Köpfen aller Mitarbeitenden verankert sein, um ein wirksames Schutzniveau zu erreichen und eine wirksame Sicherheitskultur zu etablieren.

VOM INTERNEN DIENSTLEISTER ZUM STRATEGISCHEN GESTALTER

Ein CSO sollte daher die Perspektive eines strategischen Gestalters einnehmen. Er muss Risiken nicht nur analysieren, sondern auch auf Vorstandsebene präsentieren, diskutieren und klare, umsetzbare Lösungsvorschläge entwickeln. Nur so wird Sicherheit zu einem integralen Bestandteil der Unternehmensstrategie und -kultur.

Ein zukunftsorientierter CSO geht dabei über die bloße Risikobewertung hinaus: Er nimmt aktiv Einfluss auf Geschäftsstrategien, um Sicherheitsbelange frühzeitig und effektiv einzubinden. Dies setzt jedoch voraus, dass die Person fachlich versiert ist und über umfassende Kenntnisse in den unterschiedlichsten Disziplinen der Sicherheit verfügt. Ohne diese Expertise droht eine einseitige Betrachtung und das Sicherheitsniveau bleibt auf einem Grundniveau stehen.

ZU DEN STRATEGISCHEN AUFGABEN EINES KOMPETENTEN CSO ZÄHLEN BEISPIELSWEISE:

- **Bewertung von Markterschließung und Standortentscheidungen:** Unterstützung bei der Auswahl neuer Märkte/Standorte oder Bewertung und Begleitung von Bauprojekten unter Berücksichtigung von Sicherheits- und Risikofaktoren.
- **Business Continuity:** Enge Verzahnung der Sicherheitsstrategie mit der Geschäftsfortführung sowie dem Notfall- und Krisenmanagement. Dies umfasst die Entwicklung präventiver Strategien und detaillierter Pläne für den Ernstfall sowie die aktive und verantwortungsvolle Mitwirkung im Krisenstab.
- **Technologische Innovationen und Erweiterungen:** Prüfung und Integration neuer technischer Lösungen, um Sicherheitsstandards kontinuierlich zu verbessern und potenzielle Risiken frühzeitig zu minimieren.
- **Compliance und Governance:** Sicherstellung, dass alle Sicherheitsmaßnahmen regulatorischen Anforderungen entsprechen und rechtlich einwandfrei umgesetzt werden.

>>>


Sutthiphong - stock.adobe.com

> UNTERNEHMENSSICHERHEIT AUS DER OPERATIVEN ECKE ZU HOLEN, BEGINNT MIT IHRER ORGANISATORISCHEN VERANKERUNG.

Ein starker CSO sollte in der Unternehmenshierarchie auf Augenhöhe mit anderen Chief–Level-Positionen agieren und direkten Zugang zur Geschäftsführung haben, um Sicherheitsstrategien als integralen Bestandteil des Unternehmenserfolgs zu positionieren.

Die direkte Berichtslinie ermöglicht es der Leitung der Unternehmenssicherheit, strategische Risiken und Bedrohungen oder die Auswirkungen regulatorischer Anforderungen proaktiv zu adressieren. Denn diese betreffen die gesamte Organisation.

SICHERHEITSKULTUR:
VOM REGELWERK ZUR GELEBTEN VERANTWORTUNG

Eine zentrale Aufgabe des CSO ist die Förderung einer gelebten Sicherheitskultur. Sicherheit darf nicht allein durch Policies und Checklisten definiert werden. Vielmehr muss sie von allen Mitarbeitenden und externen Partnern aktiv gelebt werden. Dies erfordert gezielte Schulungen, Sensibilisierungsmaßnahmen und ein umfassendes Verständnis für die Bedeutung von Sicherheitsfragen auf allen Ebenen des Unternehmens.

Der CSO sollte dabei als Impulsgeber und Vorbild agieren. Abteilungen und Teams müssen aktiv eingebunden werden, während praxisnahe und umsetzbare Lösungen entwickelt werden, die verdeutlichen, dass Sicherheit keine Belastung, sondern ein wirksamer Schutz und eine Unterstützung für alle ist.

RESSOURCEN UND KOMPETENZEN:
WAS UNTERNEHMENSSICHERHEIT ERFOLGREICH MACHT

Um diese strategische Rolle ausfüllen zu können, benötigt der CSO die richtigen Ressourcen. Dies umfasst nicht nur ausreichende Budgets, sondern auch personelle und technologische Mittel. Es ist entscheidend, dass Sicherheitsprojekte nicht als Kostenfaktoren, sondern als Investitionen in die Zukunftsfähigkeit des Unternehmens verstanden werden. Nur so kann die Unternehmenssicherheit von einem rein operativen Ansatz zu einer strategischen Führungsfunktion weiterentwickelt werden, die maßgeblich zur langfristigen Resilienz und Wettbewerbsfähigkeit beiträgt.

> Die Unternehmenssicherheit darf kein zahnloser Tiger sein – sie muss Biss haben!

Es ist an der Zeit, die Bedeutung der Unternehmenssicherheit neu zu denken. Statt als Kostenfaktor oder rein technische Funktion sollte sie als strategischer Hebel betrachtet werden, der nicht nur den Status quo schützt, sondern das Unternehmen in die Lage versetzt, Chancen zu nutzen und langfristig erfolgreich zu sein.

Die Unternehmenssicherheit darf kein zahnloser Tiger sein. Sie muss strategisch verankert, organisatorisch auf Augenhöhe und kulturell tief in der Organisation verwurzelt sein. Ein CSO, der über umfassende Fachkenntnisse und eine interdisziplinäre Perspektive verfügt, kann Sicherheitsstrategien entwickeln, die nicht nur operativ effizient sind, sondern auch langfristig die Resilienz des Unternehmens stärken und Sicherheit zu einem Wettbewerbsvorteil machen.

GEFAHRENMANAGEMENT REVOLUTIONIEREN

WARUM INTEGRIERTE SYSTEME UNVERZICHTBAR SIND

GEFAHRENMANAGE-MENTSYSTEM KURZ **GMS**

> **MODERNES GEFAHRENMANAGEMENT IST MEHR ALS NUR EINE ABBILDUNG DER ZUSTÄNDE!**

Ob in Pforten, an Empfängen, in Hausmeisterbüros oder in Leitstellen – Alarmmeldungen müssen nach vordefinierten Schemen effizient bearbeitet werden können. Dabei greifen technische Systeme häufig ineinander. Es nutzt wenig, wenn der Sicherheitsdienst auf einer Videokamera einen unbefugten Zutritt erkennt, der Empfang eine Warnmeldung über eine unerlaubt geöffnete Tür erhält und der Haustechniker eine eingeschlagene Scheibe des Feueralarms detektiert. Ohne übergeordnete Integration und Sichtbarkeit dieser Ereignisse bleiben sie isoliert und führen zu unkoordinierten Abläufen, die eine Reaktion erheblich verzögern.

Die Integration technischer Systeme ist daher ein essenzieller Schritt, um die Effizienz und Effektivität des Gefahren- und Reaktionsmanagements in modernen Gebäuden zu steigern. Die zunehmende Komplexität von Gebäudeleittechnik (GLT), Brandmeldetechnik (BMT) und Sicherheitstechnik erfordert eine nahtlose Zusammenarbeit, die im Ereignisfall eine schnelle, koordinierte und präzise Entscheidung ermöglicht.

WAS SIND GEFAHRENMANAGEMENTSYSTEME?

Gefahrenmanagementsysteme (GMS) agieren als zentrale Steuer- und Koordinationsplattformen, die (sicherheits-)technische Systeme nahtlos miteinander vernetzen. Durch die Integration über eine zentrale Schnittstelle werden einzelne Komponenten zusammengeführt, wodurch eine umfassende Übersicht und Steuerung sowohl der Sicherheitssysteme als auch der definierten Maßnahmen ermöglicht wird. Dieser fortschrittliche Sicherheitsansatz zeigt seine Stärken besonders bei Unternehmen, die über mehrere Standorte oder sogar länderübergreifend operieren und somit eine koordinierte Gefahrenabwehr sicherstellen müssen.

Zu den Hauptfunktionen gehört es, die Darstellung von Meldungen und Alarmgrafiken aus unterschiedlichen Quellen zentral zu visualisieren. GMS unterstützen Unternehmen zudem bei der Abwehr von Gefahrensituationen durch automatisierte und koordinierte Reaktionsstränge.

Beispielsweise kann im Interventionsfall (Feuer, Einbruch etc.) die Steuerung von Videokameras oder der Fluchtwegtechnik, die Freigabe von Schrankenanlagen oder die Aktivierung von Lautsprecherdurchsagen automatisiert erfolgen.

Natürlich können diese Systeme auch isoliert genutzt werden – gesteuert durch unterschiedliche Abteilungen oder Bereiche. Allerdings liegt der Nachteil solcher Einzellösungen auf der Hand: Der Zeitverlust und die mangelnde ganzheitliche Betrachtung des Ereignisses wirken sich negativ auf die Effizienz aus. Der Vorteil integrierter Systeme ist klar: **Alle Sicherheitslösungen werden zentral verbunden, wodurch die Arbeit mit mehreren Monitoren und isolierten Systemen entfällt.** >>>

Gefahrenmanagementsysteme lassen sich mit einer Vielzahl an Systemen/Gewerken verbinden, unabhängig vom Hersteller. Dazu zählen:

- Brandmeldeanlagen
- Fluchtwegtechnik
- Einbruchmeldeanlagen
- Überfallmeldeanlagen
- Zutrittskontrollsysteme
- Tür- und Torsteuerungen/-überwachungen
- Schrankenanlagen
- Videoüberwachungsanlagen
- Freigeländeüberwachungen
- Sprachalarmierungsanlagen
- Aufzugsnotrufsysteme
- Gegensprechanlagen
- Gebäudetechnik (HLK) und Energiemanagement
- Kommunikationstechnik

Durch ihre flexible Architektur können sie Sicherheitssysteme und technische Anlagen nahtlos miteinander verknüpfen und dadurch ein hochentwickeltes Security Operations Management schaffen.

„GEFAHRENMANAGEMENTSYSTEME NEHMEN DATEN ÜBERGEORDNET AUF UND VERKNÜPFEN DIESE MIT MASSNAHMENPLÄNEN.“

Allein das Argument der Risikovorsorge, das in zahlreichen Gesetzen, von Zertifizierungsstellen und zunehmend auch von Kunden gefordert wird, unterstreicht die Bedeutung eines leistungsfähigen GMS. Ein solches System, kombiniert mit klar hinterlegten betrieblichen Strukturen im Sicherheits- und Notfallmanagement, kann nicht nur die Sicherheit erhöhen, sondern auch haftungsbefreiend wirken.

OPTIMIERUNG UND EFFIZIENZ: EIN ÜBERBLICK DER VORTEILE

Gefahrenmanagementsysteme bieten eine Vielzahl an Vorteilen, die weit über reine Sicherheitsaspekte hinausgehen.

EFFIZIENZSTEIGERUNG: Zentrale Visualisierung und Steuerung ermöglicht eine klare Übersicht und vereinfacht komplexe Prozesse.

ENTSCHEIDUNGSFINDUNG: Konsolidierte Darstellung ermöglicht schnellere und fundiertere Entscheidungen.

AUTOMATISIERUNG: Optimierung von Sicherheitsmaßnahmen durch vordefinierte und dynamische Workflows.

FEHLALARMREDUKTION: Dank zentraler Auswertung und Verknüpfung von Daten wird die Quote von Fehlalarmen signifikant gesenkt.

ZEITEINSPARUNG: Schnellere Reaktionszeiten durch abgestimmte Prozesse und automatisierte Maßnahmen.

RESSOURCENSCHONEND: Weniger Einarbeitungsbedarf und automatisierte Prozesse entlasten Personalressourcen und reduzieren den Bedarf an spezialisierten Mitarbeitern.

FLEXIBILITÄT: Skalierbarkeit über mehrere Standorte und Gewerke.

KOSTENERSPARNIS: Reduzierter Einarbeitungsaufwand und niedrigere Betriebskosten durch effiziente Nutzung der Systemfunktionen.

KONTINUITÄTSSTEIGERUNG: Schnellere und koordiniertere Reaktionen minimieren Betriebsunterbrechungen und unterstützen die Wiederherstellung kritischer Prozesse.

RISIKOMANAGEMENT: Die Identifikation von Mustern und Trends erlaubt es, präventive Maßnahmen zu entwickeln und potenzielle Gefahren frühzeitig zu erkennen.

NOTFALLMANAGEMENT: Lebensrettende Maßnahmen können schneller und effizienter umgesetzt werden.

TRANSPARENZ: Einheitliche Benutzeroberfläche und automatische Dokumentation aller Vorfälle und Reaktionen als Grundlage für eine lückenlose Nachverfolgung (rechtskonform).

INTEGRATION: Modulare GMS lassen sich nahtlos in bestehende IT- und Sicherheitsinfrastrukturen integrieren.

INTEGRATION UND HERAUSFORDERUNGEN

Die Anwendung moderner GMS bietet Unternehmen zahlreiche Möglichkeiten, ihre Sicherheitsstrategien zu optimieren. Beispielsweise können Webzugriffe oder bereitgestellte Apps genutzt werden, um standortunabhängig auf relevante Informationen zuzugreifen. Spezialgeräte wie RFID-Scanner lassen sich integrieren, um Überwachungsrundgänge effizient zu dokumentieren.

Doch trotz des enormen Potenzials birgt die Zusammenführung von technischen Systemen im Gefahren- und Reaktionsmanagement auch Herausforderungen...

Natürlich kann der Übergang zu moderner Technik herausfordernd sein, insbesondere wenn ältere Systeme im Einsatz sind, die erst mit modernen Technologien verbunden werden müssen. Häufig erschweren inkompatible Standards oder proprietäre Protokolle die Integration, da offene Schnittstellen und standardisierte Kommunikationsprotokolle fehlen. Dabei dürfen auch die damit verbundenen Risiken für die IT-Sicherheit nicht außer Acht gelassen werden.

Ein weiterer Hemmschuh ist der Kostenaspekt. Während neue Sicherheitstechnik zunächst Investitionen erfordert, zeigt sich im Ereignisfall, dass veraltete Systeme, die den Anforderungen nicht gerecht werden, meist ein Vielfaches der Investitionskosten verursachen. Dabei reicht es jedoch nicht aus, nur in Technik zu investieren. Diese muss fachgerecht eingesetzt, zuverlässig betrieben sowie regelmäßig überwacht und gewartet werden, um ihren vollen Nutzen zu entfalten.

Wenn ein Integrationsprojekt gestartet werden soll, ist es entscheidend, herstellerunabhängige Planer oder Berater hinzuzuziehen. Diese Experten unterstützen dabei, die Integration sowie die damit verbundenen Prozesse optimal zu begleiten und sicherzustellen, dass alle Anforderungen erfüllt werden. So wird ein zukunftsfähiges und ganzheitlich durchdachtes Ergebnis gewährleistet.

Dabei sollte die **ZIELDEFINITION** klar und präzise formuliert werden, um den Rahmen des Gefahrenmanagementsystems als Gesamtsystem festzulegen. Folgende Aspekte sind dabei zu berücksichtigen:

- Welche Komponenten und Funktionen soll das GMS als Gesamtsystem umfassen?
- Welche Ausbaustufen/Standorte (Interoperabilität) soll es künftig geben?
- Welche Systeme, Geräte oder Technologien müssen in das GMS integriert werden?
- Welche spezifischen regulatorischen Anforderungen müssen Beachtung finden?
- Welche spezifischen Aufgaben und Funktionen soll das GMS erfüllen?
- Welche Schnittstellen und Verknüpfungen sind zwischen dem GMS und anderen bestehenden oder geplanten Systemen erforderlich?
- Wie sollen die in das GMS integrierten Informationen im übergeordneten System visualisiert und zugänglich gemacht werden?
- Wie sollen die einzelnen Informationen im Gesamtsystem verarbeitet, dargestellt und mit zusätzlichen Aufgabenstellungen verknüpft werden?
- Wie soll die Ausfallsicherheit und Redundanz gewährleistet werden?
- Welche Analyse- und Dokumentationsmöglichkeiten sollte das System haben?
- Welche Nutzer/Arbeitsplätze sollen Zugriff erlangen?

> DIE ZUSAMMENFÜHRUNG VON TECHNISCHEN SYSTEMEN IM GEFAHREN- UND REAKTIONSMANAGEMENT IST EINE STRATEGISCHE NOTWENDIGKEIT, UM DEN STEIGENDEN ANFORDERUNGEN AN SICHERHEIT UND EFFIZIENZ GERECHT ZU WERDEN.

Alternativ kann auch das Handbuch des Verbands für Sicherheitstechnik (VfS) eine wertvolle Unterstützung bieten. Eine erste Leseprobe finden Sie in unserem Downloadbereich.

Mit durchdachter Planung, modernen Technologien und einem Fokus auf IT-Sicherheit können Unternehmen nicht nur ihre Sicherheitsstandards verbessern, sondern auch Zeit und Kosten sparen, wenn die Systemintegration in ein übergeordnet agierendes GMS erfolgt ist.

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.

PODCAST-TIPP

CONTROL ROOM INSIDE – DER PODCAST FÜR LEITSTÄNDE UND INNOVATIONEN

Control Room Inside ist der Podcast für alle, die sich für Kontrollräume, Sicherheitszentralen, Notruf- und Serviceleitstellen und die neuesten technischen Innovationen begeistern.

Jungmann Systemtechnik-Digitalexperte Dirk Lüders nimmt Sie mit auf eine Reise hinter die Kulissen moderner Leitwarten und Monitoring-Center. Dabei zeigt er, wie zukunftsweisende Technologien, Teamwork, Künstliche Intelligenz und andere bahnbrechende Entwicklungen die Arbeitsweise in Kontrollräumen revolutionieren.

Ob Ingenieur, IT-Experte, Praktiker oder Tech-Enthusiast – dieser Podcast bietet faszinierende Einblicke rund um die Gestaltung und Optimierung von Leitständen und den Einsatz modernster Technologien in einer zunehmend digitalisierten Welt.

PODCAST

CONTROL ROOM INSIDE – Für alle, die Leitstände von morgen mitgestalten wollen.

TOOL

EINFACHER EINSTIEG IN DIE CYBER-SICHERHEIT

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat LARS ICS (Light And Right Security) als kostenfreies Open-Source-Programm entwickelt.

Dieses benutzerfreundliche Tool ermöglicht eine rein offline durchgeführte, fragengeleitete Selbsteinschätzung des aktuellen Cyber-Sicherheitsstands und bietet praxisorientierte Empfehlungen, welche Maßnahmen priorisiert umgesetzt werden sollten.

FUNKTIONEN UND VORTEILE AUF EINEN BLICK:

- Alle Maßnahmen sind den Normen ISO 27001, IEC 62443, dem BSI ICS Security-Kompendium und dem IT-Grundschutz zugeordnet.
- Das Tool vereinfacht komplexe Risiko- und Schutzbedarfsanalysen.
- Detaillierte Berichte liefern einen Überblick.

GERADE FÜR KLEINE UND MITTLERE UNTERNEHMEN (KMU) BIETET LARS ICS ALS KOSTENFREIES TOOL EINEN EINFACHEN EINSTIEG IN DIE CYBER-SICHERHEIT.

LARS ICS, das Handbuch und der Quelltext stehen kostenfrei beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung. Teile davon finden Sie auch in unserem Downloadbereich.

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® e.K. • Dorfaue 8b • 15738 Zeuthen
Telefon: +49 (0) 30 / 700 36 96 -5 • E-Mail: kontakt@sicherheit-das-fachmagazin.de • Geschäftsführer: Michael Blaumoser
Handelsregister: HRA3959CB • Umsatzsteuer-ID: DE279558068 • ISSN: 2569-3816 • Erscheinungsweise: 4 x pro Jahr
Bildquelle: www.stock.adobe.com (sofern nicht anders angegeben)

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.