SICHERHEIT. DAS FACHMAGAZIN.

SICHERHEIT AUF DEN PUNKT GEBRACHT.

EXKLUSIV Seite 7

kostenfreies E-Learning-Training zum Thema „Hygienemaßnahmen im Pandemiefall“

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.

SICHERHEIT. DAS FACHMAGAZIN.

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

UNSERE THEMEN

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

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 Ent-wicklungen mit unseren Zielgruppen zu teilen, unabhängig davon, ob das nötige Budget für ein Abonnement aufgebracht werden kann.

Wie finanziert sich SICHERHEIT. Das Fachmagazin.?

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

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

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

E-PAPER

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

Ihre Vorteile:

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

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

Nutzen Sie die Praxiserfahrung der Anbieter vor Ort und informieren Sie sich umfassend über Sicherheitsthemen und neue technische Möglichkeiten in Verbindung mit begleitenden Foren, Workshops und Fachveranstaltungen.

SICHERHEITSMESSEN 2019

Eine (Sicherheits-)Messe bietet Ihnen die Möglichkeit, (Sicherheits-) Anbieter und (Sicherheits-)Produkte zu finden, zu vergleichen und sich ein Bild von der Marktsituation zu verschaffen. Gerade im Bereich technischer Lösungen kann eine (Sicherheits-)Messe zur Markttransparenz genauso beitragen wie zur Festigung einer gewissen Vorauswahl von technischen Komponenten.

SICHER DURCHS JAHR 2019

01 POTSDAM

- 19.03. BIS 20.03.2019
  GPEC DIGITAL
  (Spezialmesse zur Digitalisierung der Inneren Sicherheit)
- 21.03. BIS 22.03.2019
  LUFTSICHERHEITSTAGE
  (Treffen der Luftsicherheitsexperten)
- 14.05. BIS 15.05.2019
  VfS-Kongress
  (Verband für Sicherheitstechnik - Kurzvorträge und Ausstellung zu neuen techn. Sicherheitslösungen)

02 MAINZ

- 28.03.2019
  VSW-JAHRESTAGUNG
  (Vereinigung für Sicherheit in der Wirtschaft als Schnittstelle zwischen Sicherheitsbehörden und Wirtschaft)

03 BASEL

- 10.09. BIS 13.09.2019
  SICHERHEIT
  (Schweizer Fachmesse für Sicherheit und Prävention)

04 MÜNCHEN

- 26.06. BIS 27.06.2019
  SICHERHEITSEXPO
  (Sicherheitstechnik demonstrieren und Fachtagung für Brandschutz)

05 NÜRNBERG

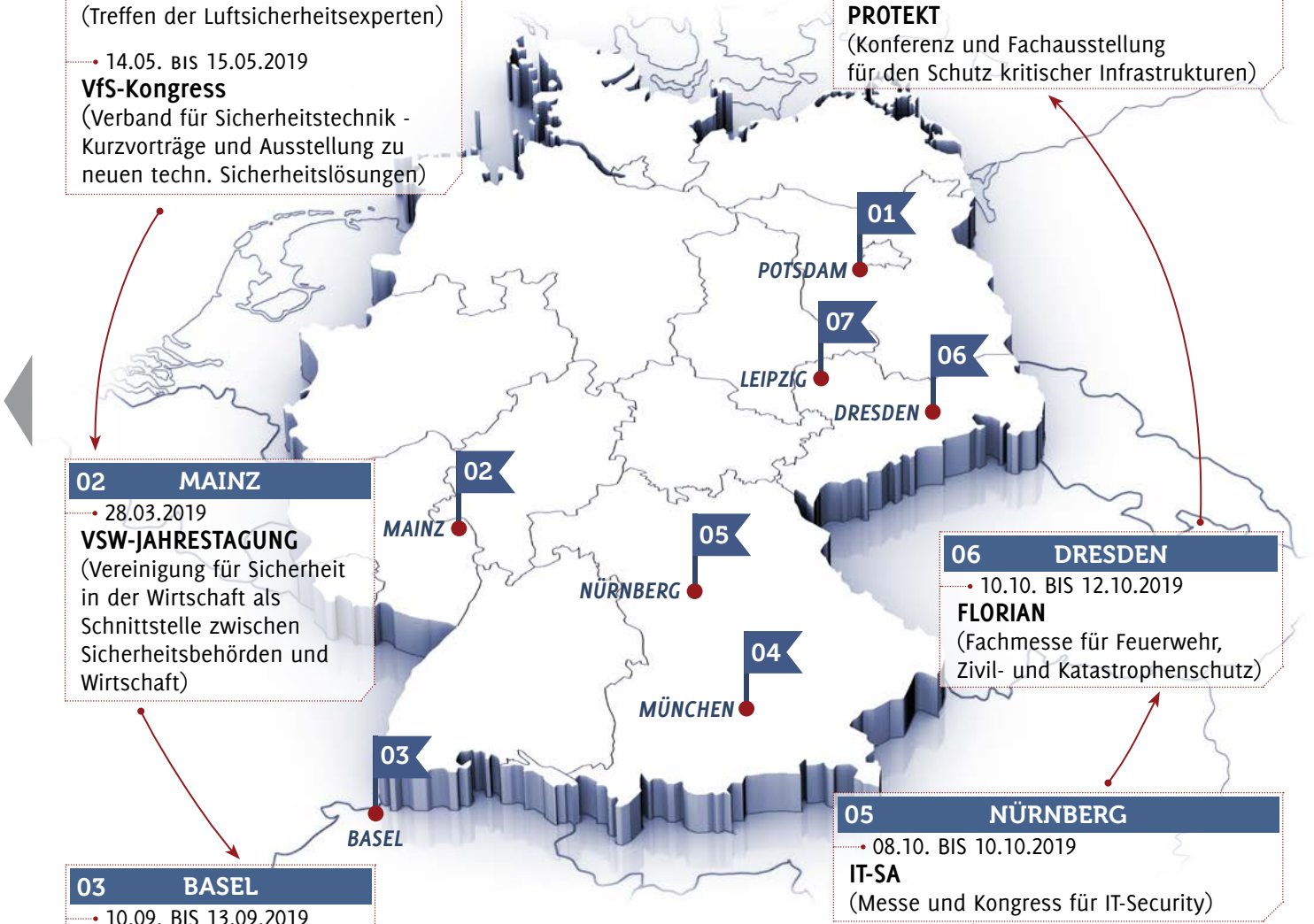
- 08.10. BIS 10.10.2019
  IT-SA
  (Messe und Kongress für IT-Security)

06 DRESDEN

- 10.10. BIS 12.10.2019
  FLORIAN
  (Fachmesse für Feuerwehr, Zivil- und Katastrophenschutz)

07 LEIPZIG

- 12.11. BIS 13.11.2019
  PROTEKT
  (Konferenz und Fachausstellung für den Schutz kritischer Infrastrukturen)



PRÄVENTIVES KRISENMANAGEMENT: PANDEMIEPLANUNG UNTER ARBEITSRECHTLICHEN UND BETRIEBLICHEN ASPEKTEN

Frau Muster, die Sicherheitsmanagerin eines internationalen Mobilfunkkonzerns, befindet sich an einem Freitagvormittag in ihrem PKW auf dem Weg zu einer Fachtagung, als sie von einem Standortleiter telefonisch kontaktiert wird.

Sein Anliegen: Meldungen über die Schweinegrippe werden medial immer stärker behandelt und die WHO (Weltgesundheitsorganisation) hat nun auch bereits die Pandemiestufe 6 ausgerufen – wäre es da nicht an der Zeit, den Krisenstab einzuberufen?

So geschehen im Juni 2009, als das Thema „Pandemie“ und „Pandemieplanung“ noch mit einer gewissen Skepsis und Unwissenheit betrachtet wurde.

Nach zahlreichen Influenza-Pandemien und Ausbrüchen von hochansteckenden Krankheiten sollte das Thema „Pandemie“ bzw. „Pandemieplanung“ – gerade auch bedingt durch die rasant wachsende Globalisierung – in allen Organisationen und Unternehmen angekommen sein und einer kritischen Betrachtung unterzogen werden. Doch was genau ist zu tun? Sollte man vorbeugen? Kann man überhaupt vorbeugen? Diese Fragen und mehr erörtern wir in dem folgenden Artikel.

Die meisten Betriebe halten Krisen- und Notfallpläne für unvorhergesehene Ereignisse vor, in denen Verantwortlichkeiten, Meldewege, Handlungsanweisungen und Checklisten festgehalten sind, um bei plötzlich auftretenden unvorhergesehenen Ereignissen reagieren zu können. Diese sind intern sowie extern abgestimmt und werden (hoffentlich!) in regelmäßigen Abständen zielgruppenspezifisch geschult und mit Hilfe von Krisen- und Notfallübungen einem Praxistest unterzogen.

Doch der Pandemiefall ist anders. Er ist eine sich anbahnende Situation, auf die mit geeigneten Vorsorgemaßnahmen und einer gewissen Vorlaufzeit reagiert werden kann, um die betriebliche Funktionsfähigkeit möglichst lange aufrechtzuerhalten und letztlich auch die Gesundheitsrisiken für Mitarbeiter zu minimieren, da sich der Ausbruch einer Pandemie über mehrere Wochen erstreckt und die wirtschaftlichen Folgen noch länger anhalten können. Daher sollte die betriebliche Pandemieplanung als Szenario bei der eigenen Krisen- und Notfallplanung Berücksichtigung finden.

ERMITTELN SIE DIE MÖGLICHEN IN- UND EXTERNEN AUSWIRKUNGEN

In einem Pandemiefall kommt es zu einer veränderten Nachfrage nach Produkten und (Dienst-)Leistungen, die die Infrastruktur der Wirtschaft und Gesellschaft gefährden können. Zudem stehen Ressourcen mitunter nur noch eingeschränkt zur Verfügung. Aufgrund der hohen Abhängigkeit von Lieferprozessen und Wertschöpfungsketten sowie der vorherrschenden Just-in-time-Produktion kann es zu einem Dominoeffekt kommen, der weite Bereiche der Wirtschaft und Gesellschaft massiv einschränken kann.

ZAHLEN ZUR ANNAHME EINER PANDEMIE GEMÄSS DEM NATIONALEN PANDEMIEPLAN

Erkrankungsraten:	15% bis 50% der Bevölkerung
Dauer einer Grippewelle:	8 bis 10 Wochen
Dauer eine Pandemie:	ungewiss

DEFINITION „EPIDEMIE" VS. „PANDEMIE“

Eine **Epidemie** ist eine örtlich begrenzte Ausbreitung einer Infektionskrankheit (z. B. Ebola in Afrika).

Eine **Pandemie** ist eine länderübergreifende globale Verbreitung einer Infektionskrankheit. Hierbei taucht eine neue Erregervariante auf, die Menschen infiziert und eine ernsthafte Erkrankung hervorruft sowie sich leicht verbreitet (z. B. Spanische Grippe).

Daher geht es bei der Pandemieplanung vorrangig darum, dem möglichen Ressourcenausfall frühzeitig vorzubeugen und sich beispielsweise auf eine hohe Erkrankungsrate beim Personal einzustellen.

Da sich eine Pandemie nicht nur lokal ausbreiten wird, sondern auch über Landesgrenzen und ggf. ganze Kontinente hinweg, sollte man sich folgende Fragen stellen:

1. Werden unsere Produkte und Dienstleistungen während einer Pandemie vermehrt nachgefragt und benötigt (z. B. Hersteller von Taschentüchern, Medikamenten und medizinischen Verbrauchsmaterialien, Speditionen/ Lieferdienste etc.)?
2. Zählen wir zu den kritischen Infrastrukturen (KRITIS), deren Leistungen kontinuierlich benötigt werden (z. B. Anbieter aus den Bereichen Ernährung, Energie, Informations- und Kommunikationstechnik, Gesundheit, Transport und Verkehr, Wasser etc.)?
3. Wird auf unsere Produkte und Dienstleistungen ggf. sogar gänzlich verzichtet werden?

Neben der Prüfung der vertraglichen Verpflichtungen gegenüber seinen Kunden und/oder weiteren Dritten, müssen auch gewisse Grundsatzentscheidungen getroffen werden, ob und inwieweit die betriebliche Funktion aufrechterhalten werden soll bzw. sogar werden muss.

Daraus ableitend ergeben sich gewisse zu definierende (Vorsorge-)Maßnahmen.

„DAS ZIEL DER BETRIEBLICHEN PANDEMIEPLANUNG IST GEMÄSS DEM NATIONALEN PANDEMIEPLAN: „DIE MINIMIERUNG DES INFEKTIONSRISIKOS AM ARBEITSPLATZ, DIE AUFRECHTERHALTUNG DER BETRIEBSABLÄUFE, SOWEIT DIES MÖGLICH IST, DER ERHALT DER BETRIEBLICHEN INFRASTRUKTUR, DIE BEGRENZUNG DES WIRTSCHAFTLICHEN SCHADENS UND DIE AUFRECHTERHALTUNG DER FÜR DIE VERSORGUNG DER BEVÖLKERUNG WICHTIGEN PRODUKTE BZW. FUNKTIONEN.“ DIES GILT SINNGEMÄSS AUCH FÜR BEHÖRDEN.

> **„DIE PANDEMIEPLANUNG SOLLTE NICHT NUR FÜR STANDORTE UND ARBEITSPLÄTZE IN DEUTSCHLAND GELTEN, SONDERN IM SINNE DER FÜRSORGE- UND SORGFALTSPFLICHT AUCH FÜR STANDORTE UND ENTSANDTE MITARBEITER IM AUSLAND.**

GEHEN SIE DIE PANDEMIEPLANUNG SYSTEMATISCH AN

Es ist nur eine Frage der Zeit, bis die nächste Pandemie eintritt. Viele Experten gehen zudem davon aus, dass die Auswirkungen weitreichender sein werden als beim Ausbruch der Schweinegrippe im Jahr 2009. Spätestens, wenn die WHO die Pandemiestufe 4 ausruft, sollte man sich entsprechend vorbereiten:

1. Welche Arbeitsschritte (bei welchen Produkten) sind unabdingbar oder müssen zwingend personell betreut werden?
2. Welche externen Leistungen und infrastrukturellen Versorgungen werden zwingend benötigt?

Diese und ggf. noch weitere betriebliche Prozesse müssen frühzeitig definiert werden. Für deren Umsetzung bzw. Aufrechterhaltung sind aber auch interne/externe Absprachen notwendig bzw. mitsprachepflichtig (z. B. Arbeitnehmervertretung, Facility Management, Unternehmenssicherheit, Arbeitsschutz, betriebsärztlicher Dienst, Finanzen etc.).

Hierzu finden Sie auf Seite 8 eine grobe Checkliste. Des Weiteren erhalten Sie in unserem Downloadbereich ein Beispiel einer „Inhaltsübersicht zur betrieblichen Pandemieplanung".

ARBEITSRECHTLICHE REGELUNGEN FÜR DEN PANDEMIEFALL

Der Arbeitgeber kann im Rahmen der arbeitsrechtlichen Regelungen – und unter Einhaltung mitgeltender Vorschriften und der aktuellen Rechtslage – gewisse Vorgaben im Pandemiefall u. a. zur Deaktivierung von Personal geben. Dies kann z. B. der Fall sein, wenn der Betriebsbereich und dessen individuelle Leistung in einem Pandemiefall nicht benötigt wird oder, um die Ansteckungsgefahr – die bereits 24 Stunden vor den ersten Anzeichen erhöht ist – zu minimieren.

Um eine rasche Umsetzung zu ermöglichen, sollten derartige Eingriffsmöglichkeiten im Vorfeld rechtlich geprüft und im Rahmen der gültigen Tarifverträge, rechtlichen Gegebenheiten oder der Mitbestimmung/Unterrichtung im Betrieb definiert werden.

Dies bezieht sich beispielsweise auf

- die Zuweisung eines anderen Arbeitsplatzes oder von Home-Office,
- die Anordnung von Überstunden,
- bestimmte Schutzmaßnahmen zu treffen wie z. B. die Desinfektion von Arbeitsräumen,
- die Anordnung von Freistellungen, Urlaub oder Nacharbeit sowie
- die Einführung von Kurzarbeit (in Abklärung mit der zuständigen Bundesagentur für Arbeit).

Weiterhin ist Folgendes zu prüfen:

- Der Umgang mit Problemstellungen resultierend durch die beschränkt steuerbare Abwesenheit von Beschäftigten (z. B. aufgrund der Betreuung Angehöriger, Kindergarten-/Schulschließungen, ehrenamtlichen Verpflichtungen oder mangels öffentlicher Verkehrsmittel oder auch bedingt durch die Angst vor Ansteckung etc.).

- Die Vertragsgestaltung mit Leiharbeitnehmern oder Subunternehmern.
- Die Fürsorge- und Sorgfaltspflicht zum (Gesundheits-) Schutz aller Arbeitnehmer (z. B. durch Zugangskontrollen, berührungsfreie Fieber-Messungen, Pflicht zum Tragen von Mund- und Nasenschutz etc.).
- Die Sicherstellung der Verfügbarkeit von Schlüsselfunktionen (Krisenstab) mit erweiterten Anwesenheitspflichten sowie deren entsprechender Versorgung.

Insbesondere für den Pandemiefall, aber natürlich auch für den Alltag und daraus resultierende Ansteckungsgefahren ist es wichtig, Mitarbeiter für das Thema zu motivieren und entsprechend zu sensibilisieren.

**Die Inhalte des Artikels basieren auf dem Handbuch „Betriebliche Pandemieplanung" des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe in Zusammenarbeit mit dem Landesgesundheitsamt Baden-Württemberg.*

KOSTENFREIES E-LEARNING-TRAINING
› HYGIENEMASSNAHMEN IM PANDEMIEFALL ‹

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

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

Der Arbeitgeber kann hier mit gutem Beispiel vorangehen, indem z. B.

- Gesundheitstage,
- Unternehmenssport- und Fitnessveranstaltungen,
- Gesunde Ernährung,
- Impfprophylaxen,
- Gesundheitschecks oder
- Verhaltensregeln für den Krankheitsfall

angeboten werden.

DIE NACHFOLGENDEN THEMEN KÖNNEN SIE BEI DER BETRIEBLICHEN PANDEMIEPLANUNG UNTERSTÜTZEN.

Stellen Sie sich die 3 Grundsatzfragen:

1. Muss der Betrieb zwingend aufrechterhalten werden und wenn ja, in welchen Bereichen?
2. Welche Betriebsabläufe und personellen Besetzungen sind zwingend erforderlich?
3. Zu welchen externen Produkten und (Dienst-)Leistungen besteht eine zwingende Abhängigkeit?

(Hinweis: Binden Sie die betroffenen Abteilungen aktiv und frühzeitig in die Planung mit ein.)

CHECKLISTE: BETRIEBLICHE PANDEMIEPLANUNG

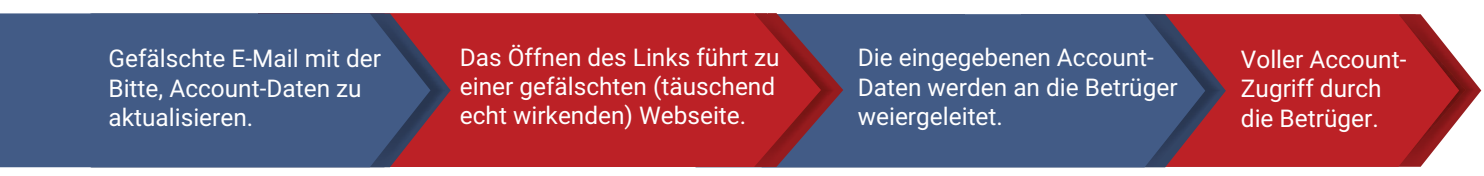
- ☐ Definieren Sie Verantwortlichkeiten und Zuständigkeiten (Pandemie-Planungsteam).
- ☐ Legen Sie interne und externe Alarmierungs-, Kommunikations- und Verhaltensregeln fest.
- ☐ Erstellen Sie konkrete Handlungsanweisungen.
- ☐ Führen Sie Sensibilisierungsmaßnahmen/-kampagnen durch.
- ☐ Vorsorgemaßnahmen und deren Ausgabemodalitäten sollten definiert und ggf. auch bevorratet werden (z. B. Desinfektionsmittel, Einmalhandtücher, Atemschutz, Handschuhe etc.)
- ☐ Eruieren und definieren Sie Schlüsselpersonen im Betrieb unter Berücksichtigung sozialer Aspekte, der Motivation sowie Betreuung und Versorgung.
- ☐ Halten Sie sich stets über die offiziellen (Behörden-)Kanäle auf dem Laufenden (Gesundheitsamt, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Robert Koch-Institut, WHO etc.).
- ☐ Erarbeiten Sie Informationsschreiben, Plakate etc. für den Pandemiefall (Empfehlung: www.infektionsschutz.de).
- ☐ Planen Sie Prophylaxe-Maßnahmen (z. B. Impfaktionen, Einhaltung von Erholungsphasen, Aktion „Arbeiten an der frischen Luft“, kostenfreies Obst etc.).
- ☐ Prüfen Sie die Bevorratung von Betriebsstoffen, Medikamenten, Getränken, Lebensmitteln etc.
- ☐ Intensivieren Sie die Zusammenarbeit mit anderen Unternehmen, Behörden und Organisationen, die ggf. vor selben oder vergleichbaren Herausforderungen stehen.
- ☐ Definieren Sie den betrieblichen (Mindest-)Personalbedarf sowie den Umgang mit erkrankten Personen.
- ☐ Finden Sie Möglichkeiten zur allgemeinen Kontaktaufrechterhaltung mit Mitarbeitern, Kunden, Geschäftspartnern etc.
- ☐ Definieren Sie Schritte und Maßnahmen zur Rückkehr in den Normalbetrieb (z. B. berufliche Rehabilitation von Mitarbeitern, Würdigung der Leistungsbereitschaft Einzelner, Betriebsabläufe normalisieren, Beweissicherung für etwaige Rechtsansprüche gegenüber Dritten etc.).

WEITERE EMPFEHLUNGEN IN FORM VON AUSFÜHRLICHEN UND MODULAR AUFGEBAUTEN CHECKLISTEN UND HANDLUNGSEMPFEHLUNGEN ERHALTEN SIE IM HANDBUCH „BETRIEBLICHE PANDEMIEPLANUNG“ DES BUNDESAMTES FÜR BEVÖLKERUNGSSCHUTZ UND KATASTROPHENHILFE IN ZUSAMMENARBEIT MIT DEM LANDESGESUNDHEITSAMT BADEN-WÜRTTEMBERG, WELCHES WIR IHNEN IM DOWNLOADBEREICH ZUR VERFÜGUNG GESTELLT HABEN.

WAS IST EIGENTLICH PHISHING UND WIE FUNKTIONIERT DAS PRINZIP?

Phishing-Angriffe stellen für Unternehmen, Behörden und Organisationen eine dauerhafte Bedrohung für die eigene Sicherheitsinfrastruktur dar. Der Begriff und auch die Gefahr des „Phishing“ ist mittlerweile allgegenwärtig. Doch die Wenigsten wissen, was er konkret bedeutet und wie man sich vor Phishing-Mails überhaupt schützen kann. Fest steht: ein rein softwarebasierter Schutz ist nicht ausreichend! Daher ist es essentiell, Computernutzer über diese Art der Betrugsmasche zu informieren und sie gegenüber den Risiken und Gefahren zu sensibilisieren.

Beim Phishing handelt es sich um das betrügerische „Angeln“ oder „Fischen“ von persönlichen oder sensiblen Daten mit unterschiedlichsten Methoden und zu unterschiedlichsten Zwecken durch Cyber-Kriminelle. Das Erlangen der Daten geht häufig mit der Forderung Login-Daten zu aktualisieren, wichtige Zahlungen auszuführen oder Kreditkarteninformationen einzugeben, einher. Außerdem enthalten Phishing-Mails immer öfter auch schädliche Dateien oder führen über beigefügte Links zu automatischen Downloads von Schadsoftware. Das Prinzip selbst stammt noch aus Zeiten, bevor E-Mail und Internet Zugang in Unternehmen und Haushalte fanden. „Damals“ war es der nette Anrufer oder der vertrauenserweckende Brief, welcher das Ziel hatte, persönliche Daten zu erfahren und abzugreifen. Die möglichst realistische Darstellung von Phishing-Angriffen führt in der Praxis dazu, dass sie so gut funktionieren. Eine Vielzahl der Betrüger agiert „blind“ in die Masse hinein, ohne eine gezielte vorhergehende Recherche zur angegriffenen Person. Doch gerade die zweite Variante, der gezielte Angriff auf Unternehmen und Personen, führt dazu, dass Phishing-Angriffe nur sehr schwer erkannt werden, da der Absender detaillierte Kenntnisse zu unternehmerischen Vorgängen, persönlichen Vorlieben und Verhaltensweisen gesammelt hat und seinen Angriff explizit darauf aufbaut.



Beispielhaftes Vorgehen bei einem Phishing-Angriff

VERSCHLEIERUNGSMETHODEN UND SCHÄDEN DURCH PHISHING-MAILS

Um Phishing-Mails erkennen zu können, sollte der potentielle Empfänger – also Bereiche im Unternehmen, die viele E-Mails erhalten und schreiben – wissen, mit welchen Tricks und Methoden die Betrüger arbeiten und worauf diese abzielen.

Die Schäden von Phishing-Mails können vielfältig sein:

- Verlust von Login- oder Account-Daten
- Ausfall von IT-Systemen
- Lösegeldforderungen zur Datenfreigabe
- Physische Systemausfälle
- Überweisungsaufträge
- Datenverlust
- Wirtschaftsspionage
- Datenschutzverletzungen

Das Schadenausmaß hängt stets von der individuellen Motivation der Betrüger ab: soll dem Unternehmen oder der Person gezielt geschadet werden oder ist es eher ein Beifang?

Die Verschleierungsmethoden von Phishing-Mails sind vielfältig, doch mit einem sensibilisierten Nutzer können sie bereits im Vorfeld erkannt werden.

VERSCHLEIERUNGSMETHODE	AUFFÄLLIGKEIT	SENSIBILISIERUNG
Nachahmung von Internetseiten oder URLs bekannter Webseiten	Aufforderung zur Dateneingabe	Passwörter, PIN und TAN werden niemals telefonisch von Kollegen, von Ihrem Lieblings-Online-Versandhaus oder einer Bank abgefragt. Dies zählt zu den wichtigsten Sicherheitsregeln!
Einbindung eines Formulars oder Hyperlinks in einer gefälschten E-Mail	Aufforderung zur Dateneingabe	Hyperlinks sollten immer überprüft werden, bevor sie angeklickt werden. Hierbei ist genau darauf zu achten, wohin der Link führt.
Gefälschte Namen der Zielseiten oder Verwendung von kyrillischen anstelle von lateinischen Buchstaben	Zielseite ähnelt nur der originalen Webseite	Im Zweifelsfall die Originalwebseite aufrufen und nach dem Pfad des Links suchen.
Massenversand von E-Mails	keine persönliche Ansprache	Immer auf die richtige Ansprache achten.

Arten der Verchleierungsmethoden

DENKEN SIE IMMER DARAN: BETRÜGER KÖNNEN MITTLERWEILE EINE GANZE MENGE FÄLSCHEN! SIGNATUREN, ABSENDERNAMEN*, WEBSEITEN…

*** Wie Sie auf einen Brief einen beliebigen Absender schreiben können, können Kriminelle das auch bei E-Mails, wenn kein entsprechender Schutz vorliegt.**

EINFALLSMÖGLICHKEITEN VERHINDERN

Viele Phishing-Mails sind für Virenscanner und Firewalls nur schwer als solche zu erkennen, da sie häufig keine Schadsoftware als Dateianhang enthalten, sondern diese erst nachladen. Daher ist hier die Schwachstelle nicht die Technik (Software), sondern der Mensch, der betrügerische E-Mails öffnet und die entsprechenden Anweisungen ernst nimmt.

☐ DATENSPARSAMKEIT

Um gezielten Angriffen gegen Unternehmen und Personen vorzubeugen, hilft es bereits, wenn insbesondere im öffentlichen Raum (z. B. Social Media) sparsam mit Daten umgegangen wird.

☐ PASSWORTSICHERHEIT

Für verschiedene Portale und Accounts sollten unterschiedliche Passwörter genutzt werden, die regelmäßig erneuert werden.

☐ REGELMÄSSIGE UPDATES

Veraltete Software und Systeme führen oft zu Sicherheitslücken, die von Betrügern als Einfallsmöglichkeit genutzt werden.

☐ PLAUSIBILITÄT PRÜFEN

Passen der Absender und die vermeintlichen Informationen zusammen. Besteht überhaupt ein Nutzerkonto? Ist dies die typische Sprache und das Design des Absenders? Stimmt die Absenderadresse?

☐ RECHNER AUSSCHALTEN

Updates werden meist erst beim Neustart installiert, daher sollten Rechner auch heruntergefahren werden und nicht stetig im Stand-By-Modus operieren.

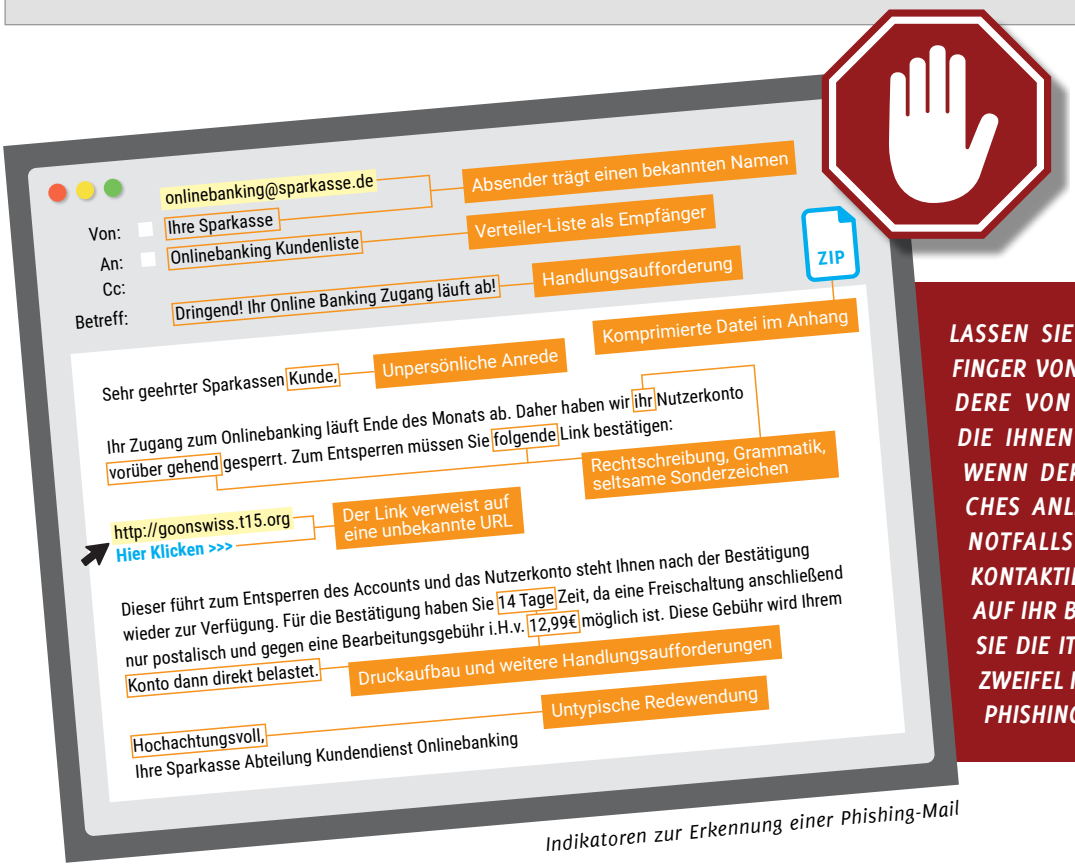
☐ KRITISCH HINTERFRAGEN

Mitarbeiter sollten E-Mails kritisch hinterfragen. Häufig werden kleine Unstimmigkeiten im Arbeitsalltag übersehen. Daher sollten bereits beim kleinsten Fragezeichen Inhalte kritisch überprüft werden.

- Dateianhänge können über einen Virenscanner geprüft werden
- Flash-Player nur bei Bedarf (manuell) starten
- Dokumente nur aus vertrauenswürdigen Quellen öffnen
- bei ZIP-Dateien: Rückfrage an vermeintlichen Empfänger oder die IT-Abteilung
- einige Links können mittlerweile über das Portal www.virustotal.com geprüft werden

☐ ÖFFENTLICHES W-LAN MEIDEN

Freies W-LAN in Verbindung mit ungesicherten Verbindungen ist eine große Schwachstelle. Für Online-Banking oder -Shopping sollte man grundsätzlich bessere Alternativen wählen.



Indikatoren zur Erkennung einer Phishing-Mail

LASSEN SIE IM ZWEIFEL LIEBER DIE FINGER VON E-MAILS UND INSBESONDERE VON ANHÄNGEN UND LINKS, DIE IHNEN KOMISCH VORKOMMEN! WENN DER ABSENDER EIN WIRKLICHES ANLIEGEN HAT, WIRD ER SIE NOTFALLS AUF ANDEREN WEGEN KONTAKTIEREN. HÖREN SIE IMMER AUF IHR BAUCHGEFÜHL UND ZIEHEN SIE DIE IT-ABTEILUNG ZUR RATE. IM ZWEIFEL IST ES IMMER BESSER, EINE PHISHING-MAIL ZU LÖSCHEN.

GEFÄHRDUNGSMINIMIERUNG DURCH DEN EINSATZ VON FREIGELÄNDESICHERUNGEN UND PERIMETERÜBERWACHUNG

In vielen Unternehmen, Behörden und Organisationen ist die Gebäudesicherung allgegenwärtig. Meist bedeutet dies jedoch nur, dass es ein mechanisches Schließsystem (Schlüssel) und ggf. noch eine Einbruchmeldeanlage (EMA) gibt. Doch die ganzheitliche Betrachtung und Berücksichtigung einer vollumfänglichen Objektsicherung sollte bereits an der Gebäude- bzw. Grundstücksgrenze beginnen. Im Folgenden werden Ihnen die Möglichkeiten eines effektiven Perimeterschutzes dargestellt und erläutert.

Gerade augenscheinlich nicht überwachte (Betriebs-)Bereiche stellen häufig ein hohes Risiko des unbefugten Zutritts dar. Besonders bei großen Industrie- und Gewerbeparks, Logistikzentren mit Außenlagerflächen, Infrastrukturobjekten, Schrottplätzen oder Autohäusern mit Freigelände gilt es, ein besonderes Augenmerk auf die Geländeabsicherung zu werfen, um es Straftätern bei (geplanten) Einbrüchen, Diebstählen oder Vandalismus- und Sabotagetaten nicht zu einfach zu machen. Die Schutzziele und der entsprechende Sicherungsbedarf müssen gemeinsam mit dem Versicherer und dem Errichter definiert werden.

Übrigens: bereits im Mittelalter gab es Freigeländesicherungen, z. B. in Form von (Wasser-)Gräben oder von Wachen bewachten Mauern.

DEFINITION DER JURISTISCHEN AUSSENGELÄNDEGRENZE

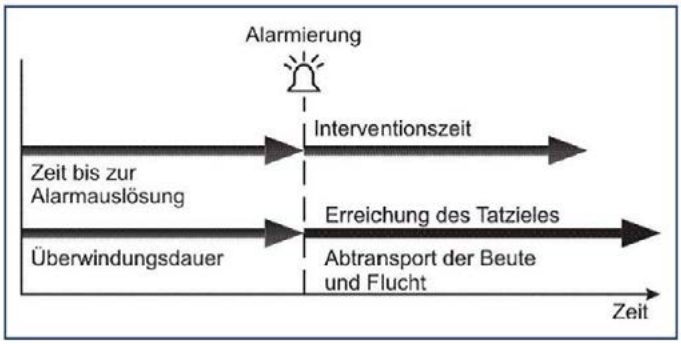
Im juristischen Sinne stellt die Außengeländegrenze in den meisten Fällen auch die äußere Perimetergrenze dar, die nicht deckungsgleich mit der Außenseite eines zu schützenden Objektes ist. Diese gilt es vor

- unberechtigtem Betreten oder Verlassen,
- unberechtigtem Befahren oder Ausfahren sowie
- Sabotage/Vandalismus an Sicherungseinrichtungen

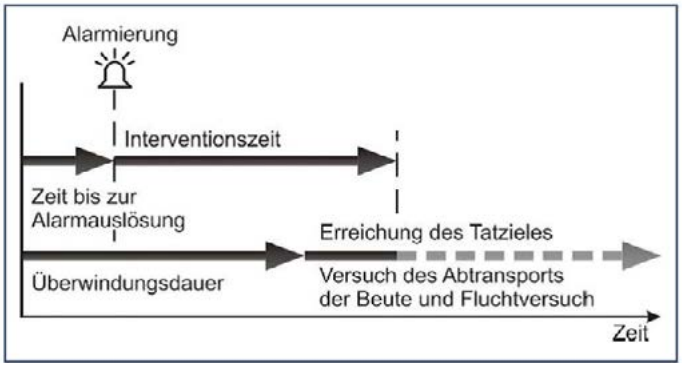
zu schützen.

Ziel der Perimeterüberwachung bzw. Freigeländesicherung ist es, dem potentiellen Täter den Weg von der Grundstücksgrenze zum Zielobjekt risikoadäquat zu erschweren, um eine Verzögerung zu erreichen (Erhöhung des Widerstandswertes), in der die Zeit ausreicht, zumindest innerbetriebliche Gegenmaßnahmen einzuleiten und diese Person in irgendeiner Form zu erfassen. Eine gesonderte Form stellt das Durchbrechen des Zauns mit einem Fahrzeug in Verbindung mit einem Blitzeinbruch dar, bei dem ein Eingreifen von Interventionskräften (Polizei, Sicherheitsdienst etc.) eher unwahrscheinlich ist. Hier gilt es möglichst viele Informationen zur Täteridentifizierung und -verfolgung zu sammeln. Abhängig von den Schutzzielen kann auch ein solcher Angriff mit baulich-mechanischen Maßnahmen erheblich erschwert oder verhindert werden.

Die Außengrenze sollte auch als solche „juristische Grenze" wahrgenommen werden. Eine lose Beschilderung, eine veränderte Grünbepflanzung oder ein anderer Bodenbelag – also eine fehlende feste Umschließung – sind nicht ausreichend, um ein Eindringen von Unbefugten zu unterbinden. Wenn unbefugte Personen eine hohe Hecke, einen Zaun, eine Palisade oder eine Mauer überwinden müssen, erhöht sich zum einen der Widerstandswert des Gesamtsystems und zum anderen kommt es zu einer zeitlichen Verzögerung, in der die Person diese juristische Grenze überwindet. Zudem ist in diesem Fall jedem klar, dass er Hausfriedensbruch begeht.



Herkömmliche Ausführung



Bevorzugte Ausführung

BEGINN UND PLANUNG DER AUSSENGELÄNDEÜBERWACHUNG

Ausgangspunkt für ein sicher funktionierendes Detektionssystem ist die lückenlose stabile Umgrenzung des Areals. Die Gefahren- und Risikoanalyse sowie die Definition der Schutzziele münden in Perimetersicherungsmaßnahmen. Diese beinhalten baulich-mechanische und elektronische Komponenten, die durch die organisatorischen und personellen Maßnahmen unterstützt werden. Im Vorfeld ist nicht nur die Angriffsrichtung zu definieren (von außen nach innen gilt beispielsweise für Gewerbe- und Industrieobjekte und von innen nach außen gilt beispielsweise für Justizvollzugsanstalten), sondern auch die Einteilung des Geländes in Sektoren sinnvoll.

ZIEL EINER FREIGELÄNDESICHERUNG KANN Z. B. SEIN, UNBEFUGTEN ZUTRITT ZUM BZW. AUFENTHALT AUF DEM FREIGELÄNDE/IM GELÄNDE MITTELS BAULICHER BARRIEREN UND (TECHNISCHER) ERKENNUNG SOWIE MELDUNG MIT ENTSPRECHENDER MASSNAHMENEINLEITUNG ZU ERSCHWEREN.

ZIEL DER PERIMETERÜBERWACHUNG IST DIE ÜBERWACHUNG DES „DRUMHERUM". DIES KANN BEISPIELSWEISE DIE GELÄNDE- ODER GEBÄUDEAUSSENGRENZE (ZAUN, MAUER ETC.) SEIN.

SEKTOREN MIT SCHUTZZIELBEISPIELEN

SEKTOR 0: Vorfeld (Geländestreifen)	Bereich sollte detektiert werden und sich daher innerhalb der juristischen Grenze befinden
SEKTOR 1: Perimetergrenze	Überwinden ohne Hilfsmittel soll verhindert werden (geschlossene Barriere)
SEKTOR 2: Perimeterbereich / Außengelände	unbefugtes Betreten soll detektiert werden
SEKTOR 3: Gebäudeaußenhaut oder sicherheitsrelevante Anlagen und Objekte	Eindringen, Beschädigen oder Entfernen soll verhindert werden (Achtung: ist unabhängig von der Außenhautüberwachung)

Beispielhafte Sektoreneinteilung

Abb. S.12-13 Zur Verfügung gestellt von der VdS Schadenverhütung GmbH

Beispielhafte Sektoreneinteilung

BAULICHE UND MECHANISCHE SICHERUNGSMASSNAHMEN

Bauliche und mechanische Sicherungsmaßnahmen sind in der Regel sehr aufwendig und im Nachhinein nur schwer umzusetzen. Doch dies ist meist die einzige Maßnahme, um einen Schaden verhindern zu können, da technische Systeme diese regulär nur melden.

Daher sollte eine herstellerneutrale und fachgerechte (Sicherheits-)Planung – die alle Umgebungseinflüsse berücksichtigt und beinhaltet – genau aufzeigen, welches Schutz- und Detektionssystem welchem Schutzzweck dient und dies auch in Plänen konkret verdeutlichen. In die Überlegungen zur Freigeländeüberwachung sind absehbare Gebäude- oder Geländenutzungsänderungen dringend einzubeziehen. Denn oftmals kann durch einen Umzug bzw. einer Umverlagerung des Schutzgutes auf eine kostengünstigere Sicherungsmaßnahme zurückgegriffen werden. Im Vorfeld muss natürlich auch der Kostenaufwand zwingend in Relation zur Effektivität der geplanten (Sicherheits-) Maßnahmen sowie im Hinblick auf die Schutzziele und etwaigen Kombinationsmöglichkeiten der Detektionsmaßnahmen, bestimmt werden. Dieser resultiert aus

- den Kosten der baulichen Absicherung,
- den Kosten, die durch die Detektion entstehen und
- den laufenden Betriebs- und Wartungskosten.

> **„BEI DER PLANUNG EINER PERIMETERÜBERWACHUNG SIND UNTERSCHIEDLICHE GEWERKE GEFRAGT WIE Z. B. STROMVERSORGUNG, MASTEN, BELEUCHTUNG, GARTEN- UND LANDSCHAFTSPFLEGE ETC.**

Je nach Ausgestaltung der Sicherungsmaßnahmen sind eine ausreichende Beleuchtung und eine Bestreifung des Areals als Unterstützung der Freigeländesicherung zu sehen.

ART DER MASSNAHME	ZIEL/BETRACHTUNG	BEISPIELE
Landschaftsbauliche Maßnahmen	Gezielte Änderung der landschaftlichen Umgebung.	Grünbepflanzung, Erdaufschüttung, Zaun, Mauer, Aushebung von Gräben, Anlegung von Gewässern, geänderte Verkehrsführung etc.
Bauliche Gegebenheiten	Bauwerke, die in der Nähe zur Grundstücksgrenze stehen, müssen betrachtet werden.	Höhe, Bewuchs, Aufstiegs- und Kletterhilfen prüfen etc.
Zäune und Mauern	Zutritte erschweren bzw. sensible Bereiche gezielt abtrennen.	Zaun oder Mauer mit angemessenem Übersteigschutz (Stacheldraht, Steckmetallgitter, Zackenleisten etc.)
Barriere-Öffnungen	Zu- und Abgänge separat voneinander betrachten.	Tore, Schranken, Poller, Türen, Drehkreuze, Drehsperren, Vereinzelungsanlagen etc.

Übersicht möglicher baulicher (Sicherheits-)Maßnahmen

SÄMTLICHE ÜBERWACHUNGSSYSTEME KÖNNEN EINZELN ODER AUCH IM VERBUND GENUTZT WERDEN, UM VERKNÜPFUNGEN UMZUSETZEN, SCHWACHSTELLEN AUSZUSCHLIESSEN SOWIE EINE REDUNDANTE SEKTORENABSICHERUNG ZU GEWÄHRLEISTEN.

TECHNISCHE SICHERUNGSMASSNAHMEN

Das Ziel der elektronisch unterstützten Freigelände-überwachungssysteme ist die frühzeitige Detektion von Unregelmäßigkeiten im Freigelände/Außenbereich sowie die Verlängerung der Reaktionszeit für Interventionsmaßnahmen. Für die Ausgestaltung ist neben dem Einsatzort/Sektor vor allem das Schutzziel zu berücksichtigen. Das jeweilige Funktionsprinzip (Sensorik) muss geeignet sein und sich an den Umgebungs- und Umweltbedingungen orientieren.

Doch jede Außengeländegrenze weist Lücken auf. Auch diese gilt es entsprechend abzusichern. Auf die Absicherung eines Gebäudes als Außengrenze wird an dieser Stelle nur bedingt eingegangen, da es hier noch andere Detektionsmöglichkeiten gibt, die nicht einzig auf das Eindringen über die Außenhaut ausgerichtet sind.

AUF DEN FOLGENDEN SEITEN FINDEN SIE EINE HILFREICHE DARSTELLUNG DER ARBEITSWEISE, SCHUTZWIRKUNG SOWIE DEN VOR- UND NACHTEILEN UNTERSCHIEDLICHER SICHERUNGSSYSTEME.

EIGNUNG DER VERSCHIEDENEN FREIGELÄNDEÜBERWACHUNGSSYSTEME

SYSTEM	DETEKTIONSPRINZIP	ARBEITSWEISE	SCHUTZWIRKUNG	VOR- UND NACHTEILE	EIGNUNG			
					BODENÜBER-WACHUNG	BARRIEREÜBERWA-CHUNG (ZAUN/MAUER)	GEBÄUDEAUSSEN-HAUT	VOLUMENÜBER-WACHUNG
Mikrofonkabel-system	Sensorkabel wird am Zaun befestigt	vom Zaun übertragene Schwingungen werden in elektrische Signale umgewandelt	übersteigen, durch-schneiden, durchstei-gen, durchfahren, überk-lettern (nur wenn Zaun berührt wird)	nachträgliche Installation und Empfindlichkeitsanpassung möglich, sichtbar verlegt (sabotageanfällig)		x	x	
Lichtwellenleiter-Sensorkabel	Sensorkabel wird am Zaun befestigt	vom Zaun übertragene Schwingungen werden in optische Signale (Reflektionsänderung) umgewandelt	übersteigen, durch-schneiden, durchstei-gen, durchfahren, über-klettern (nur wenn Zaun berührt wird), graben	nachträgliche Installation und Übertragung von Kommunikationsdaten möglich, auch für Kabeltrassen und Pipelines geeig-net, sichtbar verlegt (sabotageanfällig)	x	x	o	
Infrarot-Lichtschranken	IR-Sender und Empfänger werden am Zaun (Säulen) befestigt	Durchbruch der Lichtstrahls-Detektion	Objektdetektion bei Durchbruch des Lichtstrahls	eignen sich als Vorhangmelder und sind gut nachrüstbar, wetterbedingte Einschränkungen, Hügel und Mulden separat sichern, reflektiertes Licht, hoher Stromverbrauch, Beheizung der Montagesäulen		x	o	
Neigungs- und Beschleunigungs-sensorsysteme	Sensoren in Zaun oder Pfosten	Sensoren registrieren Erschütterungen	übersteigen, durch-schneiden, durchstei-gen, durchfahren, über-klettern (nur wenn Zaun berührt wird), graben	nachträgliche Installation und Empfindlichkeitsanpassung möglich, sichtbar verlegt (sabotageanfällig außer in Pfosten)		x		
Kapazitiver Feldänderungs-melder	parallel gespannte Drähte unter elektrischer Spannung	Änderung des elek-trischen Feldes bei Objektannäherung	übersteigen, durch-schneiden, durch-fahren, überklettern, unterkriechen	sehr Überwindungssicher, auf-wendige Montage eher für Hochsicherheitsbereiche		x		
Hochfrequenz-Meldekabel-systeme	Koaxial-Sensorkabel erzeugt elektromagne-tisches Feld	Erkennung der Feldänderung bei Objektannäherung	gehen, laufen, kriechen, graben, fahren	verdeckte Verlegung, nahezu für alle Untergründe (auch uneben) geeignet, Erdarbeiten erforderlich, Abstand zu Objekten erforderlich	x			
Seismische Melder	Mikro- bzw. Geofone im Mauerwerk oder der Erde	mechanische Schwingungen werden in elektrische Signale umgewandelt	gehen, laufen, kriechen, graben, fahren	verdeckte Verlegung, nahezu für alle Untergründe (auch uneben) und Betonflächen sowie Doppelböden ge-eignet, Erdarbeiten erforderlich	x		x	

Eignung der verschiedenen Freigeländeüberwachungssysteme

o bedingte Eignung x geeignet

EIGNUNG DER VERSCHIEDENEN FREIGELÄNDEÜBERWACHUNGSSYSTEME

SYSTEM	DETEKTIONSPRINZIP	ARBEITSWEISE	SCHUTZWIRKUNG	VOR- UND NACHTEILE	EIGNUNG			
					BODENÜBER-WACHUNG	BARRIEREÜBERWA-CHUNG (ZAUN/MAUER)	GEBÄUDEAUSSEN-HAUT	VOLUMENÜBER-WACHUNG
Druckänderungs-sensoren	detektieren Druckänderungen im Boden	(teilw. mit Flüssigkeit gefüllte) Schläuche geben Änderungen an Membran weiter (Umwandlung in elek-trische Signale)	gehen, laufen, kriechen, fahren	verdeckte Verlegung, nahezu für alle Untergründe (auch uneben) und Mauerwerk geeignet, Erdarbeiten erforderlich	x			
Laserscanner	zweidimensio-nale Abtastung mit Laserstrahlen	mittels Laufzeitmessung des reflektierten Lichts werden Objekte detektiert	durchsteigen, überklettern	Eignung als Vorhangmelder sowohl horizontal wie auch vertikal, Analyse der Objektgröße möglich, Schattenbildung kann nicht detek-tiert werden, wetterbedingte Einschränkungen		o	o	x
Passiv-Infrarot Bewegungsmelder	Erfassung abgestrahlter Wärme	Temperaturdifferenz wird detektiert	gehen, laufen, durchfahren	einfache Montage, Empfindsamkeit einstellbar, schnelle Temperaturänderungen negativ, wetterabhängig		o		x
Mikrowellen-sensoren	räumlich getrennte Sender- und Empfängereinheiten	Änderung des volume-trischen elektromagne-tischen Feldes erzeugt Alarm	gehen, laufen, kriechen, fahren	zuverlässig und witterungsunabhängig, eher für weite Überwachungsbereiche geeignet, Fremdsender (Störung), Durchdringung von Materialien, toter Bereich unterhalb des Melders				x
Radarmelder	kombinierte Sender- und Empfängereinheiten	Änderung des reflek-tierten Echos der elek-tromagnetischen Wellen erzeugt Alarm	gehen, laufen, kriechen, fahren	zuverlässig und witterungsunabhängig, eher für weite Überwachungsbereiche geeignet, Schattenbildung durch Baukörper schwierig				x
Videosensorik	verfolgt und erkennt Objekte in der Szene	typische Bewegungsmuster erzeugen Alarm	gehen, laufen, kriechen, fahren	vielseitig einsetzbar, einfache Verifizierung von Alarmen möglich, witterungsabhängig, Umgebung muss geeinet sein, ggf. mit IR-Kameras, Schattenbildung schwierig			o	x
Detektionszaun-systeme	ruhestromgeschützte Zaunüberwachung	Alarmdraht oder elek-trischer Leiter detektiert	durchbrechen, durch-schneiden, ggf. übersteigen (Abschereinrichtung)	sabotagesicher, nicht nachrüstbar		x		

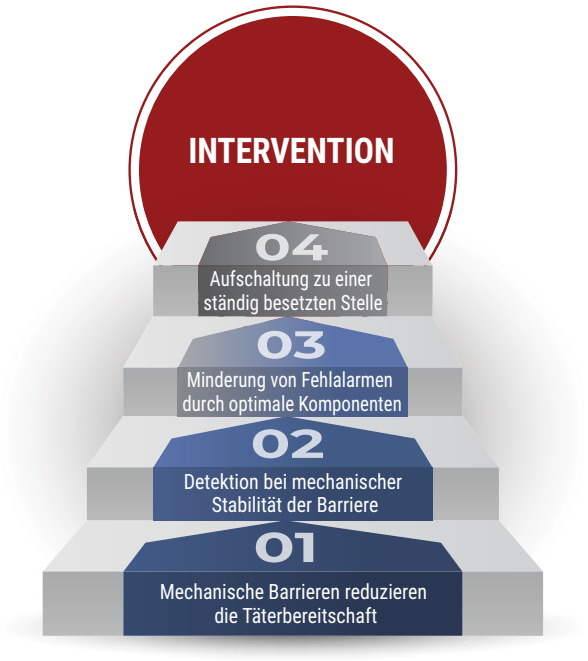
Eignung der verschiedenen Freigeländeüberwachungssysteme

o bedingte Eignung x geeignet

BAULICHE ABNAHME: UND WAS KOMMT DANACH?

Die Detektion muss auf eine Gefahrenmeldeanlage aufgeschaltet werden und in ein Gefahrenmanagementsystem münden, bei dem alle Meldungen (Perimetermeldung, Sabotagemeldung, Störungsmeldung in der Funktionsüberwachung oder Disqualifikation) getrennt voneinander – von einer ständig besetzten Stelle (z. B. interne/externe 24/7 Notruf- und Serviceleitstelle etc.) – ausgewertet und dokumentiert werden. Bei Verifikation der Alarmmeldung sind entsprechende Interventionsmaßnahmen (z. B. Verständigung der Polizei, Alarmverfolger/Interventionsdienst eines Sicherheitsdienstes etc.) einzuleiten.

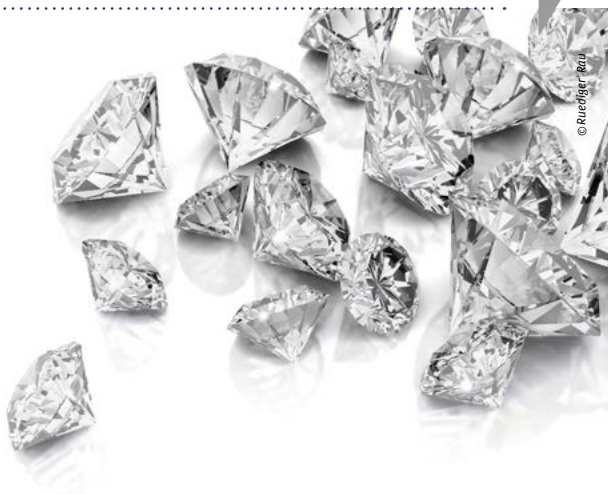
Ein Detektionssystem kann seine zuverlässige Arbeit nur dann leisten, wenn es ordnungsgemäß funktioniert. Daher sind regelmäßige Begehungen, Inspektionen sowie Wartungs- und Instandhaltungsarbeiten zwingend notwendig.



ACHTEN SIE DRINGEND AUF EINE ORDNUNGSGEMÄSSE SCHRIFTLICHE AUSFÜHRUNGS- UND BETREIBERDOKUMENTATION UND FÜHREN SIE IN JEDEM FALL EINEN MEHRTÄGIGEN PROBEBETRIEB IN KOMBINATION MIT EINER ENTSPRECHENDEN FACH-LICHEN EINWEISUNG DURCH. BEACHTEN SIE AUCH, DASS SICH DIE UMGEBUNGSBEDINGUNGEN IM JAHRESZEITLICHEN VERLAUF ÄNDERN KÖNNEN (SONNENSTAND, SCHNEE ETC.).

Dieser Artikel ist mit freundlicher Unterstützung der VdS Schadenverhütung GmbH entstanden. Weitergehende Informationen oder Musterabsicherungsbeispiele finden Sie im „Sicherungsleitfaden Perimeter“ (VdS 3143) oder der BHE-Broschüre „BHE-Planungsgrundlagen Freigeländeüberwachung“.

SCHUTZZIELE: DEFINITION VON „KRONJUWELEN“



Betriebliche Prozesse sollten so wenig Risiken wie möglich ausgesetzt sein. Dieses Bewusstsein findet sich vielerorts vermehrt im unternehmerischen Denken wieder. Bevor man sich jedoch über konkrete Sicherheitsvorkehrungen und -maßnahmen Gedanken macht, sollte man sich zunächst einmal mit der grundlegenden Identifikation und Definition der eigenen Schutzziele vertraut machen.

Schutzziele definieren das angestrebte Maß der geforderten Sicherheit vor natürlichen, menschlichen oder technischen Bedrohungen. In der betrieblichen Praxis werden Schutzziele erfahrungsgemäß nur äußerst selten konkret definiert. Hinzu kommt, dass Sicherheitsmaßnahmen häufig eher problemassoziativ (Vorfall X = Maßnahme Y) erarbeitet und geplant werden. Ein intensiver Austausch mit der Geschäftsleitung, der Entwicklungs- und Forschungsabteilung, der Produktionsleitung und/oder anderen wichtigen Abteilungen im Unternehmen kann aufzeigen, was die schützenswerten „Kronjuwelen“ überhaupt sind. Sind es spezielle Maschinen, Produktionsverfahren, Rezepturen, (Kunden-)Daten oder Forschungs- und Entwicklungsdaten? Was muss konkret vor fremdem Zugriff geschützt werden?

IDENTIFIZIEREN – BEWERTEN – SCHÜTZEN

Es ist nicht immer einfach, die essentiellen Elemente auf Anhieb zu identifizieren, zu klassifizieren und in entsprechender Reihenfolge zu priorisieren. Nach Einschätzung des Bundesamtes für Verfassungsschutz gehen die Sicherheitsbehörden davon aus, dass in Unternehmen nur etwa 5% der Informationen, Patente etc. zu den essentiellen „Kronjuwelen" zählen, also zu den Informationen und Werten, die ganz besonders schützenswert und vertraulich sind. Darunter können finanzielle, technische und andere geschäftliche Informationen und Dinge fallen. Gemäß der EU-Verordnung zum Technologietransfer zählen zu den vertraulichen Daten beispielsweise:

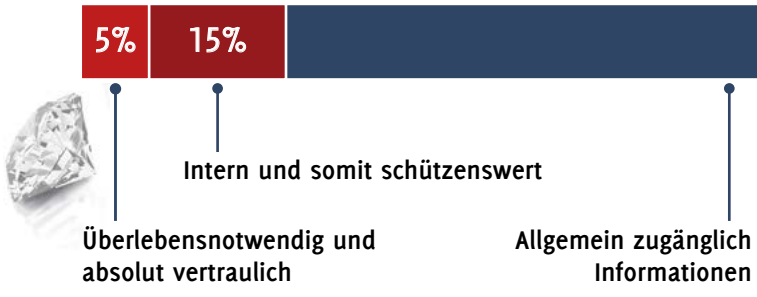
- Konstruktionsdaten, Schaltpläne, Kunden- und Vertragsdaten, Zuliefererkonditionen
- Preisberechnungen, interne Kostenaufschlüsselungen, Vorratshaltung von Zulieferteilen
- Markt- und Wachstumsstrategien, Marktforschungsdaten, Produkteinführungspläne
- Modelle, Prototypen, Programmcodes, Steuercodes, Produktentwicklungspläne
- Geschäfts-, Produktions-, Fertigungsprozesse
- Rezepturen, chemische Formeln, Laborbücher

WIE WERDEN SCHUTZZIELE DEFINIERT UND WAS KOMMT DANACH?

Bevor Schutzziele überhaupt definiert werden, sollte es ein Grundverständnis für die Zielsetzung und die individuellen betrieblichen Rahmenbedingungen geben. Für die weitere Bestimmung, insbesondere der „Kronjuwelen", sollten zudem innere und äußere Einflussfaktoren zur weiteren Beurteilung herangezogen werden wie z. B. rechtliche Rahmenbedingungen, versicherungsseitige Vorgaben, kundenseitige Vorgaben etc. Dies mündet oftmals in einer allgemeinen Definition, dass beispielsweise keine fremden Personen das Gelände betreten dürfen. Doch wie verhält es sich mit Besuchern, Dienstleistern oder Fremdmietern? Hier würde es beispielsweise mehr Sinn machen zu definieren, dass jede Person beim Zutritt identifiziert werden muss. Denn Schutzziele gelten als Beurteilungs- und Handlungsgrundlage für konkrete und angemessene Sicherheitsmaßnahmen und dienen zudem der Früherkennung von etwaigen Schwachstellen im Betrieb.

1. Schutzziel(e) definieren
2. Risiken identifizieren
3. Risikoursachen herausarbeiten
4. Anfälligkeiten zuordnen
5. Sicherheitsmaßnahmen ableiten und implementieren

„ERFAHRUNGSGEMÄSS SIND NUR ETWA 5% DER INFORMATIONEN, PATENTE ETC. IN EINEM UNTERNEHMEN ALS ABSOLUT VERTRAULICH ZU DEFINIEREN. DIESE 5% SOLLTEN JEDOCH UNTER KEINEN UMSTÄNDEN IN UNBEFUGTE HÄNDE GELANGEN!



DIE GENAUE DEFINITION DER „KRONJUWELEN" KANN AUCH NACHHALTIG DABEI HELFEN, SICH NICHT IN EINEM ÜBERHÖHTEN UND UNANGEMESSENEN MAßE VON DER AUSSENWELT ABZUSCHOTTEN, SONDERN NUR DORT EFFEKTIVE SICHERHEITSVORKEHRUNGEN UND -MASSNAHMEN EINZUSETZEN, WO SIE AUCH TATSÄCHLICH BENÖTIGT WERDEN.

Sind die „Kronjuwelen" definiert bzw. identifiziert, sollte genauestens betrachtet werden, WER? → WANN? → WAS? mit dem identifizierten Schutzziel und den darin enthaltenen Informationen und Werten im betrieblichen Alltag macht. Dabei ist das Vorgehen immer von innen – vom Kern – nach außen.

Letztlich mündet die Abwägung von Risikofaktoren, die dazu führen können, dass vertrauliche Informationen und Dokumente an Unbefugte gelangen, in konkreten Sicherheitsvorkehrungen und -maßnahmen baulicher, technischer, personeller und organisatorischer Art.

Schutzziele sollten generell auf ihre Vollständigkeit und ggf. Gültigkeit hin geprüft werden, denn jede Veränderung der individuellen inneren und äußeren Einflussfaktoren kann zu einer notwendigen Aktualisierung führen.

INTERVIEW ZUM THEMA ARBEITS- UND GESUNDHEITSSCHUTZRICHTLINIEN FÜR DIE ENTSENDUNG VON ARBEITNEHMERN INS AUSLAND

Das Projekt POOSH – „Occupational Safety and Health of Posted Workers" – betrachtet den Arbeitsschutz und die Einhaltung der Gesundheitsrichtlinien von entsandten Arbeitnehmern aus einer wissenschaftlichen Perspektive. Seit Januar 2017 führt der Lehrstuhl für Wirtschafts- und Gründungspädagogik der Universität Rostock in diesem zweijährigen Projekt Forschungsprozesse durch. Die Entsendung von Arbeitnehmern wird durch Artikel 3 der Richtlinie 96/71/EG über die Entsendung von Arbeitnehmern im Rahmen der Erbringung von Dienstleistungen geregelt und ist untrennbar mit der Gewährleistung menschenwürdiger Arbeit oder Arbeitsbedingungen verbunden. Ein entsandter Arbeitnehmer ist demnach ein Arbeitnehmer, der seine Arbeit für einen begrenzten Zeitraum im Hoheitsgebiet eines anderen Mitgliedstaates als dem Staat ausübt, in dem er normalerweise arbeitet.
Die Projektperspektive bezieht sich zwar ausschließlich auf die EU, dennoch kann man Schlussfolgerungen für eine weltweite Anwendung im Rahmen der Fürsorge- und Sorgfaltspflichten auch unter Sicherheitsaspekten ziehen. Viele Arbeitgeber unterschätzen die Herausforderungen in Bezug auf Arbeitssicherheit und Gesundheit in fremden, kulturell und ethnisch vielfältigen Arbeitsräumen.

DAS PROJEKT POOSH BESCHÄFTIGT SICH MIT DEM THEMA „ENTSENDUNG VON ARBEITNEHMERN". WAS GENAU WIRD UNTER EINEM „ENTSANDTEN ARBEITNEHMER" VERSTANDEN UND WELCHE BEDEUTUNG HAT DAS THEMA „ENTSENDUNG" AKTUELL IN DEUTSCHLAND?

Mit einer zunehmenden Arbeitskräftemobilität hat in den letzten Jahren die grenzüberschreitende Entsendung von Arbeitnehmern entscheidend an Bedeutung gewonnen. Ein „entsandter Arbeitnehmer" wird dabei als Arbeitnehmer bezeichnet, der seine Arbeit für einen begrenzten Zeitraum im Hoheitsgebiet eines anderen Mitgliedstaates (der EU) als in dem Staat ausübt, in dem er normalerweise arbeitet. Die Entsendedauer wird von Europäischem Parlament und Rat auf eine Zeit von maximal 24 Monate begrenzt.
Im Jahr 2016 wurden allein in der EU ca. 2,3 Millionen entsandte Arbeitnehmer verzeichnet, was einen Anstieg um 69% seit dem Jahr 2010 umfasst. Deutschland nimmt hierbei nicht nur aufgrund der hohen Empfängerzahlen von Arbeitskräften aus dem Ausland eine bedeutende Rolle ein. Im Jahr 2016 verzeichnete Deutschland über 260.000 Entsendungen ins Ausland und erwies sich damit nach Polen als das zweitstärkste Entsendeland in Europa. Mit dem Bedeutungszuwachs von Entsendungen treten auch arbeits- und gesundheitsschutzrechtliche Themen in den Vordergrund mit der Frage, wie nationale Gesetzesgrundlagen im Bereich Arbeitsschutz für entsandte Arbeitnehmern über Grenzen hinweg garantiert werden können.

FÜR DIE MITGLIEDSTAATEN DER EU GIBT ES EINDEUTIGE REGELUNGEN, WIE DIE FÜRSORGE- UND SORGFALTSPFLICHTEN DES ARBEITNEHMERS EINZUHALTEN SIND. WELCHE VERPFLICHTUNGEN SIND DAS?

Wenn Arbeitnehmer in ein anderes EU-Land entsandt werden, um eine temporäre Dienstleistung zu erbringen, gelten die Rechte und Vorschriften jenes Landes, in dem sie die Dienstleistungen erbringen. Dazu gehören auch Regelungen zu Gesundheit und Sicherheit am Arbeitsplatz. Eine Ausnahme stellt die Bestimmung zur Sozialversicherung des entsandten Arbeitnehmers dar.

DIE VORSCHRIFTEN ZUM SCHUTZ DER ARBEITGEBER SIND IN DEUTSCHLAND SICHERLICH AUF EINEM SEHR HOHEN NIVEAU, AUCH WAS DIE UMSETZUNG BETRIFFT. WIE SIEHT ES IN ANDEREN LÄNDERN MIT DEN ARBEITSSCHUTZRECHTLICHEN REGELUNGEN AUS?

Arbeitsschutzrecht ist nationales Recht – d. h. die hohen Standards, die in Deutschland durch Gesetzestexte wie das Arbeitsschutzgesetz, das Arbeitssicherheitsgesetz und das Sozialgesetzbuch VII rechtlich fixiert werden, gelten nur innerhalb der nationalen Grenzen. Das Arbeitsschutzrecht verschiedener Länder kann daher deutlich voneinander abweichen und muss bei einer Entsendung stets besondere Berücksichtigung finden. Ein Beispiel stellt hierbei die rechtliche Auslegung eines „Wegeunfalls" dar, welcher in Deutschland unter bestimmten Voraussetzungen als Arbeitsunfall ausgelegt, in anderen Nationalstaaten jedoch u. U. anders gesetzlich geregelt wird.
Im Zeichen einer Harmonisierung der arbeitsschutzrechtlichen Gesetze und Regelungen hat die Europäische Union in verschiedenen Richtlinien jedoch auch arbeitsrechtliche Mindeststandards und Maßnahmen festgelegt, die nicht unterschritten werden dürfen und in einzelstaatliches Recht umgesetzt werden müssen.
Doch auch was die tatsächliche

Um- und Durchsetzung der nationalen Rechtsvorschriften betrifft, bestehen große nationale Unterschiede. Diese Rechtsvorschriften sind jedoch letztlich Garant für die Absicherung der entsandten Arbeitnehmer.

WAS IST IHNEN IM RAHMEN DES PROJEKTES AUFGEFALLEN, WAS EINEN BESONDEREN STELLENWERT ODER EINE BESONDERE GEWICHTUNG VERDIENT?

Arbeitsplätze sind heute im besonderen Maße interkulturell geprägt und vereinen eine Vielfalt an Sprachen. Das Thema Sprache und Sprachbarrieren an einem interkulturellen Arbeitsplatz konnte im Rahmen der umfassenden Forschungsstudie des Projektes POOSH als bedeutsame Herausforderung identifiziert werden. Im Rahmen der POOSH-Studie konnte aufgezeigt werden, wie breit gefächert sich Sprachbarrieren entfalten und Arbeitsprozesse beeinflussen oder sogar gefährden können. Nicht nur die Kommunikation am Arbeitsplatz im Rahmen von Unterweisungen oder Gesprächen mit Vorgesetzen und Kollegen werden beeinträchtigt, sondern gleichsam das inhaltliche Verständnis der entsandten Arbeitnehmer in Bezug auf Schulungsunterlagen, Hinweisschilder oder Bedienungsanleitungen z. B. von Maschinen.

Die hieraus resultierenden Probleme und Risiken sind gleichsam vielfältig: Aus einer arbeits- und gesundheitsschutzrechtlichen Perspektive geht mit Sprachbarrieren vor allem ein erhöhtes Unfallrisiko einher, insbesondere in gefährlichen Sektoren, welche kurzfristige und langfristige Auswirkungen auf die Gesundheit der entsandten Arbeitnehmer haben können. Eine intensive Vorbereitung, Unterstützung und Qualifizierung des zu entsendenden Arbeitnehmers ist unerlässlich. Hier gibt es Ansätze verschiedener europäischer Länder dagegenzuwirken wie beispielsweise mehrsprachige Materialien, Online-Lexika und dergleichen.

ANMERKUNG DER REDAKTION: SPRACHBARRIEREN UND DAS INDIVIDUELLE SICHERHEITSVERSTÄNDNIS IN ANDEREN LÄNDERN INSBESONDERE IM HINBLICK AUF ETHIK, MORAL UND RELIGION KÖNNEN NATÜRLICH ZU ENORMEN DEFIZITEN IN BEZUG AUF DIE UNTERNEHMENSSICHERHEIT (SECURITY) FÜHREN.

DA DIE GLOBALISIERUNG UND SOMIT DIE WELTWEITEN TÄTIGKEITEN VON MITARBEITERN IMMER WEITER ZUNEHMEN, IST ES FÜR UNTERNEHMEN WICHTIG, SICH FRÜHZEITIG VOR EINER ENTSENDUNG ZU INFORMIEREN. WELCHE INFORMATIONSKANÄLE, PLATTFORMEN ODER DOKUMENTE KÖNNEN SIE HIER FÜR DEUTSCHE UNTERNEHMEN EMPFEHLEN?

Tatsächlich haben wir eine ganze Fülle an Informationsbroschüren und Plattformen zum Thema Entsendung ausfindig gemacht, die von unterschiedlichen Akteuren im Bereich Arbeits- und Gesundheitsschutz bereitgestellt werden, wie beispielsweise vom Bundesministerium für Arbeit und Soziales, dem Zoll, der Deutschen gesetzlichen Unfallversicherung und den Industrie- und Handelskammern.

DIESES THEMA GEWINNT SICHERLICH IN DEN KOMMENDEN JAHREN IMMER MEHR AN BEDEUTUNG. DAHER IST ES WICHTIG WELTWEIT EINHEITLICHE REGULARIEN ZUM SCHUTZ DER ARBEITNEHMER UND LETZTLICH DER MENSCHEN ZU DEFINIEREN. VIELEN DANK FÜR DIE ERKENNTNISSE UND WEITERHIN VIEL ERFOLG MIT DEM PROJEKT POOSH.

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.

TOOL

QUICK-CHECK ZUM THEMA CYBER-SECURITY

Die VdS Schadenverhütung GmbH hat auf ihrer Internetseite einen „Quick-Check für Cyber-Security“ zur Verfügung gestellt. Ziel des Quick-Checks ist es, sich einen groben aber informativen Überblick über die Cyber-Sicherheit ihres Unternehmens verschaffen zu können. Dargestellt wird dies in einer Risikomatrix auf Basis eines Ampelsystems. So können Sie bereits auf den ersten Blick erkennen, wo eventueller Handlungsbedarf besteht. Der „Quick-Check für Cyber-Security“ betrachtet nicht nur die Netzwerkumgebung, sondern auch organisatorische Regularien und Verantwortlichkeiten, die von der IT-Abteilung oftmals weniger Beachtung finden.

Beantworten Sie die Fragen zu sicherheitsrelevanten Themen aus den Bereichen

- Verantwortlichkeiten,
- Richtlinien,
- Schulungen und Vertraulichkeitsregelungen,
- Berechtigungen,
- mobile (End-)Geräte und Datenträger,
- Technik,
- Sicherheitsvorfälle,
- Datensicherung sowie
- Business-Continuity-Management.

Zusätzlich erhalten Sie zu jeder Frage Hintergrundinformationen und Erläuterungen. Im Anschluss der Auswertung erhalten Sie kostenfrei eine Einschätzung der Informationssicherheit im Unternehmen.

Nutzen Sie diese Möglichkeit, um für sich bzw. gemeinsam mit ihrer IT-Abteilung einen ersten Anhaltspunkt zu haben, wo Sie stehen. Den Test finden Sie auf der Internetseite **www.vds-quick-check.de**

TIPP

BSI FÜR BÜRGER: KOSTENFREIES ANGEBOT „INS INTERNET - MIT SICHERHEIT!“

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt im Bereich der Informations- und Kommunikationstechnik mit unterschiedlichen Ansätzen die präventive Förderung der Informations- und Cyber-Sicherheit. Das Thema „IT-Sicherheit“ sollte in der heutigen Informationsgesellschaft wahr- und ernstgenommen sowie eigenverantwortlich umgesetzt werden.

Die Sensibilisierung von Bürgern ist das Kernelement der Cyber-Sicherheitsstragegie, denn der Umgang mit Informationstechnik birgt bei allen positiven Möglichkeiten auch Risiken, die minimiert werden sollten.

Auf der Internetseite **www.bsi-fuer-buerger.de** werden vielfältige Themen auch für den technischen Laien verständlich behandelt. Neben reinen Informationsangeboten gibt es Handlungsempfehlungen und Mindeststandards, beispielsweise zu folgenden Themen:

- E-Mail Verschlüsselung
- Smartphone-Sicherheit
- Online-Banking
- Cloud-Computing
- Soziale Netzwerke
- W-LAN unterwegs sicher nutzen

Des Weiteren wurde eine Telefonhotline eingerichtet, an die sich Privatanwender mit Fragen rund um die IT- und Internetsicherheit wenden können. Zudem gibt es die Möglichkeit, sich für den kostenfreien Newsletter „Sicher informiert“ anzumelden. Darüber hinaus kann man sein Wissen in verschiedenen IT-Sicherheits-Quiz testen oder Podcasts zum Thema „Sicherheit im Internet“ hören.

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.