SICHERHEIT. DAS FACHMAGAZIN.

SICHERHEIT AUF DEN PUNKT GEBRACHT.

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.

SICHERHEIT. DAS FACHMAGAZIN.

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

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.

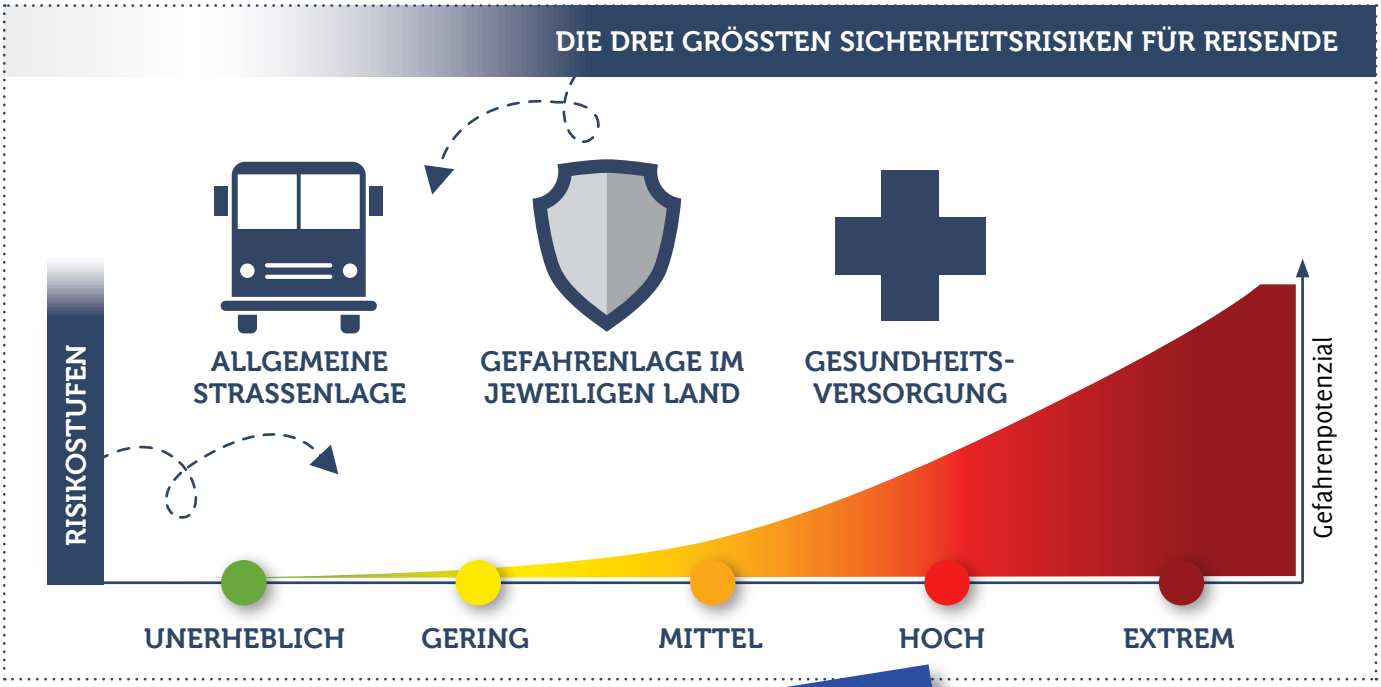
Ihre Vorteile:

› 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 „TRAVEL RISK MAP“ FÜR IHRE REISETÄTIGKEITEN

Die „Travel Risk Map“, welche jährlich veröffentlicht wird, ist die führende Prognose gegenüber politischen sowie sicherheits- und gesundheitsspezifischen Risiken auf internationalen Reisen und richtet sich dabei vor allem an Geschäftsreisende. Diese interaktiv gestaltete Weltkarte kann allen Reisenden im Unternehmen als schnelle Orientierungshilfe dienen und dabei unterstützen, etwaige länderspezifische Risiken bereits im Vorfeld optimaler einschätzen zu können.



Quelle: International SOS und Control Risks

Die oben dargestellten Risikostufen werden in einer interaktiven Weltkarte farblich dargestellt. Darüber hinaus werden auf weiterführenden Webseiten zusätzlich die politischen Situationen und gegebenenfalls daraus resultierende Risiken beleuchtet sowie individuelle und regionalspezifische Informationen zur Verfügung gestellt.

KATEGORISIERUNG VON VERTRAULICHEN INFORMATIONEN ALS PRÄVENTIVMASSNAHME GEGEN WIRTSCHAFTSSPIONAGE

In Unternehmen sowie bei Behörden und Organisationen gibt es eine Vielzahl von Informationen (und somit auch Daten), die sich in ihrer Wichtigkeit und Relevanz für den – meist wirtschaftlichen – zukünftigen Erfolg und ggf. sogar Fortbestand unterscheiden. Das Spektrum reicht von öffentlich zugänglichen Werbeunterlagen über vertrauliche Mitarbeiter- und Kundendaten bis hin zu hochsensiblen Ergebnissen aus Forschung und Entwicklung. Daher sollte die Geheimhaltung wichtiger Informationen von hoher Bedeutung sein, denn geraten derartige Informationen in die falschen Hände, könnte dies fatale Folgen haben.

Führungskräfte können beim Thema „Informationssicherheit" nicht zwangsläufig auf ein gemeinsames und einheitliches Verständnis im Unternehmen vertrauen. Vielmehr gilt es, Präventionsstrategien zu erarbeiten, die ungewollte Informationsabflüsse bereits frühzeitig verhindern.

Eine kürzlich veröffentlichte Studie („Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa"/ kurz WISKOS) kommt zu der Erkenntnis, dass „fast ein Fünftel der im Projekt befragten Unternehmen mit weniger als 50 Mitarbeitern über keine Strategie gegen physische Spionage oder Cyberangriffe verfügt." Dies ist in Anbetracht der öffentlich zugänglichen Zahlen von betroffenen und geschädigten Unternehmen, der Dunkelziffer sowie den beträchtlichen Schadenssummen pro (Sicherheits-)Vorfall nahezu unvorstellbar. Oftmals scheint bei den Unternehmen immer noch der Gedanken zu herrschen, dass gerade SIE für Täter doch absolut uninteressant seien. Doch weit gefehlt! In der heutigen Zeit der Digitalisierung und der damit einhergehenden Schnelllebigkeit sollten Unternehmen erst recht auf das eigene Know-how und deren wesentlich zu schützenden Informationen Acht geben.

WIRTSCHAFTSSPIONAGE bezeichnet das staatlich gelenkte Ausspähen, Ausforschen und Abgreifen von Daten und Informationen auf wirtschaftliche Akteure – also Unternehmen.

KONKURRENZ- BZW. INDUSTRIESPIONAGE hingegen ist das Ausspähen, Ausforschen und Abgreifen von Daten und Informationen durch Konkurrenten bzw. Mitbewerber.

DIE WEGE DES INFORMATIONSABFLUSSES

So, wie es die unterschiedlichsten Wege gibt, durch die Informationen in Unternehmen gelangen können, so gibt es auch eine Vielzahl von Wegen, wie Informationen wieder nach außen gelangen können – bewusst oder unbewusst. In Zeiten von Wirtschaftsspionage und Konkurrenzausspähung ist es essentiell, derartige Informationen und das vorhandene Wissen effektiv zu schützen. Doch wo oder wie setzt man dabei an? Denn der Täter ist nicht immer nur hinter der feindlichen Linie zu finden!

Generell sollte man bei Wirtschaftsschutzmaßnahmen folgende Tätergruppen berücksichtigen:

DER INNENTÄTER

Der Innentäter ist eine Person, die eine bestehende Rolle innerhalb des Unternehmens missbraucht (unzufriedener Mitarbeiter, neu eingestellter Mitarbeiter, Praktikant, Beschäftigter aus Drittunternehmen etc.).

DER AUSSENTÄTER

Der Außentäter ist eine Person, die über eine spezielle Vertrauensstellung innerhalb des Unternehmens verfügt (Besucher, Lieferanten, Fremde).

Innentäter können bewusst vorgehen oder unbewusst zum Täter werden, indem sie zur Informationsbeschaffung eines Außentäters missbraucht/ benutzt werden oder gar als eigentlicher Außentäter in das Unternehmen eingeschleust werden. Oftmals erfolgt die Weitergabe von Informationen durch Innentäter allerdings nicht mit böser Absicht, sondern eher durch Unwissenheit, Fahrlässigkeit oder mangelnden Weitblick.

> UNABHÄNGIG VON PHYSISCHEN ZUGANGSBARRIEREN, INTERNEN SICHERHEITSVORSCHRIFTEN, IT-SICHERUNGSMASSNAHMEN ODER REGELMÄSSIGEN MITARBEITERSENSIBILISIERUNGEN SOLLTEN INFORMATIONEN JE NACH SCHUTZBEDARF ENTSPRECHEND KLASSIFIZIERT WERDEN.

DATEN sind Symbole und Zeichen, deren Bedeutung nur im Kontext zu verstehen ist. Daten stellen Informationen formal dar.

INFORMATIONEN stellen Daten in einer komplexeren Kontextebene dar. Somit sind Informationen Kenntnisse über Sachverhalte oder Personen.

KLASSIFIZIERUNG VON INFORMATIONEN

Eine „Klassifizierung von Informationen" bedeutet, dass Informationen und Daten in unterschiedliche Sicherheitsklassen kategorisiert werden. Dabei bestimmt sich der Wert einer Information durch den Schaden, der dem Unternehmen im Falle eines unerwünschten Bekanntwerdens entstehen könnte. Diese Informationsklassifizierung kennt man auch aus dem Bereich der Sicherheitsbehörden oder des Militärs. Unterschieden wird dabei zwischen vier Vertraulichkeitsstufen:

BEGRIFFE IN UNTERNEHMEN	BEGRIFFE IN BEHÖRDEN/ ÖFFENTLICHEN EINRICHTUNGEN
frei zugänglich	Verschlusssache - nur für den Dienstgebrauch
intern	Verschlusssache - vertraulich
vertraulich	geheim
streng vertraulich	streng geheim

Bei der Kategorisierung der internen Daten ist es wichtig, dass alle Abteilungen aktiv beteiligt werden und daran mitwirken, da jede Abteilung für sich selbst am besten weiß, welche Daten und Informationen besonders sensibel sind. Bedenken Sie bei der Kategorisierung stets, dass es dabei nicht nur um elektronische Daten und Informationen geht, sondern auch um Dokumente in Papierform.

Um wichtige Daten von Unwichtigen zu trennen, sollten zunächst einmal die Informationen klassifiziert werden. Hierbei können verschiedene Anforderungsarten relevant sein:

- Unternehmensweit definierte Klassifizierungen wie beispielsweise Vertraulichkeit, Relevanz für den Betrieb, Schaden bei Verlust etc.
- Anforderungen von Geschäftspartnern, Kunden oder Behörden etc.
- Rechtliche oder regulatorische Anforderungen, z. B. aus der europäischen Datenschutz-Grundverordnung, dem BSI-Grundschutz 100-2, der ISO 27001 etc.

Mithilfe dieser Klassifizierung lassen sich schützenswerte Daten und Informationen bereits näher identifizieren. ›››

	INTERNER GEBRAUCH	VERTRAULICH	STRENG VERTRAULICH
SCHADENS-AUSMASS	▪ keine weitreichenden Konsequenzen	▪ Betroffen ist ein spezieller Unternehmensbereich (z. B. finanzieller Schaden, rechtliche Konsequenzen bis hin zu Ordnungswidrigkeiten und Geldstrafen etc.) ▪ (Vertrauens-)Verlust einzelner Kunden oder Lieferanten (z. B. personenbezogene Daten gem. Bundesdatenschutzgesetz etc.)	▪ Betroffen ist das gesamte Unternehmen (z. B. rechtliche Konsequenzen bis hin zu Haftstrafen, Imageverlust, Vertrauensverlust, Schaden für weitere Geschäftszweige und -ziele)
BEISPIELE	▪ Organigramme ▪ Arbeitsanweisungen ▪ Protokolle	Informationen, die im Rahmen von Vertraulichkeitsvereinbarungen erlangt wurden ▪ EDV-Daten ▪ Kalkulationen ▪ Arbeitsverträge ▪ Mitarbeiterbeurteilungen ▪ Bewerberunterlagen	▪ Forschungsunterlagen ▪ Entwicklungspläne ▪ Strategiepläne ▪ Passwörter ▪ relevante Daten zu Neuproduktentwicklungen ▪ Kundenlisten ▪ Einkaufsbedingungen bei Lieferanten
KENNZEICHNUNG	▪ auf jeder Seite	▪ auf jeder Seite ▪ Empfängerliste empfohlen	▪ auf jeder Seite ▪ Empfängerliste notwendig ▪ Zusatzangaben auf dem Deckblatt
VERTEILUNG/ VERVIEL-FÄLTIGUNG	▪ nur unternehmensintern ▪ an Dritte nur nach schriftlicher Vereinbarung ▪ Kopieren erlaubt	▪ nur an berechtigte Personen ▪ an Dritte nur nach schriftlicher Vereinbarung ▪ Kopieren nur nach Rücksprache mit Urheber erlaubt	▪ jedes Exemplar (ggf. mit Kennung) registrieren ▪ nur an namentlich bekannte Personen ▪ Verteiler- und Zugriffsliste anlegen ▪ keine Weitergabe an Dritte (in Sonderfällen mit Rechtsabteilung klären) ▪ Kopieren verboten
VERSAND/ ÜBERTRAGUNG	▪ intern kein Umschlag notwendig ▪ extern mit Umschlag ▪ elektronische Übertragung, wenn möglich mit Verschlüsselung	▪ intern und extern im Umschlag mit Versandvermerk „Persönlich oder Vertreter“ ▪ elektronische Übertragung nur verschlüsselt	▪ persönliche Überbringung (z. B. via Kurier) ist vorzuziehen ▪ extern nur als Übergabe-Einschreiben; intern 2 Umschläge mit Versandvermerk „Persönlich oder Vertreter“ + Namenszug auf dem inneren Umschlag ▪ Empfangsbestätigung schriftlich einholen ▪ elektronische Übertragung nur verschlüsselt
AUFBEWAHRUNG	▪ Außenstehenden nicht zugänglich ▪ Bei Mitnahme Kenntnisnahme durch Unbefugte verhindern	▪ unter Verschluss halten (vorzugsweise in verschlossenem Aktenschrank) ▪ verschlüsselte Aufbewahrung bei elektronischen Daten ▪ bei Mitnahme, speziell auf Reisen, erhöhte Vorsicht	▪ unter Verschluss halten (vorzugsweise im Tresor) ▪ verschlüsselte Aufbewahrung bei elektronischen Daten ▪ Mitnahme, speziell auf Reisen, nur in besonderen Ausnahmefällen und nur mit schriftlicher Genehmigung

Klassifizierung und Umgang mit Daten und Informationen

ACHTUNG! UNERWÜNSCHTER INFORMATIONSABFLUSS KANN ZUR PERSÖNLICHEN HAFTUNG DER GESCHÄFTSLEITUNG FÜHREN. INFORMATIONSSICHERHEIT IST FÜHRUNGSAUFGABE!

FESTLEGUNG VON SCHUTZMASSNAHMEN

Definieren Sie gemeinsam mit dem Datenschutzbeauftragten und der Führungsebene auf Basis der Datentrennung und -identifizierung angemessene Nutzungsberechtigungen sowie technische und organisatorische Schutzmaßnahmen. Dabei hängt die konkrete Ausprägung von den individuellen Bedürfnissen und der individuellen Unternehmensphilosophie ebenso ab wie das generelle Bewusstsein über die Gefahren von durch Dritte genutzte Informationen aus dem eigenen Unternehmen. Die ganzheitliche Implementierung von Maßnahmen zur Informationssicherheit kann dem wirtschaftlichen Selbsterhalt des Unternehmens sowie der etwaigen Erfüllung von rechtlichen und regulatorischen Anforderungen nachhaltig dienen.

Die Einhaltung der Schutzmaßnamen steht und fällt mit den Mitarbeitern. Jeder Mitarbeiter, der tagtäglich mit Unternehmensdaten zu tun hat, muss unternehmerische Informationen aktiv schützen. Mit der Datenkategorisierung werden Regeln im Umgang mit Informationen im Unternehmen entstehen, die den Mitarbeitern nahegebracht werden müssen. Dies kann beispielsweise in Form eines Leitfadens, einer Schulung oder einer Informationssicherheitsrichtlinie erfolgen.

In unserem Downloadbereich finden Sie ein kostenfreies Beispiel für eine „Informationssicherheitsrichtlinie" zur Verwendung im eigenen Unternehmen.

„ NEBEN EINER KLAREN RICHTLINIE, WIE WELCHE DATEN BEHANDELT WERDEN MÜSSEN, IST DIE UNTERSTÜTZUNG DURCH DAS MANAGEMENT UNABDINGBAR.

VIDEOÜBERWACHUNG: RECHTLICHE ANFORDERUNGEN UND GRENZEN IM ÜBERBLICK

Die Ausweitung der Videoüberwachung im öffentlichen und nicht-öffentlichen Raum gewinnt immer mehr an Bedeutung. Der Fortschritt der Technik und neue gesetzliche Regelungen stellen die Nutzer zunehmend vor neue Herausforderungen. Damit einhergehend stellt sich die Frage, welche Anforderungen an eine Videoüberwachungsanlage zu stellen sind, damit die Aufnahmen in einem späteren Strafermittlungsverfahren ausreichende Beweiskraft erlangen.

Der Ursprung des Einsatzes von Kameras findet sich bereits in den 50er Jahren in der Verkehrsbeobachtung und später auch der Verkehrslenkung. Mit der Beobachtung von Versammlungen und der Möglichkeit der Strafverfolgung (Beweislast) hielt die Videoüberwachung immer mehr Einzug in die Polizeiarbeit.

Heute und auch zukünftig wird die Videoüberwachung immer mehr ein Instrument der Sicherheitsstrategie in Unternehmen und Organisationen, um mit Hilfe von intelligenten Systemen (Mustererkennung) präventiv tätig werden zu können. Mit dem zunehmenden Einsatz solcher Technik wurden rechtliche Anforderungen geschaffen, die die Akzeptanz verbessern sollen und einen gesetzlichen Rahmen (Schutz) schaffen sollen.

VIDEOÜBERWACHUNG UND DATENSCHUTZ (INTERESSENABWÄGUNG)

EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Das Inkrafttreten der DSGVO im Mai 2018 hat die Bevölkerung für Datenschutzthemen wachgerüttelt und führt auch im Bereich des Videokameraeinsatzes zu vielen Fragen. Die DSGVO enthält jedoch keine spezifischen Regelungen zur Videoüberwachung. Da diese einen Anwendungsvorrang vor dem Bundesdatenschutzgesetz (BDSG) hat, ist fraglich, ob und inwieweit die Regelungen des § 4 BDSG (Videoüberwachung öffentlich zugänglicher Räume) zu beachten sind.[1]

In erster Linie ist daher die Videoüberwachung durch nicht-öffentliche Stellen auf die Generalklausel des Art. 5 Abs. 1 DSGVO abzustimmen. Demnach ist die Verarbeitung rechtmäßig, soweit sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte oder Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Die zu prüfenden Kriterien nach Art. 6 Abs. 1 DSGVO entsprechen im Wesentlichen denen des BDSG. Demnach ist die Videoüberwachung nur zur Wahrung berechtigter Interessen zulässig, wenn diese erforderlich ist und zuvor eine Interessenabwägung erfolgte. Neu ist, dass unter der Wahrung berechtigter Interessen auch sog.

[1] *Vgl. DSK (2018). Videoüberwachung nach der Datenschutzgrundverordnung, Kurzpapier Nr. 15, Verlag o. A.., S.1*

„Drittinteressen“ fallen. Dies ist z. B. dann der Fall, wenn ein Vermieter für seine Mieter die Videoüberwachung betreibt. Die Erforderlichkeitsprüfung umfasst, dass die Videoüberwachung nur dann als Maßnahme zu wählen ist, wenn weniger tiefgreifende Maßnahmen in das Recht auf Schutz der personenbezogenen Daten nicht zum Erfolg führen. Diesen rechtlichen Anforderungen kann durch einen entsprechenden Aushang entsprochen werden.

§ 4 BDSG - VIDEOÜBERWACHUNG
(§ 6 B BDSG - ALT)

Mit der Novellierung des § 6 b BDSG haben sich keine wesentlichen Änderungen ergeben. Die Videoüberwachung in öffentlich zugänglichen Bereichen (z. B. Tankstellen, Cafés, Shoppingcenter, Hotelfoyers etc.) darf durch öffentliche Stellen des Bundes und nicht-öffentliche Stellen durchgeführt werden. Bei diesen Orten handelt es sich um Räume, die öffentlich zugänglich sind, dem öffentlichen Verkehr gewidmet sind oder durch einen unbestimmten Personenkreis betreten werden dürfen. Die Videoüberwachung muss zur Aufgabenerfüllung dienen und zur Wahrung des Hausrechts oder anderer berechtigter Interessen erforderlich sein. Der Umstand der Beobachtung und die verantwortliche Stelle sind durch textliche Hinweisschilder oder Symbole kenntlich zu machen. Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind.

VIDEOÜBERWACHUNG DURCH SICHERHEITSBEHÖRDEN

Die Videoüberwachung zur Strafverfolgung ist nach § 100 c StPO ohne Wissen des Betroffenen rechtlich zulässig. Allerdings nur, wenn die Erforschung des Sachverhalts oder die Ermittlung des Täters auf andere Weise wenig Erfolg versprechend oder erschwert wäre und sich bestimmte Tatsachen auf eine im Gesetz genannte schwere Straftat begründen.

Im Zusammenhang mit öffentlichen Versammlungen dürfen z. B. nach §§ 12 a, 19 a Versammlungsgesetz Bildaufnahmen angefertigt werden, wenn Tatsachen die Annahme rechtfertigen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen. Die Gefahrenabwehrgesetze der Länder sehen darüber hinaus weitergehende Regelungen zur Videoüberwachung vor.[2]

ANFORDERUNGEN AN DIE VIDEOÜBERWACHUNG UND DEREN BEWEISKRAFT

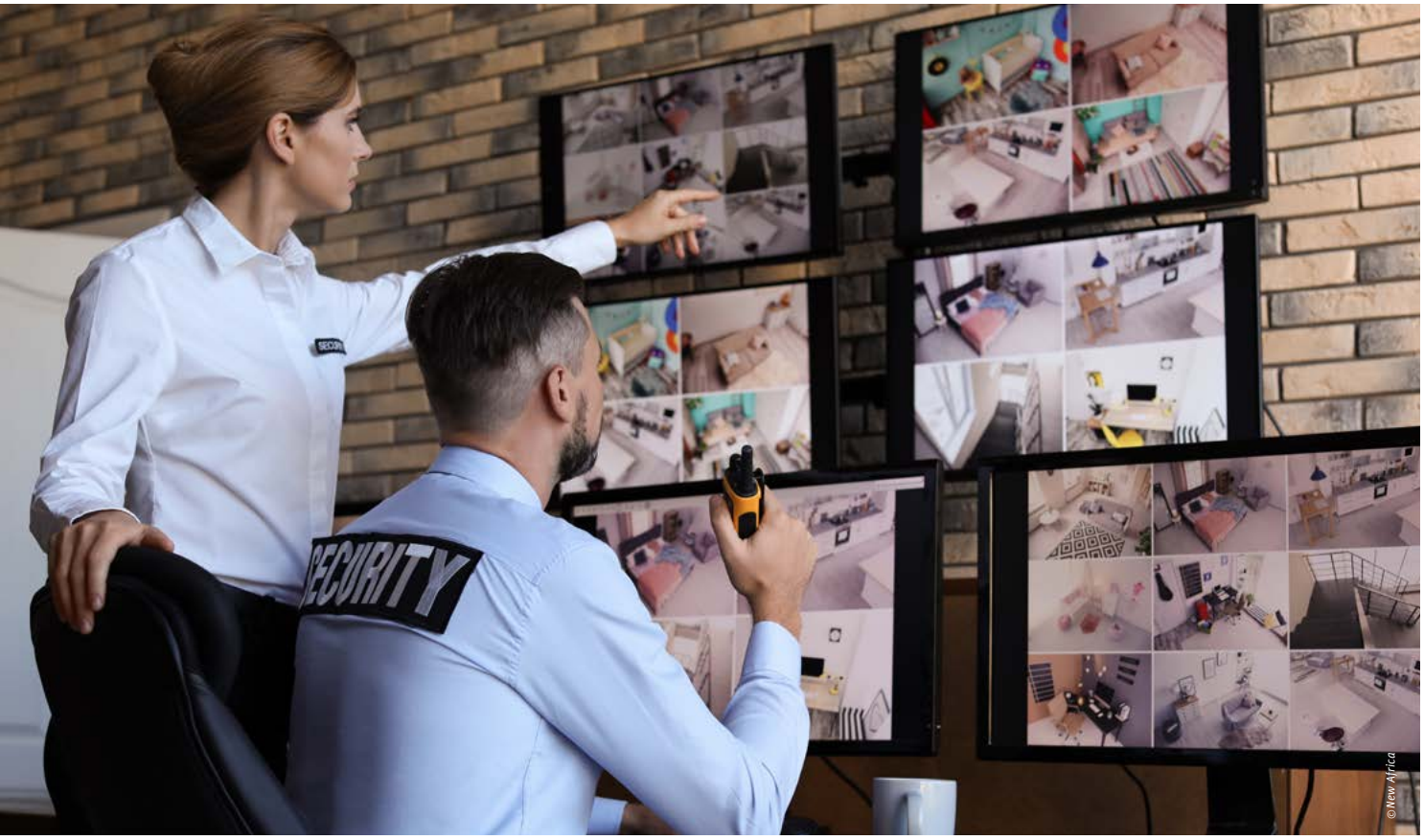
Der Literatur und der Rechtsprechung sind weitestgehend keine Hinweise zu entnehmen, die Aussagen zu den technischen Anforderungen einer Videoüberwachungsanlage treffen, damit diese Bilder auch im späteren Strafermittlungsverfahren als Beweismittel geeignet sind. Anders stellt sich dies in gerichtlichen Urteilen zu Verkehrsordnungswidrigkeiten dar. Demnach muss das Gericht durch die Inaugenscheinnahme der Aufnahme und des Betroffenen zu dem Ergebnis kommen, dass es sich zweifelsfrei um dieselbe Person handelt. Entscheidend ist hierbei die Qualität der Aufnahme, insbesondere der Kontrast, die Schärfe und die Frontansicht der Person.[3] Diese Aussage deckt sich auch mit den Erfahrungen der Strafverfolgungsbehörden. Diese stellen hinsichtlich der Anforderungen auf die Identifikation der Person ab. Also dem zweifelsfreien Erkennen des Täters. Weiterhin muss technisch gewährleistet sein, dass die Aufnahmen nicht zu einem späteren Zeitpunkt verfälscht wurden (Originalität). Darüber hinaus sind die Gesamtumstände der Videoüberwachung relevant, wie das Urteil vom Amtsgericht Castrop-Rauxel zeigt. Der Frontansicht der Person sollte durch einen geringen Neigungswinkel der Kamera Rechnung getragen werden, um Verzerrungen zu vermeiden. Zu beachten sind hierbei auch die Lichtverhältnisse, um Schattenbildungen weitestgehend auszuschließen. Daher sollte der Überwachungsbereich stets gut ausgeleuchtet sein. ›››

Aus der DSGVO ergeben sich neben den RECHTMÄSSIGKEITSANFORDERUNGEN auch weitergehende INFORMATIONSPFLICHTEN. Die verantwortliche Stelle hat folgende Mindestanforderungen zu beachten:

- Information über den Umstand der Beobachtung durch Hinweisschilder,
- Name und Kontaktdaten der für die Videoüberwachung verantwortlichen Person,
- Hinweis zu dem betrieblichen Datenschutzbeauftragten,
- Rechtsgrundlage der Videoüberwachung und Zweck sowie Erläuterung des berechtigten Interesses,
- Dauer der Speicherung der Daten sowie
- weitergehende Informationen zum Auskunfts- und Beschwerderecht sowie dem Empfänger der Daten.

[2] *Vgl. Zilkens, Martin (2007). Videoüberwachung, eine rechtliche Bestandsaufnahme, in: DuD 31 (2007), S. 279*

[3] *Vgl. AG Castrop-Rauxel. Urteil vom 22. Januar 2016 – 6 Owi 200/15-, juris, S. 2*



DASHCAMS

Der Bundesgerichtshof (BGH) hat sich mit der Frage befasst, ob die fortlaufende Aufzeichnung einer Dashcam, die den Verkehrsraum dauerhaft anlassunabhängig aufnimmt, als Beweismittel zulässig sei. Der BGH kam zu dem Ergebnis, dass eine anlasslose dauerhafte Aufzeichnung des Verkehrsraums gegen § 4 BDSG a.F. verstoße, da dies insbesondere auch technisch vermeidbar wäre. Hinsichtlich der Verwertbarkeit in einem Zivilprozess führte der BGH aus, dass die Unzulässigkeit oder Rechtswidrigkeit der Beweiserhebung nicht auch automatisch zu einem Beweisverwertungsverbot führe. Vielmehr sei eine Abwägung der Interessen des Klägers und des Beklagten vorzunehmen, so dass zumindest eine Inaugenscheinnahme der Aufnahme durch das Gericht zulässig sei.[4]

AUSSAGEN ZU EINSATZMÖGLICHKEITEN

VIDEOKAMERA-ATTRAPPEN SIND UNZULÄSSIG

Attrappen, auch wenn sie tatsächlich keine Videoüberwachung darstellen, sind rechtlich unzulässig. Sie stellen einen nicht gerechtfertigten Eingriff in das allgemeine Persönlichkeitsrecht dar. Dies ist insbesondere dann der Fall, wenn zur Abwehr von Gefahren auch weniger einschneidende Mittel zur Verfügung stehen. Denn ein Eingriff liegt nicht nur dann vor, wenn tatsächlich eine Überwachung erfolgt, sondern auch dann, wenn Dritte eine Überwachung bereits ernsthaft befürchten müssen. Es kann dadurch ein Überwachungsdruck und somit auch eine Befangenheit des Verhaltens eintreten.[5]

VIDEOÜBERWACHUNG AM ARBEITSPLATZ - INTERESSENABWÄGUNG

Bei der Überwachung am Arbeitsplatz ist das schutzwürdige Allgemeine Persönlichkeitsrecht des Arbeitsnehmers gegenüber dem Interesse des Unternehmers abzuwägen.[6]

Die Gewichtung und Abwägung ist in erster Linie von dem Zweck anhängig. Das Interesse des Arbeitgebers überwiegt in der Regel, wenn die Videoüberwachung der Gefahrenabwehr oder der Zugangskontrolle dient.[7] Die Überwachung sensibler Bereiche sowie mit dem Ziel der Leistungs- und Verhaltenskontrolle ist grundsätzlich unzulässig, da das Allgemeine Persönlichkeitsrecht überwiegt.[8] Sofern die Mitaufzeichnung des Arbeitsnehmers nur eine Nebenfolge darstellt, ist die Videoüberwachung zulässig. In jedem Fall ist im Vorfeld der Zweck der Videoüberwachung festzulegen.

[4] *Vgl. Kunkel | Kunkel, jurisPR-Compl 4/2018 Anm. 4, S. 2 ff.*

[5] *Vgl. WuM 2018, 654-656*

[6] *Vgl. Jerchel, Kerstin / Schubert, Jens (2015). Videoüberwachung am Arbeitsplatz – eine Grenzziehung, in: DuD 3 (2015), S. 151*

[7] *Vgl. Zilkens, Martin (2007). Videoüberwachung, eine rechtliche Bestandsaufnahme, in: DuD 31 (2007), S. 283*

[8] *Vgl. BAG, Beschluss vom 29.06.2004, AZ 1 ABR 21/03, DUD 2004 747*

MINDESTANFORDERUNGEN AN DEN EINSATZ VON VIDEOÜBERWACHUNGSTECHNIK

Für eine optimale Zielerreichung der Videoüberwachungsanlage sind folgende Vorgaben einzuhalten:

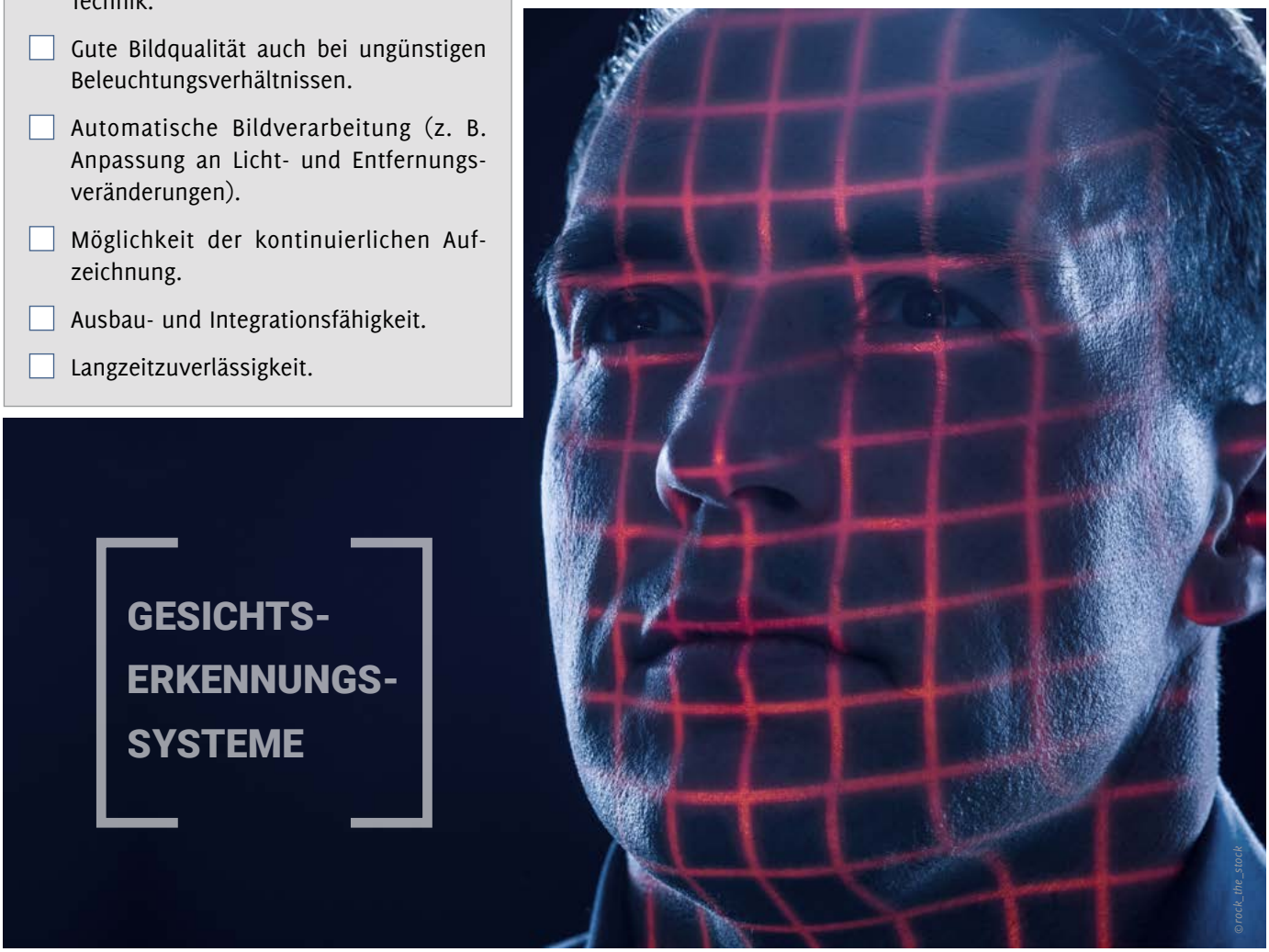
- ☐ Weitestgehend lückenlose Überwachung.
- ☐ Begrenzung der Überwachungsbereiche der einzelnen Kameras aus technischen und datenschutzrechtlichen Gründen.
- ☐ Einsatz von Kameras mit der Möglichkeit zum Schwenken, Neigen und Zoomen.
- ☐ Bildaufzeichnung der Videobilder mit voller Auflösung.
- ☐ Hohe Bildfolgerate, angemessene Bildqualität und geeignete Steuerfunktionen.
- ☐ Einsatz von hochauflösenden Kameras (z. B. Megapixel-Kameras) gemäß dem Stand der Technik.
- ☐ Gute Bildqualität auch bei ungünstigen Beleuchtungsverhältnissen.
- ☐ Automatische Bildverarbeitung (z. B. Anpassung an Licht- und Entfernungsveränderungen).
- ☐ Möglichkeit der kontinuierlichen Aufzeichnung.
- ☐ Ausbau- und Integrationsfähigkeit.
- ☐ Langzeitzuverlässigkeit.

INTELLIGENTE VIDEOÜBERWACHUNG ALS ZUKUNFTSTECHNOLOGIE

Die intelligente Videoüberwachung gleicht die Gesichter von Personen, die in einem gekennzeichneten Bereich erfasst werden, mit Lichtbildern von Personen ab, die in einer Datenbank gespeichert sind. Dadurch sollen Übereinstimmungen festgestellt werden (automatisierte Gesichtserkennung). Des Weiteren werden im Zuge der intelligenten Videoanalyse bestimmte Verhaltensmuster ausgewertet (wie z. B. liegengelassene Gegenstände, Personenströme etc.).

ANFORDERUNGEN AN VIDEOÜBERWACHUNGSSYSTEME

Weitere Hinweise zu den Anforderungen an ein Videoüberwachungssystem sind dem Leitfaden des BSI zur „IT-Forensik“ zu entnehmen. Dieser führt unter anderem aus, dass an eine forensische Untersuchung besondere Anforderungen an die Integrität der Daten und somit ihrer Sicherung gestellt werden. Sichergestellte Spuren dürfen durch die Untersuchung nicht unbemerkt verändert worden sein. Die Sicherung der Integrität digitaler Beweise muss jederzeit belegbar sein. Es muss sichergestellt werden, dass zu jedem Zeitpunkt beginnend mit der Erfassung der digitalen Beweisspuren ein potentieller Missbrauch beziehungsweise eine Verfälschung nachgewiesen werden kann.[9] ›››



[9] *Vgl. BSI (2008). Leitfaden „IT-Forensik“, Version 1.0.1 (März 2011), Verlag o. A., S. 23*

Bei der Projektierung, der Installation sowie dem Betrieb der Videoüberwachungsanlage sollte der jeweilige „Stand der Technik“ zugrunde gelegt und eingehalten werden.[10] Für den Bereich der Videoüberwachungstechnik sind daher insbesondere folgende europäische und nationale Normen sowie Richtlinien in der jeweils neuesten veröffentlichten Fassung zu beachten:

- DIN EN 50132 (CCTV-Überwachungsanlagen für Sicherheitsanwendungen).
- VdS 2364 (VdS Richtlinie für Videoüberwachungsanlagen – Systemanforderungen).
- VdS 2366 (VdS Richtlinie für Videoüberwachungsanlagen – Planung und Einbau).

Die Planung und Installation der Videoüberwachungsanlage sollte durch einen VdS-anerkannten Errichter erfolgen.

Ohne den Einsatz intelligenter Videoüberwachungssysteme lässt sich der kriminalpräventive Ansatz nur schwer nachweisen.

KRITISCHE UND ABSCHLIESSENDE BETRACHTUNG DER VIDEOÜBERWACHUNG[11]

1. Eine lückenlose und vollständige Videoüberwachung ist meist nicht möglich. Potentielle Täter werden verdrängt und weichen auf unbeobachtete Bereiche aus.
2. Die Detektion von Fehlalarmen und deren Intervention können Sicherheitsrisiken auslösen.
3. Videoüberwachung kann zu einem trügerischen Sicherheitsgefühl führen, wenn kein ausreichendes Interventionspersonal zur Verfügung steht und/oder die Videoüberwachung nicht durch qualifiziertes Personal permanent betreut wird.
4. Die Beweiskraft ist aufgrund eventueller Manipulationsmöglichkeiten begrenzt oder fragwürdig.
5. Hilfeleistungen unterbleiben, da feststellende Personen auf die Unterstützung und das Handeln professioneller Sicherheitsdienste und -behörden vertrauen.

[10] *Vgl. Welzbacher, Sebastian (2012). Planung eines Videoüberwachungssystems, Diplomica Verlag, Hamburg, S. 4 ff.*

[11] *Vgl. www.datenschutzbeauftragter-online.de, 10.12.2018*

Die Inhalte des Artikels wurden von Prof. Marcel Kuhlmey (Professor für Risiko- und Krisenmanagement an der Hochschule für Wirtschaft und Recht Berlin) und Heike Nagora (Ausbildungsleiterin im Polizeivollzugsdienst an der Polizeiakademie Berlin) recherchiert und freundlicherweise zur Verfügung gestellt.

Mit diesem Artikel möchten wir einen Anstoß zur Verhaltensänderung bei Führungskräften geben, um (inneren) Kündigungen durch gute Mitarbeiter vorzubeugen. Denn gute Mitarbeiter sind motivierte Mitarbeiter, die an einer positiven Reputation des Unternehmens interessiert sind.

SECURITY AWARENESS
(SICHERHEITSBEWUSSTSEIN)
EINMAL ANDERS GEDACHT

Security Awareness (Sicherheitsbewusstsein) bezeichnet allgemeinhin die Sensibilisierung von Mitarbeitern gegenüber potentiellen Gefahren und Risiken. Doch Security Awareness ist viel mehr als nur reine Wissensvermittlung. Security Awareness ist auch eine Art „Sicherheitskultur im Unternehmen", die ganzheitlich und nachhaltig in vielen Prozessen verankert sein sollte.

KÜNDIGUNGEN ERNST NEHMEN - MISSMANAGEMENT BEHEBEN

Kündigungen kosten ein Unternehmen nicht nur viel Geld und Ressourcen für Arbeitsumverteilung, Neueinstellung und Einarbeitungszeit, sondern führen auch zu Know-how-Verlust und teilweise sogar zu einer schlechteren Arbeitsatmosphäre. Im Fall von inneren Kündigungen kommt es in der Praxis immer wieder zu besonders unsensiblem Verhalten im Hinblick auf die Einhaltung von Sicherheitsvorgaben oder gegenüber sicherheitsrelevanten Ereignissen (böswillig unterstellt: man freut sich sogar über den Schaden für das Unternehmen).

Gute Mitarbeiter zu finden ist in der heutigen Zeit nicht einfach und diese dann zum Bleiben zu bewegen, noch viel weniger. Daher ist es umso wichtiger, mit ausscheidenden Mitarbeitern die Gründe für einen Jobwechsel zu eruieren, um dadurch ggf. weiteren Verlusten von Know-how und Arbeitskraft vorzubeugen. Daraus lassen sich mitunter Rückschlüsse auf die Arbeitsmoral oder andere Unstimmigkeiten im Unternehmen ziehen, die der Reputation des Unternehmens langfristig erheblichen Schaden zufügen können.

Einer Kündigung sollte nicht mit den Worten „Reisende soll man nicht aufhalten!" oder „Wer gehen will, soll gehen!" entgegengetreten werden. Vielmehr gilt es, die vielen offenen Fragen zu klären. Warum ist derjenige gegangen? Lag es am Betriebsklima, dem Team, dem Vorgesetzten, den Aufgaben, der Wertschätzung …? Diese Fragen kann und sollte eine Führungskraft ausscheidenden Mitarbeitern stellen, denn nur in dieser Situation kann der Mitarbeiter offen und schonungslos die Wahrheit aussprechen. Derartige Wahrheiten und Informationen sind im Prinzip für jeden Arbeitgeber bares Geld wert, denn nur so lässt sich ein Unternehmen weiter voranbringen und in der Konsequenz auch besser auf die „verbliebenen" Mitarbeiter eingehen.

Durch ein besseres (Mitarbeiter-)Verständnis, verbesserte (Arbeits-)Abläufe sowie der Nachjustierung einiger kleiner Stellschrauben im Unternehmen werden verbliebene Mitarbeiter ggf. motivierter und dadurch im Arbeitsalltag auch wiederum sensibler gegenüber potentiellen Gefahren und Risiken. ›››

MEHR SICHERHEIT DURCH MOTIVIERTE UND ENGAGIERTE MITARBEITER! “

WARNSIGNALE FÜR SCHLEICHENDEN REPUTATIONSVERLUST

1. SINKENDE ARBEITSMORAL
2. INTERNE POLITIK IST WICHTIGER ALS QUALITATIV HOCHWERTIGES UND PROFESSIONELLES ARBEITEN
3. „GUTE" MITARBEITER VERLASSEN DAS UNTERNEHMEN

DIE SCHRITTE EINES KLÄRENDEN (KÜNDIGUNGS-)GESPRÄCHS

1

INTENTION DES GESPRÄCHES KLÄREN

Bereitschaft erkunden, ob der Mitarbeiter dazu bereit ist, Kritik zu üben, um aus begangenen (Unternehmens-)Fehlern Lehren für die Zukunft zu ziehen.

Nicht der Mitarbeiter steht am Pranger, sondern das Unternehmen!

2

GESPRÄCHSPARTNER SINNVOLL AUSWÄHLEN

Nicht jede Führungskraft ist für derartige Gespräche geeignet, besonders dann nicht, wenn zwischenmenschliches Verhalten mutmaßlich zur Kündigung geführt oder zumindest dazu beigetragen hat.

Der Mitarbeiter sollte den Gesprächspartner mitbestimmen können.

3

GESPRÄCHSSTART ALLGEMEIN HALTEN

Wie würde das Gegenüber die Sicht auf das Unternehmen seinen Freunden beschreiben? Welche Punkte haben am meisten gestört bzw. gab es auch Dinge, die sehr gut waren?

4

ÄNDERUNGSVORSCHLÄGE ERFRAGEN

Gezielte Fragen und die Aufforderung zu Vorschlägen nach Struktur- und Prozessveränderungen sollten folgen. Aber auch die Frage nach Dingen, die beibehalten werden sollten.

5

WECHSELGRUND ERFRAGEN

Nun sollte der konkrete Wechselgrund und das „Warum“ erfragt werden. Hierauf wird der Mitarbeiter nicht immer (wahrheitsgemäß) antworten. Auch das gilt es zu respektieren.

Ein solches Gespräch dient in keiner Weise dazu, Leistungen von einzelnen Mitarbeitern oder Führungskräften zu bewerten, sondern muss zum Anlass genommen werden, mit den Antworten und dem Wissen die ggf. bestehenden oder begangenen Fehler nachhaltig abzustellen.

Harmonie im Arbeitsumfeld
=
mehr Sensibilität gegenüber Sicherheitsrisiken und -gefahren

UMGANG MIT KONFLIKTEN: „NUR EIN STREIT OHNE SIEGER IST EIN GEWONNENER STREIT."

Das Leben besteht aus Konflikten. Überall dort, wo Menschen zusammenarbeiten, kommt es zwangsläufig zu Auseinandersetzungen, Meinungsverschiedenheiten oder gar Streitereien. Konflikte sind jedoch nicht immer schädlich. Oft bieten sie auch die Möglichkeit zu konstruktiven Veränderungen und positiven Weiterentwicklungen jedes Einzelnen und im Team.

> GEHEN SIE NICHT DAVON AUS, DASS IHR GESPRÄCHSPARTNER DIE WELT EBENSO SIEHT WIE SIE SELBST. "

Dass die Botschaft, die wir gerne vermitteln möchten, beim Gesprächspartner so nicht ankommt, erleben wir immer wieder. Der Grund dafür liegt in unserer Wahrnehmung. Jeder Mensch hat seine persönliche Sicht der Dinge. Diese ist geprägt durch unsere:

- Ansichten und Einstellungen,
- Wertvorstellungen und Ziele sowie
- Erwartungen und Machtpotenziale.

Konfliktmanagement hat das Ziel, Konflikte, Streitereien und Meinungsverschiedenheiten erst gar nicht weiter eskalieren zu lassen. Es geht nicht darum, andere geschickt zu dominieren oder einen Streit zu gewinnen. Vielmehr dient der professionelle Umgang mit Konflikten dazu, gegenseitiges Verständnis zu wecken und dauerhaft stabile Kompromisse zu finden.

ANNÄHERUNG AN EINE GEMEINSAME SICHT DER DINGE

Was nützt einem die Frage nach „richtig" oder „falsch", wenn jeder Mensch ein eigenes Verständnis hat? Suchen Sie nicht nach dem „Schuldigen" für ein Missverständnis, sondern nach dem Missverständnis selbst. Gute Kommunikation bedeutet somit im Wesentlichen nichts anderes, als sich auf sein Gegenüber einzustellen. Somit kann man sich nur durch die Bereitschaft zum Dialog und zum Klären von Konflikten an eine gemeinsame „Sicht der Dinge" annähern.

1. ENTSTEHUNG Rufen Sie sich die Entstehung des Konfliktes ins Gedächtnis. Was ist der Grund für den Konflikt? Welche Situation hat den Konflikt ausgelöst?

2. PERSPEKTIVENWECHSEL Nehmen Sie andere Perspektiven ein. Bevor Sie mit Ihrem Konfliktgegner reden, versetzen Sie sich in seine Lage.

3. RESPEKT Nehmen Sie Ihren Konfliktgegner ernst. Die Fronten verhärten sich, wenn man das Gefühl hat nicht ernst genommen zu werden. Machen Sie Ihrem Konfliktgegner deutlich, dass Sie ihn als Person respektieren.

4. HÖFLICHKEIT Bleiben Sie höflich. Je mehr Emotionen den Konflikt bestimmen, umso schwieriger wird es eine Lösung zu finden. Denken Sie daran, dass eine einzige Beleidigung die Konfliktlösung zum Stillstand bringen kann.

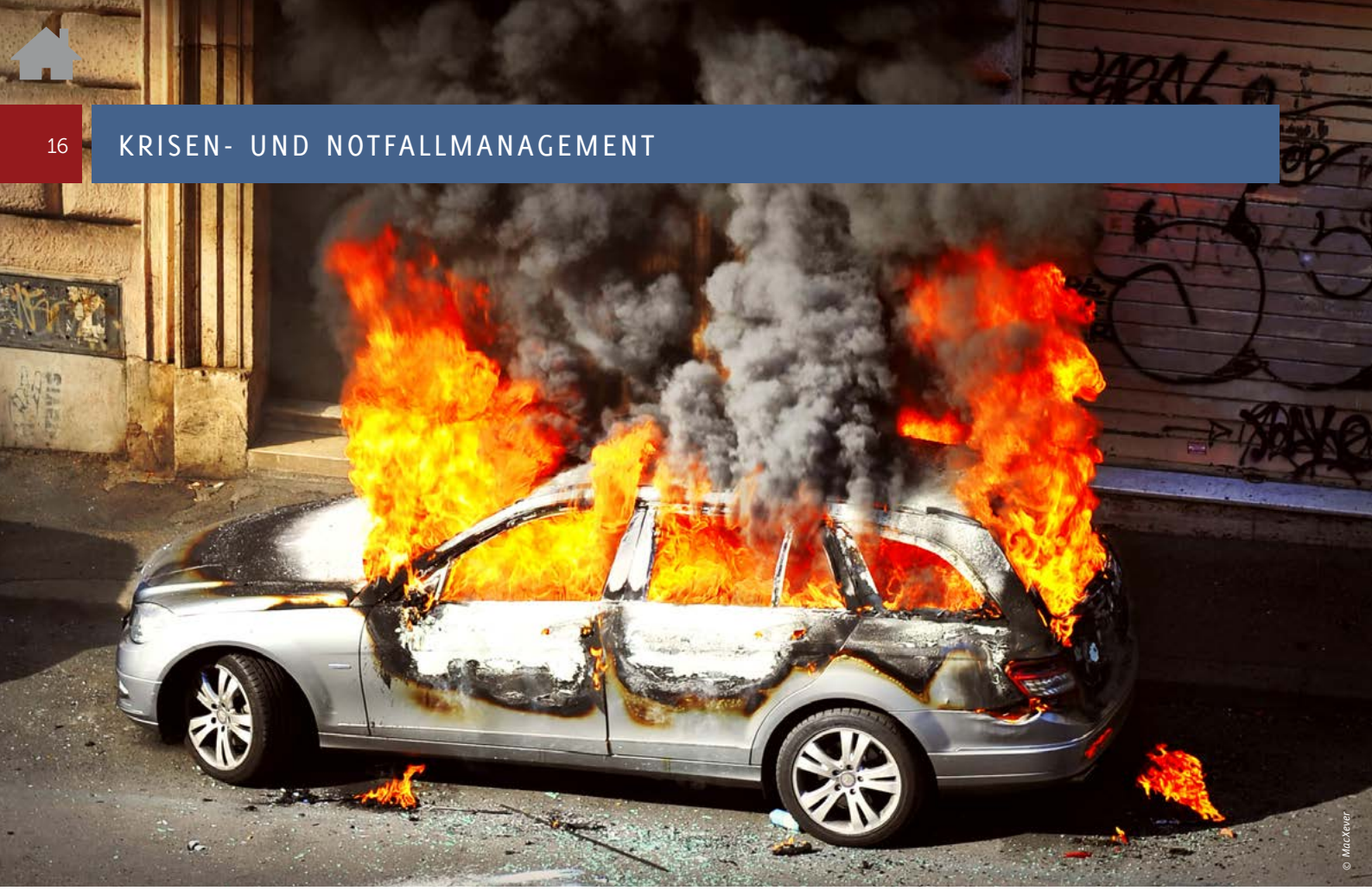
5. SACHLICHKEIT Je größer der Konflikt, umso schneller rutschen die Konfliktparteien bewusst oder unbewusst in Emotionen und das Persönliche ab. So kann es leicht vorkommen, dass auch nicht betroffene Teammitglieder in den Konflikt hineingezogen werden.

6. STREITPUNKTE - STREITURSACHE Bleiben Sie bei Konflikten bei der Streitursache und lassen Sie sich nicht zu generellen Aussagen wie „Was ich schon immer sagen wollte …" verführen. Allzu leicht wird alles auf den Tisch gelegt, was uns an dem Anderen nicht passt. Somit kommen immer mehr Konfliktpunkte ins Spiel.

7. OFFENHEIT Um nicht verwundbar zu wirken, zeigen sich viele Personen in Konflikten desinteressiert an einer Lösung. Schon bald können Sie sich in Widersprüche verwickeln, was die Lösung weiter erschwert.

8. GEMEINSAMKEITEN Suche Sie nach Punkten, bei denen Sie im Streitthema oder auch darüber hinaus, mit Ihrem Gegenüber übereinstimmen. Das ist der erste Schritt zu einer Lösung. Dadurch gewinnt man gegenseitiges Vertrauen und baut die Hürden für eine Konfliktlösung ab.

Probieren Sie es aus! Das Grundproblem vieler Konflikte liegt in den Motiven des Einzelnen. Diese Motive zu erkennen trägt maßgeblich zur Lösung bzw. Kompromissfindung bei.



VERHALTENSEMPFEHLUNGEN BEI BRANDANSCHLÄGEN

Brandanschläge, ob in Deutschland oder anderen Teilen der Welt, sind meist politisch motiviert (Vernichtungs- oder Aufmerksamkeitswille) oder durch persönliche Motive veranlasst. Wenn man den Begriff „Brandanschlag“ bei Online-Suchmaschinen eingibt, gelangt man schnell zu der Erkenntnis, dass dies auch in Deutschland ein durchaus übliches Phänomen ist.

Durch den Einsatz von Brandsätzen oder Brandmitteln wird ein Feuer entfacht, welches größtmöglichen Schaden an Gebäuden oder Fahrzeugen anrichten soll. Im Internet kursieren diverse Anleitungen zum Bau von Brandsätzen, die mit Alltagsgegenständen kinderleicht hergestellt werden können. Die Beschädigung benachbarter Objekte oder gar die Verletzung von Personen wird hierbei in Kauf genommen. Doch wie verhält man sich im Falle eines Brandanschlages?

Sollten Sie einen Brandanschlag unverletzt überstanden haben, können Sie sich mit bestimmten Verhaltensweisen optimaler schützen. Denn die Gefahr lauert nicht nur im Moment der Zündung (Druckwelle, umherfliegende Teile, einstürzende Bauteile etc.) sondern insbesondere durch die Rauchentwicklung und die Brandausbreitung (Hitze, Brandgase, Sauerstoffmangel etc.).

Sollte ein Brand festgestellt werden, ist dieser unverzüglich zu melden. Die 112 ist die gängige Rufnummer der Feuerwehr in Europa. Weltweit muss man sich mit den landesspezifischen Nummern der Rettungsdienste entsprechend vertraut machen. Der Sachverhalt ist so genau wie möglich zu

DAS GRUNDSÄTZLICHE HANDLUNGSPRINZIP BEI BRANDANSCHLÄGEN ODER AUCH BEI BRÄNDEN JEGLICHER URSACHE LAUTET:

MELDEN RETTEN BEKÄMPFEN

schildern und etwaige Rückfragen sind abzuwarten, um den Rettungskräften ein möglichst detailliertes Schadensbild zu liefern.

Dann erst sollte die Rettung von Menschenleben erfolgen. Die noch im Gebäude befindlichen Personen bzw. in der näheren Umgebung anzutreffenden Personen sind zu warnen, indem beispielsweise der Feuermelder oder die akustische Lautsprecheranlage aktiviert wird. Anschließend sollten Personen zur Unterstützung bei der Räumung herangezogen werden (ggf. sind diese im Rahmen eines Räumungskonzeptes bereits als Räumungshelfer benannt).

Hierbei sind die gängigsten Maßnahmen zu beachten:

1. Ruhe bewahren.
2. Schließen der Brandschutztüren und Rauchklappen.
3. ggf. Betätigen von Notausschaltern (Heizung, Lüftung, Spannungsversorgung).
4. Geordnetes Verlassen der Gefahrenbereiche.
5. Keine Benutzung der Fahrstühle.
6. Registrierung an der Sammelstelle (Sammelplatz).

Das wichtigste Credo lautet Ruhe bewahren, denn Panik und somit Fluchtreaktionen können eine Kette unkontrollierter Ereignisse nach sich ziehen, die zu einer Verschlimmerung des ursprünglichen Schadens führen kann. Insbesondere ängstliche Personen sind zu beruhigen und ggf. zu begleiten. Dies trifft auch auf schutzbedürftige Personen oder Geh- bzw. Sehbehinderte zu.

In jedem Fall erhöht das gebückte Gehen die Chance, bei Bewusstsein zu bleiben, denn Rauch und Hitze steigen nach oben und gefährden die Atmung sowie den Bewusstseinszustand. Bei sehr starker Verrauchung kann es sogar hilfreich sein, sich kriechend am Boden entlang fortzubewegen. Im Idealfall ist ein Stück Stoff parat, welches vor Mund und Nase gehalten werden kann.

EIGENSICHERUNG BEACHTEN

Gerade bei einem Brandanschlag ist es essentiell, auf Eigensicherungsmaßnahmen zu achten. Dies bedeutet, dass die Situation möglichst exakt erfasst werden sollte. Doch in den meisten Fällen ist augenscheinlich nicht ersichtlich, dass es sich um einen Anschlag handelt. Dies liegt nur nahe, wenn es entsprechende Bedrohungen gab oder Augenzeugen den oder die Täter gesehen haben, wie beispielsweise ein Brandsatz geworfen wurde oder kurz vor der Situation ein entsprechender Ausruf kam.

Bei Verdachtsmomenten, die auf einen Brandanschlag hinweisen oder Ihr Instinkt Sie warnt, sollten Sie besonders vorsichtig und umsichtig sein. Es könnten weitere Brandsätze versteckt sein, die mittels Zeitzünder aktiviert werden oder es


© flas100

kann auch eine Bedrohung außerhalb des Gebäudes lauern (Bombe, Waffengewalt etc.).

Beobachten Sie vor dem Verlassen des Gebäudes das Gelände aufmerksam und achten Sie auf Personen oder Gegenstände, die merkwürdig aussehen oder sich verhalten.

Erst danach erfolgt die Brandbekämpfung, die durch örtliche Rettungskräfte unterstützt wird. Hier ist es wichtig auf Anweisungen zu warten, Mitarbeiter und Kollegen zu zählen und zu informieren und in keinem Fall das geschädigte Gebäude zu betreten.

© Hallbauer Fioretti Fotografie

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

INTERVIEW ZUM THEMA: „PHYSISCHE IT-PRÄVENTIONS-SICHERHEITSLÖSUNG GEGEN UNBEFUGTEN DATENAUSTAUSCH AN PORTS“

Interview mit Nils Fleischhauer, Geschäftsführender Gesellschafter der Smart Light Solutions GmbH

Stellen Sie sich ein beliebiges Büroumfeld, Besprechungsräume, einen Anmeldetresen oder eine klassische Produktionsstraße vor. Überall stehen PCs, Server, Drucker, Tablets oder Laptops. Diese verfügen über diverse Ein- und Ausgänge, von denen sich Zugang zu eigentlich geschützten (internen) Daten verschaffen lässt. Wie schnell ist da ein USB-Stick oder Smartphone angeschlossen, das Daten abgreift oder beispielsweise Schadprogramme aufspielt.

DIE IT-SECURITY BETRACHTET IN DEN MEISTEN UNTERNEHMEN „NUR“ DEN SCHUTZ VOR ANGRIFFEN ÜBER DAS INTERNET, ANWENDERSYSTEME ODER SOFTWARE – ALS KLASSISCH VERSTANDENE IT-SECURITY. DOCH GERADE BEI BZW. AN DER HARDWARE GIBT ES ENORME DEFIZITE. WELCHES SIND HIER DIE POTENTIELLEN BEDROHUNGSHERDE UND EINFALLMÖGLICHKEITEN?

Grundsätzlich tut sich in dem Bereich Sicherheit sehr viel. Gerade auf Bundes- und Europaebene sind einige Dinge auf den Weg gebracht worden, die auch auf den physischen Schutz von IT-Hardwareschnittstellen zielen und die Unternehmen entsprechend in die Pflicht nehmen, hier zu handeln.

USB-Ports lassen sich zum Beispiel flexibel nutzen, ein USB-Stick oder das Handy ist schnell angeschlossen, etwa auch zum unbefugten Kopieren oder dem unerwünschten Datenaustausch. Aber auch vermeintlich harmlose USB-Sticks, die etwa auf dem Firmenparkplatz von einem Mitarbeiter entdeckt wurden, könnten von Dritten mutwillig dort platziert worden sein und stellen eine große Gefahr dar. Steckt der neugierige Mitarbeiter diesen gefundenen Stick an seinem Arbeitsplatz-System an, kann beispielsweise im Hintergrund eine Schadsoftware installiert werden – ohne dass die Mitarbeiter oder die Administratoren dies zunächst bemerken.
Zum anderen ist es denkbar, dass manipulierte Geräte oder Keylogger eingesetzt werden, um Kollegen zu bespitzeln, oder an Passwörter zu gelangen. Dabei geht auch von unzufriedenen Mitarbeitern eine Gefahr aus, etwa könnten sich diese Personen vertrauliche Informationen beschaffen und auf einem USB-Speichermedium aus dem Unternehmen entwenden.
Eine ähnlich große Gefahr geht hier gleichermaßen von externen Personen aus; ob nun Mitarbeiter gezielt angesprochen oder Personen in Unternehmen eingeschleust werden, um an Daten heranzukommen.

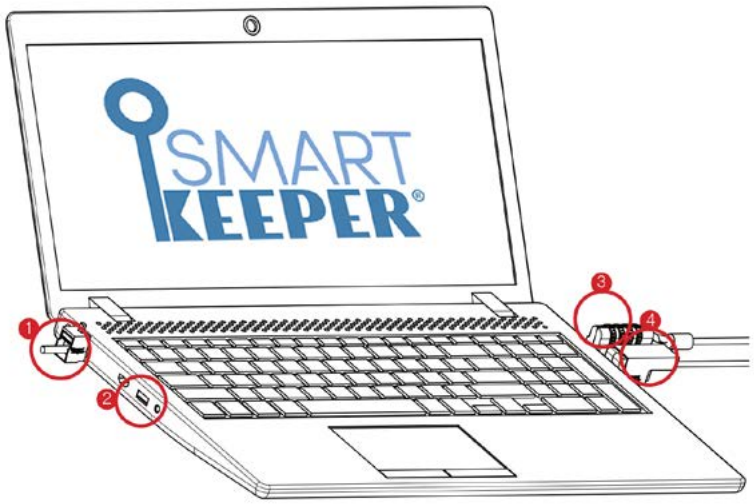
HIER MÜSSTE ES DOCH SYSTEMSEITIGE LÖSUNGEN GEBEN, UM PORTS ZU SCHLIESSEN BZW. ZUGRIFFE ZU VERHINDERN ODER ZUMINDEST UNAUTORISIERTE ZUGRIFFE ZU DETEKTIEREN?

Selbstverständlich kann softwareseitig schon viel geschützt und gesichert werden. Bei unserem Produktkonzept geht es auch weniger darum, die Softwaresysteme außen vor zu lassen – vielmehr ist es als eine weitere, zusätzliche Schutzbarriere zu sehen.
Unser System ist das physische Komplementär zu allen bereits existierenden, softwarebasierten Sicherheitsprodukten. Es ist ein neuer Baustein in der Sicherheitsmauer gegen Eindringlinge – an einer Stelle, für die es bisher überhaupt keinen oder nur äußerst schwachen Schutz gab.
Hinzu kommt, dass das Managen jeder einzelnen Schnittstelle an jedem kritischen Rechner sowohl zeitaufwendig als auch kostenaufwendig ist. Darüber hinaus gibt es nicht nur Schlösser, um den Zugriff auf Schnittstellen generell zu verhindern, vielmehr können auch angeschlossene Peripherieprodukte, Netzwerkkabel u. v. m. vor unbefugten Zugriffen schützen.

EINE SOFTWAREBASIERTE LÖSUNG WÜRDE FÜR DIE IT-ABTEILUNG NATÜRLICH EINEN ENORMEN ARBEITSAUFWAND BEDEUTEN. DAHER SETZEN SICH NACH UND NACH RESSOURCENSCHONENDERE UND UNKOMPLIZIERTERE LÖSUNGEN DURCH, PORTS VON AUSSEN ZU SICHERN. WO SETZEN DERARTIGE PRODUKTE AN?

Bei diesen Lösungen handelt es sich um physische IT-Präventions-Sicherheitslösungen, welche verschiedene Möglichkeiten bieten, alle kritischen Eingangs- und Ausgangsports der IT-Hardware – wie z. B. USB-Ports, Netzwerkanschlüsse von PCs, Switches, Druckern oder Servern – mechanisch zu verschließen und somit zu sperren.
Diese Lösungen sind meist komplett unabhängige Sicherheitslösungen, welche keine separate Softwareinstallation erfordern und die Kosten für Wartung und Kontrolle dadurch erheblich reduzieren können. Dies führt dazu, dass derartige Lösungen flexibel, effizient, unkompliziert und leicht zu verwalten sind. Die jeweiligen Schlösser können ausschließlich mit dem eigens für sie erstellten Schlüsseltypen mechanisch ver- und entriegelt werden. Die Basis des Systems bildet das USB-Schloss, welches in vielen Schlössern als Schlossmechanismus fungiert. Das System bietet dank einer individualisierten Codierung – sowohl für USB-Schlüssel als auch für die dazugehörigen USB-Schlösser – für jeden Kunden ein äußerst hohes Maß an Sicherheit und Zugriffskontrolle.

PHYSISCHE IT-SICHERHEITSLÖSUNGEN FÜR FÜR NOTEBOOKS UND COMPUTER



1. LAN Kabel-Lock

Netzwerkport-Lock dient dazu, um unbefugte Benutzer daran zu hindern LAN-Kabel zu entfernen.

2. USB Port-Lock (oder Closing-Lock)

Blockiert den nicht verwendeten USB-Port.

3. Notebook-Lock via USB Port

Diebstahlsicherung über USB-Anschluss.

4. Link-Lock

Verhindert das Entfernen von autorisierten USB-Geräten und das Einstecken von nicht autorisierten USB-Geräten.

USB-C Port-Lock

Secure USB & Connector

Linklock & USB Port-Lock

Network Port-Lock

Network Modul-Lock

WIE GENAU MUSS ICH MIR SOLCH EIN PRODUKT IM ARBEITSUMFELD VORSTELLEN?
Die verantwortlichen Personen müssen sich darüber Gedanken machen, wo und an welcher Stelle Ports geschlossen und/oder angeschlossene Produkte, wie USB-Mäuse, -Tastaturen etc. gesichert werden sollen. Nachdem das geschehen ist, können die einzelnen Schnittstellen ganz unkompliziert von der autorisierten und verantwortlichen Person gesichert werden.
Die Anwendungsmöglichkeiten sind zahlreich. Besonders bei technologieorientierten und innovativen Unternehmen, KMUs aber auch öffentlichen Einrichtungen, KRITIS-Unternehmen, Städten und Gemeinden sowie Universitäten, Krankenhäusern oder aber in der Schifffahrt finden die Produkte Anwendung. In asiatischen Ländern sind diese beispielsweise bereits vollends etabliert.

STELLT ES AUCH EINE RECHTLICHE ODER VERSICHERUNGSSEITIGE KOMPONENTE DAR, WENN PORTS AN PCS ODER LAPTOPS OFFEN SIND UND JEDER NAHEZU EINGELADEN WIRD, SCHADEN ANZURICHTEN?
Selbstverständlich. Es ist ein großer Unterschied, ob z. B. Mitarbeiter informiert und sensibilisiert werden, offene Ports nicht zu nutzen, oder ob der Zugriff generell durch mechanische Schlösser verwehrt wird und es somit eine Straftat darstellt. Sofern versucht wird, die Schlösser zu entfernen, ist in der Regel sofort ersichtlich, ob hier ein Zugriff auf die Ports stattgefunden hat, denn ohne jeweiligen Schlüssel können die Schlösser nicht schadlos entfernt werden und das fällt auf.
Die visuelle Wirkung der Schlösser spielt sicherlich auch eine entscheidende Rolle. Darüber hinaus bewegen wir uns im Falle von unbefugten Zugriffen von nicht autorisierten Personen rein rechtlich betrachtet auf anderen Ebenen.
Letztlich geht es auch um den wichtigen Faktor ZEIT. Es bedarf schon eines großen Zeitaufwands, um die Schlösser mutwillig zu entfernen.
SIE ZIELEN ALSO AUF DIE ABSCHRECKENDE (AUCH MENTALE WIRKUNG) UND DIE ZUGRIFFSVERZÖGERUNG AB. ICH BEDANKE MICH FÜR DIE INFORMATIVEN UND NÜTZLICHEN AUSFÜHRUNGEN UND BIN ÜBERZEUGT, DASS DERARTIGE LÖSUNGEN IMMER MEHR ZUGANG IN DEN ARBEITSALLTAG FINDEN.

BEI SICHERHEITSLÖSUNGEN FÜR INFORMATIONSTECHNISCHE SYSTEME GEHT ES NICHT MEHR NUR UM DIEBSTAHLSCHUTZ ODER DEN ZUGRIFF AUS DEM INTERNET, SONDERN AUCH UM DEN SCHUTZ DER HARDWARE UND LETZTLICH AUCH DARUM, DASS DER AUTORISIERTE BEDIENER WACHSAM UND SICHERHEITSORIENTIERT MIT DEN SYSTEMEN UMGEHT!

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

IDENTITÄTSDIEBSTAHL? MACHEN SIE NOCH HEUTE DEN TEST

Pro Jahr werden ca. 35 Millionen Identitätsdaten durch kriminelle Cyberangriffe entwendet – Tendenz steigend. Diese werden dann in speziellen Internetforen und Datenbanken veröffentlicht – darunter Nutzernamen, Passwörter und Kontonummern – und dienen somit zur Verwendung für weitere kriminelle Aktivitäten.

Ob Ihre Identität auch im Internet zu finden ist, können Sie ganz einfach selbst prüfen. Mit dem „HPI Identity Leak Checker“ des Hasso-Plattner-Instituts finden Sie heraus, ob Ihre E-Mail-Adresse im Internet veröffentlicht wurde. Das Tool kontrolliert dabei, ob Ihre E-Mail-Adresse in Verbindung mit persönlichen Daten, wie Telefonnummer, Adresse etc. im Internet zu finden ist und somit für kriminelle Handlungen genutzt werden könnte.

Auf der Webseite werden ebenfalls weiterführende Fragen beantwortet.

https://sec.hpi.de/ilc/

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

TIPP

TERRORISMUS - WIE WIR UNS SCHÜTZEN KÖNNEN

Dieses Buch zeigt auf, wie man sich der immer weiter verbreiteten Angst vor terroristischen Anschlägen – die uns überall treffen können – stellen kann und, was jeder Einzelne gegen diese latente Bedrohung tun kann.

Fachlich fundiert, mit Hintergrundempfehlungen angereichert und mit vielen Praxisbeispielen untermauert, erhält der Leser praxisorientierte Handlungsempfehlungen, die der Hilflosigkeit entgegenwirken sollen.

Die Motivation von Terroristen, das Vorgehen sowie die Bedrohungslage werden ausführlich beschrieben und es wird insbesondere auf Verhaltensempfehlungen bei verschiedensten Anschlagsarten sowie die Möglichkeiten der Früherkennung durch die Gesellschaft eingegangen.

Das Buch schafft eine solide Basis für sicherheitsbewusstes Handeln gegenüber terroristischen Bedrohungen und ist somit nicht nur für die Reisesicherheitsorganisation im Unternehmen – im Hinblick auf Handlungsempfehlungen – sondern auch für jeden Einzelnen interessant, denn Terrorismusbekämpfung ist nicht alleinige Aufgabe der Sicherheitsorganisationen der Länder oder des Bundes.

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.