AUSGABE 8

SICHERHEIT. DAS FACHMAGAZIN.

SICHERHEIT AUF DEN PUNKT GEBRACHT.

SIUS Consulting

KOMPETENZPARTNER

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.

SICHERHEIT. DAS FACHMAGAZIN.

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

DOWNLOADS

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

SECURITY-SERVICE-CENTER

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

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

KOSTENFREI & UNVERBINDLICH

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

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

Wie finanziert sich SICHERHEIT. Das Fachmagazin.?

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

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

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

UNSERE KERNTHEMEN

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

E-PAPER

SICHERHEIT. Das Fachmagazin. als ePaper bringt Ihnen alle Vorzüge eines gedruckten Magazins auf Ihren Bildschirm: ob 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 klassischen PDF-Format

RETTUNGSKARTE FÜR FAHRZEUGE ERMÖGLICHT GEFAHRLOSE UND EFFEKTIVE UNFALLRETTUNG

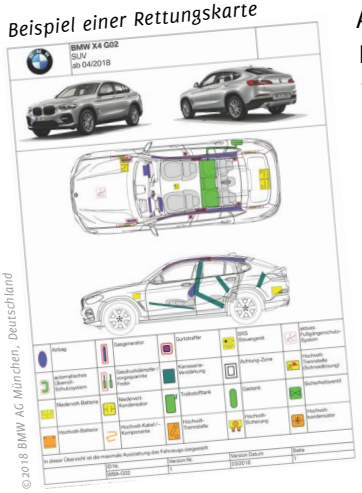
Bereits eine kleine Unachtsamkeit oder widrige Straßenverhältnisse können dazu führen, einen schweren Unfall zu verursachen. Durch die Vielzahl von Sicherheitsausstattungen in modernen Fahrzeugen ist die Überlebenschance für Insassen in den letzten Jahren deutlich gestiegen. Doch manchmal sind Opfer eingeklemmt und Rettungskräfte müssen diese unverzüglich befreien oder verkeilte Karosserien mit entsprechendem Einsatzgerät trennen. Was die wenigsten wissen: Alle Fahrzeuge weisen aufgrund ihrer unterschiedlichen Bauweisen verschiedenste Gefahrenstellen für Rettungskräfte auf wie beispielsweise nicht ausgelöste Airbag-Patronen oder Hochvolt-Systeme.

SAG'S WEITER!

*Die **kostenfrei erhältlichen Rettungskarten** der Automobilhersteller führen zu **genaueren Informationen zum Fahrzeug** für Rettungskräfte und somit zur **schnelleren Rettung von Fahrzeuginsassen!***

Stabilere Materialien, mehr Airbags oder Notbremsassistenten – all dies macht das Autofahren sicherer. Doch wenn es zu einem Unfall kommt, sollte die Rettung durch neue und sichere Materialien oder Sicherheitssysteme nicht unnötig verzögert oder gar erschwert werden. Denn bei einem Unfall zählt jede Sekunde! Was die Fahrzeuginsassen schützt, kann für die spätere Rettung zum Verhängnis werden. Nicht ausgelöste Airbag-Patronen können explodieren, extra gehärtete Karosserieteile können Rettungsgeräte zerstören oder wirkungslos machen und Hochvolt-Stromleitungen können zur Gefahr für die Unfallopfer und Rettungskräfte werden. Daher ist es für Rettungskräfte am Unfallort wichtig zu wissen, wo Rettungsspreizer und Rettungsscheren gefahrlos und effektiv angesetzt werden können und bei welchen Bauteilen mit besonderer Vorsicht vorgegangen werden muss. An dieser Stelle setzt die vom „Allgemeinen Deutschen Automobil-Club e. V. (ADAC) standardisierte und kostenfrei erhältliche Rettungskarte der Automobilhersteller an. Die Rettungskarte stellt das jeweilige Fahrzeug im schematischen Aufbau dar, wie das Beispiel auf der linken Seite verdeutlicht.

Beispiel einer Rettungskarte



SCHRITT FÜR SCHRITT ZUR RETTUNGSKARTE

1. RETTUNGSKARTE FINDEN

Unter www.adac.de/rund-ums-fahrzeug/unfall/rettungskarte/ Fahrzeugmarke und Fahrzeugmodell auswählen.
Hinweis: Im Feld D.2 des Fahrzeugscheins findet sich die exakte Baureihenbezeichnung.

2. RETTUNGSKARTE PRÜFEN

Stimmt die schematische Fahrzeugansicht mit Ihrem Fahrzeug überein? Hinweis: Es wird immer die maximale Sicherheitsausstattung angezeigt.

3. RETTUNGSKARTE AUSDRUCKEN

Rettungskarte farbig im DIN A4-Format ausdrucken, damit die farblichen Markierungen erkennbar sind. Rettungskarte nach außen falten, damit diese auch als solche zu erkennen ist. Hinweis: Sondereinbauten sollten ggf. durch die Werkstatt auf der Rettungskarte vermerkt werden.

4. RETTUNGSKARTE DEPONIEREN

International ist kommuniziert, dass Rettungskarten hinter der Fahrer-Sonnenblende befestigt sind.

5. AUFKLEBER ANBRINGEN

Damit die Rettungskräfte auf Anhieb wissen, dass es eine Rettungskarte gibt, sollte auf der rechten Seite der Windschutzscheibe ein entsprechender Hinweisaufkleber angebracht werden.

Ein Beispiel für einen solchen Aufkleber können Sie dem Dokument „Flyer Rettungskarte (Dekra)“ im Downloadbereich zu dieser Ausgabe entnehmen – der Aufkleber ist aber auch in jeder ADAC-Geschäftsstelle kostenfrei erhältlich.

SOCIAL ENGINEERING: DIE KUNST DER SOZIALEN MANIPULATION

Social Engineering ist die sogenannte „Kunst des Täuschens“. Der Täter beeinflusst durch das gekonnte Ausnutzen menschlicher Eigenschaften sein Opfer, um beispielsweise bestimmte Verhaltensweisen hervorzurufen, an vertrauliche Informationen zu gelangen, die Freigabe von Finanzmitteln zu erhalten oder die Person zum Kauf von Produkten zu bewegen. Anders ausgedrückt kann man auch sagen, dass mittels Social Engineering technische Sicherheitsvorkehrungen durch menschliches Fehlverhalten umgangen werden. Es dient häufig auch der Vorbereitung des Eindringens in ein fremdes Computersystem.

Die Art der Betrugsmasche gibt es schon seit Menschengedenken. Durch die zunehmende Digitalisierung ergeben sich viele neue Möglichkeiten, um Millionen von Opfern zu erreichen.

Social Engineering stellt eine große Gefahr für jedes Sicherheitssystem dar, weil die Abhängigkeit von Informationen und Daten immer größer wird. Immer mehr Menschen haben Zugriff auf Daten, deren Vertraulichkeit – und somit der Schaden, der durch Missbrauch entstehen könnte – ihnen überhaupt nicht bewusst ist. Diesen Umstand machen sich die Täter zunutze. Ihr Ziel ist die Erlangung von vertraulichen Daten und Informationen.

VORGEHENSWEISE DER TÄTER

Social Engineering betreiben Täter vor allem für den Zweck

> „TÄTER NUTZEN BEIM SOCIAL ENGINEERING DEN „FAKTOR MENSCH“ ALS VERMEINTLICH SCHWÄCHSTES GLIED IN DER SICHERHEITSKETTE AUS, UM IHRE KRIMINELLE ABSICHT ZU VERWIRKLICHEN.

von „Industrie- und Wirtschaftsspionage“. Dabei zählt sogar die Einschleusung von Personen in das Unternehmen zum Repertoire der Täter, was Sicherheitsbehörden wie beispielsweise der Verfassungsschutz oder das Bundeskriminalamt immer wieder bestätigen.

Das Hauptmerkmal des Täters besteht darin, das Opfer über die Identität und die Absicht zu täuschen. Social Engineers (Täter) spionieren beispielsweise das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder

nutzen Verhaltensweisen wie Autoritätshörigkeit, um an Hintergrundinformationen zu gelangen.
Diese Informationsgewinnung geschieht in zwei Phasen:

1. Sammeln von öffentlich zugänglichen Informationen (Webseite, Flyer, Broschüren, Berichte, Soziale Medien etc.)
2. Herantasten an das Zielunternehmen (Vortäuschung von Gesprächsgründen – Student, potentieller Kunde, ehemaliger Kollege, IT-Abteilung etc.)

Mit dem so erworbenen Wissen tasten sie sich anschließend an die Zielperson heran. Der Erfolg des Täters basiert in den meisten Fällen auf seinem autoritären Auftreten, einer ausgenutzten Stresssituation des Mitarbeiters und dem Überraschungsmoment. Der Social Engineer kann dabei in die unterschiedlichsten Rollen schlüpfen:

- Ein Vorgesetzter oder Kollege aus einer anderen Niederlassung, der einige Informationen zum Unternehmen benötigt.
- Als Mitarbeiter eines Kunden, der beispielsweise sein Passwort vergessen hat oder in Vertretung eines Kollegen dringend benötigte Verkaufszahlen erfahren muss.
- Ein neuer Bekannter im näheren Umfeld, der an Ihrer beruflichen Tätigkeit äußerst interessiert ist.
- Als Journalist, der ein Interview über die Erfolge und Ziele des Unternehmens führen möchte.
- …

BEISPIELE AUS DER PRAXIS

- Der vergessene USB-Stick, der Neugier weckt.
- Phishing-E-Mails von der Bank, Krankenkasse, Versicherung oder Personalabteilung, die zum Klicken, Downloaden oder Antworten auffordern.
- Der freundliche Support-Mitarbeiter, der Login-Daten oder die Verifizierung einer Adresse benötigt.

Wenn Sie jemals den Film „Catch Me If You Can“ gesehen haben, wissen Sie, was man mit Social Engineering so ALLES erreichen kann!

Social Engineering kann jedoch auch mit scheinbar zufälligen Gesprächen in der Kantine, bei einer wohlverdienten (Raucher)Pause oder während eines vermeintlich harmlosen Messebesuchs beginnen. Es gibt eine Vielzahl von Situationen, bei denen man Menschen dazu bringen kann, vertrauliche und schützenswerte Informationen eigenständig preiszugeben.

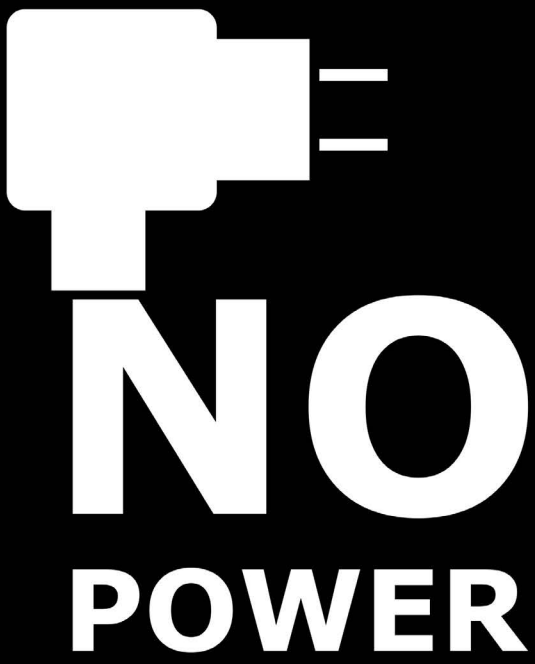
Von dem Begriff „Social Engineering“ haben mittlerweile viele gehört, doch was sich konkret dahinter verbirgt, wissen leider nur die wenigsten. Daher ist es wichtig, über die verschiedensten Formen und Herangehensweisen der Täter aufzuklären, um die eigenen Informationen und Daten bestmöglich zu schützen. Es gibt kein „Standard-Gegenmittel“ – daher ist Aufklärung, Sensibilisierung und die Arbeit mit Praxisbeispielen das „A“ und „O“, um potentielle Sicherheitslücken zu schließen.

SOCIAL ENGINEERING VORBEUGEN

Die Abwehr von Social Engineering gestaltet sich teilweise äußerst schwierig, da der Täter im Grunde positive Eigenschaften der Menschen wie beispielsweise Hilfsbereitschaft, Vertrauen und Respekt ausnutzt. Dennoch können die Aufmerksamkeit und das Wissen zum Vorgehen der Täter dazu führen, Social Engineering bewusster wahrzunehmen und somit vorbeugen zu können. Im Folgenden finden Sie elf Punkte zum bewussteren Umgang gegenüber fremden Personen:

1. Sicherheit geht vor Höflichkeit.
2. Geben Sie vertrauliche Informationen/Zugangsdaten niemals ungeprüft weiter und schützen Sie diese.
3. Seien Sie vorsichtig in sozialen Medien.
4. Auch scheinbar geringfügige und nutzlose Informationen können zum Abgrenzen eines größeren Sachverhalts beitragen.
5. Prüfen Sie unbekannte Anrufer immer kritisch oder rufen Sie die Nummer nach einigen Minuten zurück.
6. Die Identität des Absenders einer E-Mail sollte immer sichtbar und verifizierbar sein.
7. Hinterfragen Sie außergewöhnliche Kontaktaufnahmen, bevor Sie handeln.
8. Bitten Sie ggf. um einen Augenblick Geduld, um sich intern über den Vorgang zu vergewissern.
9. Verwenden Sie keine Links aus E-Mails, die eine persönliche Eingabe verlangen, sondern geben Sie die URL selbst im Browser ein.
10. Lassen Sie sich keinesfalls einschüchtern und verweisen Sie ggf. auf Ihren Vorgesetzten.
11. Melden Sie Auffälligkeiten und Beobachtungen einem Vorgesetzten oder dem Sicherheitsverantwortlichen.

Im Download-Bereich zu dieser Ausgabe finden Sie weitere nützliche Informationen zum kostenfreien Herunterladen.



UND PLÖTZLICH WIRD ES DUNKEL

Produktionsmaschinen stoppen, Klima- und Kühlgeräte schalten sich ab, Rechner, Drucker und Telefone funktionieren nicht mehr, Zutrittskontrollsysteme, Einbruchmeldeanlagen, Videoüberwachungsanlagen versagen ihren Dienst und zu allem Übel ist auch noch die Heizung ausgefallen – von der Warmwasserzufuhr oder den Pumpenanlagen der Toilettenspülung ganz zu schweigen. Und noch schnell etwas Bargeld am Geldautomaten holen: Fehlanzeige!

„BLACKOUT": MIT DIESEN FRAGEN BEREITEN SICH UNTERNEHMEN AUF DEN ERNSTFALL VOR

Zur präventiven Vorbereitung auf Krisen- und Notfalllagen ist es nicht nur wichtig, sich mit internen Szenarien auseinanderzusetzen, sondern auch externe Gefahren- und Ereignismöglichkeiten frühzeitig zu betrachten und in das Vorgehen einzubinden. Beispielsweise sollte das Szenario eines großflächigen und länger andauernden Ausfalls der Stromversorgung („Blackout") in Erwägung gezogen werden, welches einer anderen Herangehensweise bedarf als „klassische" Krisen- und Notfalllagen.

Viele Unternehmen betrachten in den Krisen- und Notfallszenarien und den damit einhergehenden BCM-Plänen (Business Continuity Management), die der Aufrechterhaltung der Geschäftstätigkeit dienen, einen kurzfristigen Ausfall der Ressource „Strom" und binden somit elementare Bestandteile, die zur Fortführung des Geschäftsbetriebes vonnöten sind, an eine Notstromversorgung (USV: Unterbrechungsfreie Stromversorgung) an. Doch für welchen Zeitraum ist die Stromversorgung autonom?

Grundsätzlich unterscheidet man bei „Stromproblemen" gemäß „IEEE" („Institute of Electrical and Electronics Engineers") zwischen 7 Arten:

- Spannungsabfall/Unterspannung
- Spannungsanstieg/Überspannung
- Spannungsschwankungen
- Frequenzschwankungen
- Spannungsstöße
- Unterbrechungen
- Verzerrung der Wellenform

Aber auch Cyberangriffe oder Anschläge auf das Stromnetz sind denkbar. Doch wenn ein sogenannter „Blackout" eintritt, stellt sich nicht mehr die Frage WAS oder WIE etwas passiert ist oder aufrechterhalten werden kann, sondern für Unternehmen (und auch Privatpersonen) geht es jetzt ums „Überleben". Das Szenario eines flächendeckenden und langanhaltenden Stromausfalls in weiten Teilen Deutschlands oder gar Europas wird auch in den Medien immer mal wieder thematisiert – und die Frage dabei lautet nicht, ob es passiert, sondern wann!

FAKT IST:

Die derzeitigen globalen Schäden – bedingt durch die Unterbrechung der Netzversorgung oder durch Stromschwankungen – betragen mehrere Milliarden Euro. Hier sind flächendeckende Stromausfälle oder größere „Blackout-Szenarien" noch nicht mit eingerechnet.

EXPONENTIELLE AUSWIRKUNGEN

Ein plötzlich auftretender, überregionaler und länger andauernder Strom- und Infrastrukturausfall („Blackout") in weiten Teilen Deutschlands: Es passiert plötzlich und ohne jegliche Vorwarnung. Eine vollständige Wiederherstellung der Stromversorgung kann Stunden, wenn nicht sogar Tage dauern. Es fallen alle anderen lebenswichtigen und stromabhängigen Infrastrukturen wie beispielsweise Transport, Kommunikation, Versorgung etc. nach und nach aus bzw. stehen nur noch sehr eingeschränkt zur Verfügung. Kein Licht, keine Fernwärme, keine Klimageräte, keine Kühlfunktion, kein Internet, kein Telefon, keine Tankstellen für jedermann. Ampeln und Aufzüge bleiben stehen. Sanitärinstallationen wie Toilettenspülungen funktionieren nicht mehr. Wir sind abhängig vom Strom, ohne dass uns dies im Alltag bewusst ist. So etwas gab es bisher noch nicht und ist auch in einer derartigen Flächenausdehnung kaum vorstellbar – aber Zufälle passieren oft. Gemäß Hochrechnungen kann es bis zu 7 Tage dauern, bis das europäische Energieversorgungssystem wieder halbwegs normal funktionieren würde. **Die Kernfrage lautet: Ist Ihr Unternehmen auf einen solchen Ausfall vorbereitet? Und wie sieht es in Ihrem privaten Umfeld aus?** ›››

> DIE **WECHSELWIRKUNGEN** UND DIE **KOMPLEXITÄT** DES SYSTEMS **„STROMVERSORGUNG“** SOLLTE IN KEINEM FALL **UNTERSCHÄTZT** WERDEN!

Wenn Sie nicht zu den Unternehmen zählen, die als „Kritische Infrastruktur“ gelten und daher in Krisenlagen einen gewissen „Sonderstatus“ haben, müssen Sie sich eigenständig aufstellen. Das oberste Management muss sich Gedanken darüber machen, ob der Geschäftsbetrieb sukzessive heruntergefahren werden oder eine Art „Notbetrieb“ weiter aufrechterhalten werden soll, mit allen Widrigkeiten, die in einem solchen Fall auf das Unternehmen zukommen und nicht nur die Anfangsphase betreffen:

- Werden Ihre Waren und Dienstleistungen überhaupt noch benötigt?
- Wie gelangen Ihre Waren zu Ihren Kunden?
- Wie gelangen Ihre Mitarbeiter zur Arbeit?
- Wie versorgen Sie bei einem Notbetrieb Ihre Mitarbeiter mit Getränken, Nahrungsmitteln und Hygieneartikel und über welchen Zeitraum?
- Was geschieht mit den Angehörigen von Mitarbeitern?

Schaffen Sie eine Akzeptanz für das Thema und machen Sie sich das Szenario und die möglichen Auswirkungen einmal konkret bewusst. Diskutieren Sie das Thema mit den unterschiedlichen Fachabteilungen in Ihrem Unternehmen. Prüfen Sie gemeinsam mit den Fachabteilungen, welche Betriebsprozesse vom Stromnetz abhängig sind und wie lange die Geschäftstätigkeit im Fall eines „Blackouts“ aufrechterhalten werden muss bzw. sollte.

FRAGEN ÜBER FRAGEN, DENEN SICH EIN UNTERNEHMEN STELLEN SOLLTE

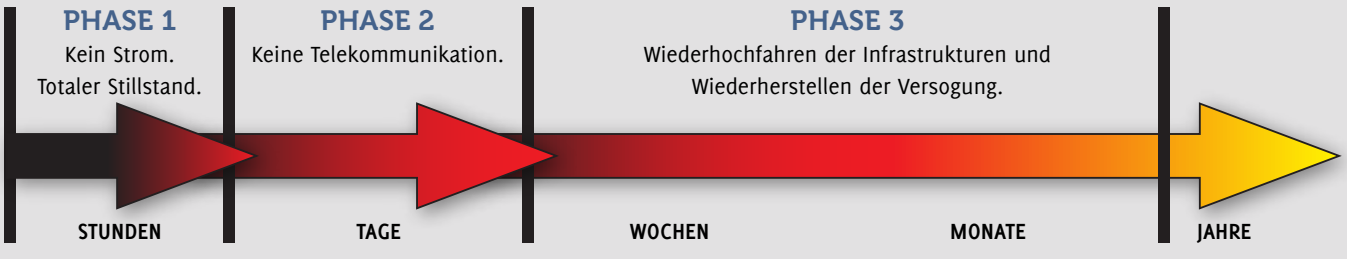
Bevor sich ein Unternehmen mit dem Thema „Blackout“ konkreter befasst, müssen vom Management grundlegende Fragen beantwortet werden:

1. Inwieweit müssen die eigenen Leistungen/Produkte bzw. der Betrieb für Dritte aufrechterhalten werden? Wie steht es um rechtliche, vertragliche oder gar versicherungsseitige Verpflichtungen?
2. Welche zwingenden betrieblichen Abhängigkeiten bestehen gegenüber Dritten?
3. Wie kann ein sicherer Notbetrieb oder ein sicheres Herunterfahren einzelner Bereiche gewährleistet werden?
4. Was ist für einen Notbetrieb erforderlich? Welche elektrische Leistung wird hierfür benötigt und wie lange soll bzw. muss diese aufrechterhalten werden? Wurde die innerbetriebliche Notstromversorgung in der Vergangenheit getestet?
5. Welche EDV-Abhängigkeiten bestehen und inwieweit sind diese Systeme redundant (Offline-Systeme)?
6. Wie gestaltet sich der Umgang mit Mitarbeitern, Kunden, Geschäftspartnern etc.?
7. Welche innerbetrieblichen Positionen müssen zwingend besetzt werden und bleiben?

> **EINE INNERBETRIEBLICHE AKZEPTANZ UND DISKUSSION ZUM THEMA „BLACKOUT“ IST EINE WESENTLICHE VORAUSSETZUNG, UM KONKRETE SCHRITTE ZUR VORBEREITUNG TREFFEN ZU KÖNNEN.**

DIE 3 PHASEN EINES „BLACKOUTS“

Zu Beginn wird sich ein „Blackout“ nicht viel anders als ein „normaler/regionaler“ Stromausfall darstellen. Doch spätestens, wenn die Telekommunikation nicht mehr möglich ist, die Transportlogistik zum Erliegen kommt und die hygienischen Verhältnisse schlechter werden, sollte man sich Gedanken machen. Selbst die Wiederanlaufphase birgt Risiken, da in der heutigen Zeit der „Just-In-Time-Produktion“ nicht alle Produkte und Dienstleistungen sofort wieder verfügbar sein werden.



Folgende Fragestellungen helfen Sicherheitsverantwortlichen, sich mit dem Thema eines flächendeckenden Stromausfalls im Hinblick auf Sicherheitsfragen vertraut zu machen:

1. Sind einzelne Geräte, Prozesse etc. an eine Notstromversorgung angeschlossen?
   - Wie lange läuft die Notstromversorgung? Beachten Sie, dass auch der Diesel von Generatoren irgendwann aufgebraucht ist.
   - Sind Aufzüge so lange in Betrieb, bis sie sicher das Erdgeschoss oder die nächstgelegene Etage erreicht haben und die Türen offen stehen bleiben?
   - Ist das Zutrittskontrollsystem ebenfalls an die Notstromversorgung angeschlossen? Stehen Türen durch den Ausfall auf einmal offen oder bleiben ggf. sogar geschlossen?
   - Läuft die Videoüberwachung weiter? Wird diese in einem solchen Fall überhaupt benötigt?
   - Sind Einbruchmeldeanlagen noch aktiv? Und wenn ja, wie lange?
2. Wie werden Mitarbeiter im Ablösefall erreicht?
   - Welche Mitarbeiter sind ggf. durch die Einbindung in Rettungsorganisationen oder die Familiensituation bereits anderweitig gebunden oder können die Arbeitsstätte eventuell nicht erreichen (Pendler)?
   - Werden Sicherheitsmitarbeiter noch in der derzeitigen Position benötigt oder ist ggf. eine andere Positionierung sinnvoller?
3. Stehen beispielsweise Taschenlampen, Megaphone oder batteriebetriebene Radios inklusive der entsprechenden Batterien für einen Zeitraum X zur Verfügung?
   - Wenn ja: Werden die Geräte in regelmäßigen Abständen auf ihre Funktion überprüft?
4. Werden Wasserreserven für die Nutzung der Unternehmensprozesse oder -abläufe inklusive der Nothygiene (Händewaschen und Toilettenspülung) vorgehalten?
5. Könnten eventuell Solar- oder Öllampen dabei helfen, bis zum Herunterfahren der Betriebstätigkeit oder im Notbetrieb für Licht zu sorgen?
6. Wo könnten geeignete Anlaufstellen für Informationen eingerichtet werden?
7. Wer trifft Entscheidungen im Ereignisfall und welche Aushänge oder Informationen sollten ggf. schon vorab vorbereitet sein?

KOMPLEXE HERAUSFORDERUNGEN ERFORDERN VERNETZTES UND SYSTEMISCHES DENKEN UND HANDELN

Eine offene und ehrliche Kommunikation mit und zwischen den Mitarbeitern ist unabdingbar, um Probleme zu erkennen und ggf. Improvisationsmaßnahmen ergreifen zu können. Das unternehmerische Handeln endet gerade in solchen Fällen nicht an der Unternehmensgrenze. Auch Gemeinden und Kommunen müssen und sollten sich vorbereiten, daher kann dieses Thema mit allen Fragestellungen und Schnittstellenproblemen durchaus auch auf dieser Ebene thematisiert werden. Und es ist besser, es werden Probleme vor einer Krise erkannt, wo sie ggf. noch behoben werden können, als in einer Krise, wenn es bereits zu spät ist.

Viele Maßnahmen sind auf organisatorischer/kommunikativer und weniger auf technischer Basis zu lösen, da in einem solchen Fall die Technik nur bedingt zur Verfügung stehen wird. Eine Organisation, die im Ereignisfall adäquat reagiert, erreicht einen Wettbewerbsvorteil und eine Imageverbesserung, wenn die Vorbereitung entsprechend kommuniziert wird. Auch innerbetrieblich trägt die Vorbereitung auf Notfall- und Krisenlagen zu einem Sicherheitsgefühl der Mitarbeiter bei und erhöht dadurch auch die „unternehmerische Fürsorge“. Zudem können derartige Vorbereitungen zu einer adäquaten Schadensminimierung im Ernstfall führen, was wiederum auch zu Prämienvorteilen bei Versicherungen führen kann.

Beschäftigen Sie sich jedoch auch mit dem sogenannten „Business Continuity Management“ – also dem „Wiederanlauf von Geschäftsprozessen“:

1. Welche Voraussetzungen müssen für einen adäquaten Wiederanlauf greifen?
2. Welche Prozesse – insbesondere in welcher Reihenfolge – laufen zu welchem Zeitpunkt in welcher Intensität wieder an?
3. Welche Stelle trifft welche Entscheidungen in welchem Umfang?

Gerade in der Wiederanlaufphase sind Kriseninterventionsteams aus IT, Facility Management etc. gefragt. Mit diesen steht und fällt jede Krisenbewältigung, daher ist es essentiell, diese wichtigen Ressourcen entsprechend vorzubereiten!

SPIELEN SIE DIE SITUATION EINMAL DURCH: PLANSPIELE UND ÜBUNGEN ZEIGEN AUF, OB DIE EIGENEN VORBEREITUNGEN UND ÜBERLEGUNGEN AUCH PRAXISTAUGLICH SIND. VERZICHTEN SIE KEINESFALLS AUF DIESES ERFAHRUNGSLERNEN!

Im Download-Bereich zu dieser Ausgabe finden Sie weitere nützliche Informationen zum kostenfreien Herunterladen.

AUSNAHMESITUATION DURCHSUCHUNG - WIE ENTSCHEIDUNGSTRÄGER OPTIMAL AUF DEN BESUCH VON STAATSANWALT & CO. REAGIEREN

Egal ob Mittelständler oder Großkonzern: Durchsuchungen sind für die Beteiligten auf Unternehmensseite niemals Alltag. Wenn die Ermittlungspersonen, Beamten der Staatsanwaltschaft, das Hauptzollamt, die Kartellbehörden oder die Steuerfahndung vor der Tür stehen, gilt es ebenso schnell wie besonnen zu reagieren. Gründe für Durchsuchungsmaßnahmen liegen häufig noch nicht einmal in der eigenen Sphäre des betroffenen Unternehmens oder Personen. Rechtliches Gehör spielt leider bei Zwangsmaßnahmen (dazu zählt eine Durchsuchung beim Beschuldigten oder auch Nichtbeschuldigten) in der Praxis kaum eine Rolle. Mit bewährten Tipps will dieser Beitrag den betroffenen Personen einen Leitfaden mitgeben, um strafprozessuale Rechte aller Beteiligten bestmöglich zu gewährleisten.

Durch regelmäßige und spezialisierte Vorbereitung von Schlüsselpersonen auf Zwangsmaßnahmen kann der Überraschungseffekt einer Durchsuchung häufig verpuffen. Nicht zuletzt sind vorausschauende Maßnahmen für Unternehmen und Personen aufgrund der häufig mit einer Durchsuchung einhergehenden medialen Aufmerksamkeit von existenzieller Bedeutung.

> STEUERVERGEHEN, KARTELLORDNUNGSWIDRIGKEITEN, KORRUPTION, NICHTABFÜHRUNG VON SOZIALABGABEN, BETRUG ODER UNTREUE VON VERTRAGSPARTNERN BIETEN NICHT SELTEN ANLASS ZU EINER DURCHSUCHUNG.

DA GERADE DER ERSTKONTAKT DIE ATMOSPHÄRE EINER BEVORSTEHENDEN DURCHSUCHUNG STARK BEEINFLUSSEN KANN, MUSS SICH ZWINGEND JEDE PERSON DIE VERHALTENSANWEISUNGEN FÜR DEN ERNSTFALL VERINNERLICHEN.

DER ERSTKONTAKT MIT ERMITTLUNGSPERSONEN

In der Regel treffen die Ermittlungspersonen als erstes auf Personen an der Pforte, am Empfang oder vielleicht im Sekretariat. Die dort tätigen Personen sind häufig mit derartigen Situationen überfordert.

Durchsuchungen können nicht verhindert werden. Höchste Priorität soll daher die Wahrung der Rechte aller betroffenen Personen haben. Hier hilft als erste Reaktion – man mag es nicht glauben – Höflichkeit und das Signalisieren von Kooperationsbereitschaft. Die Versorgung der Ermittlungspersonen mit einem Kaffee und ein ruhiger, abgelegener Raum für die Erörterung von Einzelheiten zur Durchsuchung können Wunder bewirken.

Allen Personen muss allerdings klar sein, dass nicht rechtzeitig wahrgenommene Rechte zu dramatischen und irreparablen Folgen in einem Strafverfahren führen können.

ZEIT GEWINNEN

Diese Zeit sollte genutzt werden, um die wichtigsten Entscheidungsträger, Unternehmensbereiche und Abteilungen für den Ernstfall zu informieren. Keinesfalls sollte jedoch der Eindruck entstehen, dass die Durchsuchung verzögert werden soll, um Beweismittel beiseite zu schaffen oder gar zu vernichten (ggf. Haftgrund!). Zeit wird insbesondere dafür benötigt, um organisatorische Vorkehrungen zu treffen, damit die Rechte der betroffenen Personen oder des ganzen Unternehmens wahrgenommen werden können.

Entscheidungsträger oder Vertretungsberechtigte (Geschäftsführer, Prokuristen, Vorstände etc.) sollten erreichbar sein und möglichst zeitnah im Unternehmen eintreffen, da Strafverfolgungsbehörden nicht verpflichtet sind, eine Zeitverzögerung von erheblicher Dauer zu dulden.

In den meisten Fällen wird ein Informationsgespräch zwischen den Ermittlungspersonen, den vertretungsberechtigten und einem Rechtsanwalt/Verteidiger den Druck aus der Situation nehmen. Der Rechtsanwalt/Verteidiger sollte im Vorfeld mit den Strukturen und Räumlichkeiten des Unternehmens vertraut gemacht werden.

Alle Mitarbeiter sämtlicher Abteilungen und Unternehmensbereiche sind darüber zu unterrichten, dass Personen der Strafverfolgungsbehörden unverzüglich zu den Entscheidungsträgern oder vertretungsberechtigten Personen geführt werden. Verzögerungen sind zwingend zu vermeiden, um die Ermittlungspersonen nicht zur Unruhe zu veranlassen.

ZUR PSYCHOLOGIE DER ÜBERRUMPELUNG

Der Überraschungs- und Überrumpelungseffekt einer Durchsuchung ist der gewollte psychologische Vorteil der Strafverfolgungsbehörden. Diesen Vorteil gilt es auszuschalten.

ES IST DAS OBERSTE GEBOT, KEINE ANGABEN GEGENÜBER ERMITTLUNGSPERSONEN ZU TÄTIGEN OHNE ZUVOR MIT DEM RECHTSANWALT ODER VERTEIDIGER GESPROCHEN ZU HABEN. DIES GILT FÜR FÖRMLICHE VERNEHMUNGEN VOR ORT, ABER AUCH FÜR INFORMATORISCHE BEFRAGUNGEN „GANZ NEBENBEI".

Das Mittel der informatorischen Befragung wird gerne genutzt, um erste Anhaltspunkte für das schnelle Auffinden von Beweismitteln zu erhalten.

Die vertretungsberechtigten Personen oder das einberufene Krisenmanagement müssen darauf achten, dass alle Mitarbeiter – sei es als Beschuldigte oder Zeugen – keine Äußerungen zur Sache tätigen.

Ermittlungspersonen neigen teilweise dazu, mit vermeintlichen Ermittlungserkenntnissen zu bluffen oder den betroffenen Personen weitere Durchsuchungen oder andere Zwangsmaßnahmen in Aussicht zu stellen, wenn sie nicht kooperieren. In den meisten Fällen wird sich dies als Finte herausstellen. Solche weiteren Zwangsmaßnahmen dürften in der Regel rechtswidrig sein. Die Erfahrung in der Praxis zeigt aber, dass solche Vorgehensweisen nicht selten Früchte tragen. Die Gründe, warum sich die betroffenen Personen immer wieder zur Kooperation verleiten lassen und somit auf ihre Rechte verzichten, sind vielseitig. Dies können persönliche Ängste sein aber auch ein mangelndes rechtliches Verständnis. Dies gilt es durch regelmäßige Schulungen und Anweisungen zu verhindern. Rechtliches Bewusstsein beugt auch der Gefahr vor, sich des Geheimnisverrats gem. § 203 StGB strafbar zu machen.

DIE DURCHSUCHUNG

Der Hausrechtsinhaber hat nur die Durchsuchung zu dulden und nicht eine Befragung von Kunden, Mitarbeitern oder anderen vor Ort befindlichen Personen. Das betroffene Unternehmen ist auch nicht verpflichtet, den Strafverfolgungsbehörden eine Ermittlungszentrale in eigenen Räumlichkeiten einzurichten. Aus psychologischer Sicht sollten die betroffenen Personen stets höflich jedoch bestimmt ihre Rechte wahrnehmen. ›››

„ES IST DRINGEND ZU RATEN, EINEN ODER MEHRERE „BEOBACHTUNGSPOSTEN“ AUFZUSTELLEN. DIE FUNKTION EINES BEOBACHTERS SOLLTE SICH AUF DAS BEOBACHTEN BESCHRÄNKEN. DENN ER KANN BEI MÖGLICHEN RECHTSVERSTÖSSEN (Z. B. UNZULÄSSIGE „UMSCHAU“ NACH ZUFALLSFUNDEN, BETEILIGUNG VON FREMDEN ERMITTLUNGSPERSONEN AUS ANDEREN ERMITTLUNGSVERFAHREN ETC.) ENTSPRECHEND SCHNELL REAGIEREN.

Insbesondere besteht die Möglichkeit bei Zufallsfunden oder bei der Durchsicht von Unterlagen (z. B. Dokumente/Papiere, aber auch EDV-Datenspeicher) darauf zu bestehen, dass die Durchsicht unterlassen wird und Unterlagen verpackt und versiegelt werden. Dasselbe gilt für die Mitnahme von Gegenständen und Unterlagen zur Durchsicht. Solch höfliche Aufforderungen und entsprechende Widersprüche gegen die Beschlagnahme durch die vertretungsberechtigten Personen lassen die Ermittlungspersonen wissen, dass die rechtlichen Grenzen nicht überschritten werden dürfen. Schließlich darf auch auf das Hausrecht freundlich aber bestimmt aufmerksam gemacht werden.

NACH DER DURCHSUCHUNG

Ist die Durchsuchung beendet, muss das Unternehmen den Informationsfluss gegenüber allen Beteiligten, also allen Betroffenen und gegebenenfalls außenstehenden Personen (Presse, Gesellschafter, Aktionäre, sonstige Mitarbeiter, Staatsanwaltschaft etc.) steuernd aufrechterhalten. Welche Maßnahmen im Einzelfall notwendig sind, lässt sich kaum pauschal beantworten.

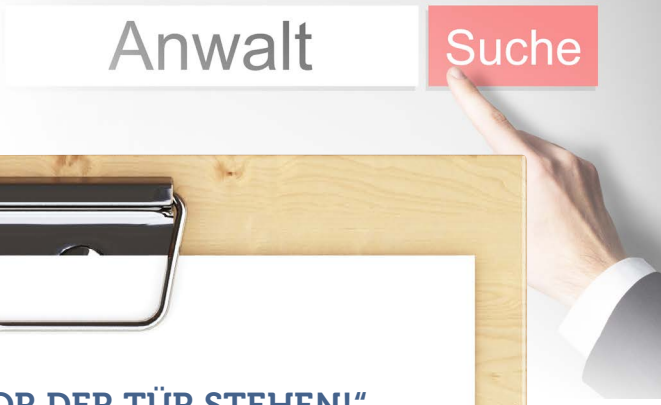
Große Bedeutung für den Verlauf des weiteren Verfahrens hat aber fast immer die erste Wahrnehmung und Interpretation des Falles durch die Beteiligten – insbesondere durch jene Personen, die später auch als Zeugen geladen werden könnten. Daher müssen alle Beteiligten unbedingt eine konsistente und klarstellende Erläuterung des Sachverhalts aus Unternehmenssicht erhalten, damit Gerüchten, Spekulationen und verschiedenen Versionen des Sachverhalts vorgebeugt werden kann. Behält das Unternehmen die Deutungshoheit über das Geschehen, hat dies einen psychologisch wichtigen Einfluss auf das weitere Ermittlungsverfahren. Hier ist eine sofortige, spezialisierte und professionelle Beratung durch erfahrene Verteidiger und bestenfalls auch Psychologen erforderlich.

> **i** Es ist dringend zu empfehlen, eine umfassende Dokumentation der Durchsuchung zu gewährleisten. Dies muss unmittelbar nach der Maßnahme erfolgen, weil Eindrücke und Gespräche noch im Wortlaut wiedergegeben werden können. Es empfiehlt sich hierzu ein zentralisiertes Erfassungssystem zu implementieren, mit welchem z. B. bereits strukturelle Vorgaben zentral gesteuert werden könnten.

WENN ERMITTLUNGSBEHÖRDEN KLINGELN IST GUT ÜBERLEGTES HANDELN DAS „A“ UND „O“!

Durchsuchungen stellen selbst erfahrene Unternehmer und Entscheidungsträger auf die Probe. Die größte Herausforderung ist das psychologische Überraschungsmoment. Unbedachtes Verhalten gegenüber Ermittlungspersonen kann schwerwiegende Folgen – auch strafrechtlicher Art – haben und darüber hinaus dem Unternehmen unnötig Schaden zufügen. Umso wichtiger ist es, Angestellte und Führungskräfte schon im Vorfeld möglicher Durchsuchungen über ihre Rechte aufzuklären und Abläufe sowie Verantwortlichkeiten für den Fall der Durchsuchung im Detail zu planen. Mit gut vorbereiteten Mitarbeitern, funktionierenden Alarmierungsketten, qualifiziertem Rechtsbeistand und dem richtigen Maß an Kooperation und Distanzierung sind die handelnden Verantwortlichen für diese Extremsituation gut gerüstet.

Dieser Artikel ist mit freundlicher Unterstützung von Th. Christian Jurascheck, Rechtsanwalt, Wilhelm Rechtsanwälte in Düsseldorf entstanden.



CHECKLISTE

„WENN ERMITTLUNGSBEHÖRDEN VOR DER TÜR STEHEN!“

- ☐ Wahrung von Rechten heißt rechtzeitige Information aller Beteiligten und genaue Dokumentation
  - ☐ Vorlage von Dienstausweisen / Vorsicht vor Pressevertretern!
  - ☐ Recht auf Anwesenheit bei der Durchsuchung (§ 106 StPO)
  - ☐ Anspruch auf Aushändigung des Durchsuchungsbeschlusses (§ 35 StPO) und des Beschlagnahmeverzeichnisses (§ 107 StPO)
  - ☐ Beschuldigte haben das Recht auf einen Verteidiger (§ 137 StPO)
  - ☐ Zeugen haben das Recht auf Beistand durch einen Rechtsanwalt
  - ☐ Aufklärung der Mitarbeiter über ihre prozessualen Rechte
  - ☐ Typische Erstkontaktpersonen bestimmen und konkret anweisen
- ☐ Entscheidungsträger für den Ernstfall bestimmen und besonders für den Umgang mit der Durchsuchungssituation schulen
- ☐ SOFORT einen Rechtsanwalt (Strafverteidiger) anrufen und diesen mit der Einsatzleitung verbinden
- ☐ Vertretungsbefugte Personen benachrichtigen
- ☐ Recht der vertretungsbefugten Personen zur Teilnahme an Durchsuchung gewährleisten
- ☐ Durchsuchungsumfang abstecken
  - ☐ Durchsuchungsbeschluss in Ruhe und genau lesen und prüfen …
    - ▸ Wer ist Beschuldigter?
    - ▸ Wo soll die Durchsuchung stattfinden?
    - ▸ Welche Gegenstände (Akten, Computer, etc) unterliegen möglicherweise der Beschlagnahme?
  - ☐ Unklarheiten beseitigen
  - ☐ Kommunikation mit den Ermittlungspersonen
- ☐ Heraussuchen von Beweismitteln, um Zufallsfunde zu vermeiden! Kopien fertigen! Keine freiwillige Herausgabe!
- ☐ Der Sicherstellung/Beschlagnahme von sämtlichen Gegenständen widersprechen (auch bzgl. dieser, welche herausgesucht wurden)
- ☐ Dokumentation ALLER Gespräche/Bemerkungen/Angaben, sichergestellter/beschlagnahmter Gegenstände und der beteiligten Ermittlungspersonen unmittelbar bei oder sofort nach der Durchsuchung! (Protokollierung im Wortlaut!)

SICHERHEITSBEWUSSTSEIN IMPLEMENTIEREN: INTRANET-RUBRIK „SECURITY“

Security Awareness wird als das „Schaffen von Sicherheitsbewusstsein“ verstanden. Dies bedeutet, dass mit Security Awareness das Wissen und die Einstellung zum Schutz der physischen und der informativen Werte etabliert wird. Doch das Wissen um das richtige Sicherheitsverhalten ist das eine, den Grund dafür zu verstehen und das Thema nachhaltig zu leben, das andere.

Das Schaffen von Sicherheitsbewusstsein kann durch vielerlei Methoden erzeugt werden. Der „Faktor Mensch“ sollte verstehen, dass es vielfältige Bedrohungsarten gibt und man sich bzw. das Unternehmen davor schützen muss. Daher ist der klassische Aufbau von „Security Awareness-Kampagnen“ wie folgt:

> „MITARBEITER MÜSSEN SICH PERSÖNLICH ANGESPROCHEN UND ABGEHOLT FÜHLEN, DENN NUR DANN WIRD SECURITY AWARENESS AUCH NACHHALTIG FUNKTIONIEREN.

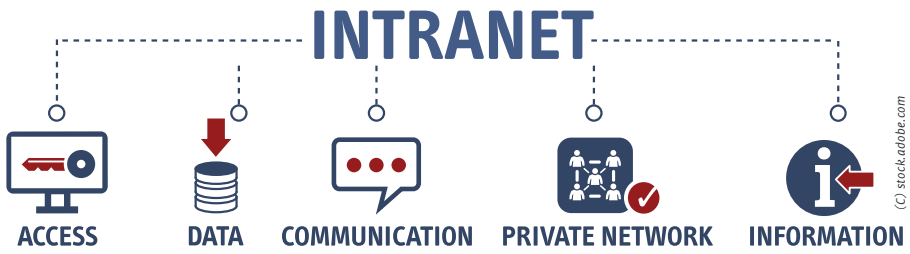
Bedrohungslage herausarbeiten → Daraus resultierende Risiken darstellen → Schutzmaßnahmen ableiten → Handlungsempfehlungen geben → Richtiges Verhalten vorgeben

Bei allen Lernprozessen, somit auch bei Security Awareness, ist es wichtig, dass das Interesse und die Motivation für das Thema erzeugt werden sollte. Dies kann man erreichen, indem beispielsweise eine persönliche Betroffenheit geschaffen oder der Bezug zum Privatleben hergestellt wird.

SICHERHEITSBEWUSSTSEIN NACHHALTIG INTEGRIEREN

Neben den klassischen Security Awareness-Schulungen sollte man Sicherheitsthemen im Unternehmen präsent gestalten. Denn 45 Minuten Schulung können keine Nachhaltigkeit entfalten, sondern lediglich einen ersten Ansatz zur Sensibilisierung darstellen. Dies gilt es im Alltag aufrecht zu erhalten. Gibt es einen Newsletter, eine Unternehmenszeitschrift, Informationswände oder dergleichen, auf denen das Thema „Sicherheit“ immer mal wieder „beworben“ wird? Viele Unternehmen nutzen das Intranet für die interne Unternehmens- und Abteilungsdarstellung sowie als Informationsportal. Warum also dort nicht auch eine eigene Sicherheits-Rubrik schaffen?

Wichtig im Intranet ist, dass der Inhalt möglichst übersichtlich dargestellt wird und von den Nutzern schnell gefunden und aufgerufen werden kann.



GLIEDERUNGS-ENTWURF INTRANET-RUBRIK „SECURITY“

„FÜR DIE SICHERHEITSKULTUR UND DIE AKZEPTANZ DES THEMAS LEISTET EINE INFORMATIVE UND NUTZWERTIGE INTRANET-RUBRIK EINEN EINDEUTIGEN MEHRWERT.

Die themen- bzw. aufgabenbezogene Einbindung in das Intranet bringt den Vorteil, dass sich interaktive Inhalte zur Verfügung stellen lassen, tagesaktuelle Meldungen eingestellt und verbreitet werden können und alle Bausteine der Sicherheit im Unternehmen abgebildet und erläutert werden können. Diverse Vorlagen können zum Herunterladen bereitstehen, Ansprechpartner und Prozesse können dargestellt werden und eine aktive Einbindung wie beispielsweise ein (Sicherheits-)Meldewesen oder ein Störfallmanagement lassen sich ebenfalls über digitale Formulare integrieren und abbilden.

Solch ein Informations- und Datensammel-Tool wie das Intranet entfaltet seine Wirkung als Security Awareness-Baustein nur, wenn die Rubrik nachhaltig und interessant gestaltet wird und die Mitarbeiter einen Grund haben, sich dort auch tatsächlich zu informieren. Dies kann beispielsweise durch Besucher- oder Fremdfirmenmeldungen, als Reisesicherheitsportal (Buchungen, Reisehinweise etc.), Ideen-Tool, für das Ausweiswesen („Laufkarte“ für neue Mitarbeiter) oder als Informations-Tool für beispielsweise Geheimschutz- oder Sabotageschutzanwendungen der Fall sein. Generell sollte für das Projekt „Intranet-Rubrik Security“ in jedem Fall ein Projektteam zusammengestellt werden, welches sich intensiv mit diesem Thema befasst, abteilungsübergreifend agiert und die redaktionelle Kontrolle behält.

SECURITY

1. **UNTERNEHMENSSICHERHEIT**

   → ANSPRECHPARTNER

   IT-Sicherheit / Unternehmenssicherheit / Krisen- und Notfallmanagement / Geheimschutz / Sabotageschutz / Sicherheitszentrale / Empfang / Datenschutz / Reisesicherheit etc.

   → KRISEN- UND NOTFALLMANAGEMENT
   - Bedeutung / Hintergrund
   - Was ist, wenn ...? ▸ Verhalten in Not- und Krisensituationen
   - Gebäuderäumung, Verhalten an der Sammelstelle etc.
   - Krisenkommunikation

   → SOCIAL ENGINEERING

   Erläuterung / Verhaltensempfehlungen / CEO Fraud etc.

   → SICHERHEIT AUF REISEN

   Ob Bus, Bahn, Taxi, Flugzeug: Richtiges Verhalten / Besonderheiten bei Auslandsreisetätigkeiten etc.

   → SICHERHEIT IM UNTERNEHMEN

   Besuchermanagement / Ausweisordnung / Fremdfirmenmanagement / Security-Awareness-Plakat / Richtiges Verhalten bei XY / Vorlagen, wie z. B. Diebstahl-/Verlustmeldung, Sicherheitsmeldungen etc. / Umgang mit Fundsachen etc.

2. **INFORMATIONSSICHERHEIT**

   Basisregeln / IT-Richtlinien / Sichere Passwörter / Umgang mit vertraulichen Daten (Datenklassifizierung) / Arbeitsplatz / Mobiles Arbeiten/ Arbeiten im Web etc.

3. **DATENSCHUTZ**

   Basisregeln / Datenschutz-Richtlinien / Umgang mit persönlichen Daten etc.

4. **AKTUELLES**

   Sicherheits-News / Sicherheitsmeldungen aus XY (Reisehinweise) etc.

5. **INTERAKTIVES SICHERHEITSFORUM**

   Interview des Monats / Sicherheitsvorschläge und -ideen / häufig gestellte Fragen und Antworten (Empfang, Sicherheitszentrale ...) etc.

6. **SICHERHEITSHINWEISE UND FORMULARE**

   Dokumentensammlung aller Kategorien etc.

Sicher-Gebildet.de
Qualität bildet den Unterschied

E-LEARNING-TRAININGS HEALTH + SAFETY + SECURITY

AUSZUG AUS UNSEREM ANGEBOT

CORPORATE SECURITY:

- IT-Sicherheit
- Unternehmenssicherheit
- Compliance im Unternehmen
- Krisen- und Notfallmanagement
- Datenschutz und Datensicherheit
- Umgang mit Bombendrohungen & Co.
- Reisesicherheit bei Auslandsaufenthalten
- u. v. w.

HEALTH AND SAFETY:

- Arbeitssicherheit
- Erste-Hilfe Unterweisung
- Brandschutzunterweisung
- Wahrnehmung von Gefahren
- Richtiger Umgang mit Gefahrstoffen
- Gebäuderäumungsübung
- Räumungshelfer/-in
- u. v. w.

Besuchen Sie uns online unter www.Sicher-Gebildet.de

DOKUMENTENSICHERHEIT UND SICHERE PROZESSE IM BEHÖRDEN- UND UNTERNEHMENSUMFELD

Der Schutz vor Manipulationen und Fälschungen von Dokumenten, Verträgen oder Entwicklungs-Know-how spielt seit jeher eine fundamentale Rolle. Ebenso wichtig ist die Möglichkeit einer nahtlosen Integration von Schutzmechanismen – idealerweise mit Zusatzfunktionen – in vorhandene Prozesse. Das heißt, für jeden Anwendungsfall die individuell passende Lösung zu gestalten und Möglichkeiten für eine effiziente Dokumentation und Kontrolle zu schaffen und zwar unabhängig von Tresorlagerung oder IT-Sicherheit. Doch wie funktioniert das Zusammenspiel von Sicherheits- und Zusatzfunktionen im Bereich Dokumentensicherheit?

Informationssicherheit, Datenschutz und Cybersecurity sind die derzeit heiß diskutierten Themen. Aber beim Schutz von Informationen, Daten und letzlich auch Know-how sollte man Printversionen – also die klassische Dokumentensicherheit (nicht die Sicherung von Dokumenten) – nicht außer Acht lassen. Verträge, behördliche Dokumente, Zertifizierungen etc. sind alle in einer Originalversion auf Papier verfügbar und müssen somit auch entsprechend geschützt werden. Denn der „klassische“ Stempel reicht bei weitem nicht aus, um ein Dokument fälschungssicher zu gestalten. Gleichzeitig soll und kann nicht jedes Dokument aus teurem Sicherheitspapier mit integrierten Sicherheitsmerkmalen hergestellt werden. Eine einfache und flexible Lösung, die neben der Sicherheit weitere Vorteile im Prozess bietet, sind Dokumentenklebesiegel.

DOKUMENTENKLEBESIEGEL: UNKOMPLIZIERT UND SICHER

Das Prinzip dieser Siegel ist einfach, aber wirksam: Beim Aufkleben werden der Klebstoff und die Farbe von einer Trägerfolie direkt auf das Dokument übertragen. Im Gegensatz zu Etiketten gibt es also keine Trägerfolie, die sich wieder ablösen ließe. Transfersiegel können anstelle konventioneller Stempel oder zum Schutz von Unterschriften eingesetzt werden. Sie dienen der Validierung bzw. rechtsgültigen Kennzeichnung (Authentifizierung, Beglaubigung) und erleichtern die Verfolgung von Straftaten wie beispielsweise dem Beschädigen, Ablösen oder Unkenntlichmachen dienstlicher Siegel nach § 136 Absatz 2 StGB (Siegelbruch). Dank ihres speziellen Aufbaus und ihrer integrierten Sicherheitselemente dienen sie als Originalitätsnachweis und bieten zusätzlichen Fälschungsschutz für Behördenformulare und sonstige Dokumente wie

- Urkunden
- Begleit- und Zolldokumente
- Verpackungsversiegelung
- Zulassungsunterlagen
- Schulungsbescheinigungen
- Zeugnisse
- Zertifikate
- Lieferscheine
- Parkausweise
- etc.

Denkbar wäre die Anwendung auch auf Geburtsurkunden, denn diese sind häufig das schwächste Glied in der Identitätskette. Werden diese manipuliert, ist der Weg zu einem gültigen Pass unter falscher Identität nicht mehr weit.

Hochsichere Dokumente wie Pässe und Ausweise entfalten nur dann ihren Nutzen, wenn sie auf korrekten Daten beruhen. Die Basis für deren Ausstellung sind häufig „einfache“ Dokumente, deren Sicherheit beispielsweise mittels der beschriebenen Dokumentenklebesiegel deutlich erhöht werden kann.

„Ein Original ist nur dann ein Original, wenn die Echtheit gewährleistet werden kann. Mit konventionellen Stempeln versehene Unterlagen sind leicht zu fälschen und derartige Manipulationen sowohl von Laien als auch von Behördenvertretern nur schwer zu erkennen. Abhilfe schaffen sogenannte Dokumentenklebesiegel, auch Transferklebesiegel genannt, die einen zuverlässigen Schutz vor Fälschung oder Vervielfältigung bieten.“

Kai Schnapauff, Leiter Geschäftbereich PrinTrust der Schreiner Group.

EIN DOKUMENTENKLEBESIEGEL MIT VIELFÄLTIGEN FUNKTIONEN

Ergänzend zu den „Basisfunktionen“ kann das Dokumentenklebesiegel je nach Anforderung individuell an die jeweilige Anwendung angepasst werden – Form, Farbe und Beschriftung sind frei wählbar. Zur genauen Dokumentation müssen Siegel immer mit einer Seriennummer ausgestattet werden. Diese macht die Siegel „zählbar“, das bedeutet, eine unbefugte Ausgabe von Siegeln wird so verhindert. Zudem wird die genaue Zuordnung eines Siegels zu einer ganz bestimmten Anwendung ermöglicht.

Wenn im Prozess eine exakte Positionierung des Siegels erforderlich ist – oder ganz allgemein die Handhabung vereinfacht werden soll – können die Siegel um eine Anfasslasche ergänzt werden. Dies ermöglicht eine sichere Handhabung, ohne dass die sensible Klebeschicht auf der Siegelrückseite beschädigt wird.

GERADE DIE VERBESSERTE KONTROLLE DER AUSGABE UND DOKUMENTATION IST EIN WICHTIGER BAUSTEIN IN EINEM SICHERHEITSKONZEPT. OHNE KONTROLLIERTE AUSGABE SIND SICHERHEITSMERKMALE IM SCHLIMMSTEN FALL SOGAR KONTRAPRODUKTIV, WEIL GEFÄLSCHTE DOKUMENTE MIT EINEM UNBEFUGT AUFGEBRACHTEN ECHTEN SICHERHEITSMERKMAL NUR NOCH SCHWER ERKANNT WERDEN KÖNNEN.

KLEBESIEGEL - FUNKTIONSWEISE

Das Dokumentensiegel wird an der Anfasslasche aus der Spendebox entnommen. Diese ermöglicht eine sichere Handhabung, ohne dass die sensible Klebeschicht auf der Siegelrückseite beschädigt wird. Optional ist die Anfasslasche mit einem 2D-Code für die Seriennummer versehen.

Die nur leicht klebende Lasche stellt sicher, dass das Siegel sauber geführt werden kann. Nach Aufbringen des Siegels verbleiben keine Klebereste am Finger.

Das selbstklebende Dokumentensiegel mit patentierter Anfasslasche erhöht den Manipulations- und Fälschungsschutz.

ANWENDUNGSBEISPIELE

→ NOTREISEDOKUMENT

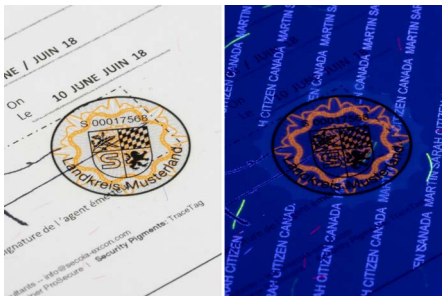
Notreisedokumente (Emergency Travel Documents – ETD) werden für humanitäre Zwecke an Personen ausgestellt, die keinen Reisepass oder ein sonstiges anerkanntes Reisedokument besitzen. Ein vom Internationalen Komitee des Roten Kreuz (IKRK) ausgestelltes Dokument dieser Art wurde mit Hilfe der Schweizer Sicherheitsberatungsfirma SECOIA entwickelt. Jedes dieser ETDs ist mit einer eindeutigen, im Letterpressverfahren gedruckten, sechsstelligen Seriennummer versehen. Diese ist zudem auf der Vorder- und Rückseite ertastbar und erscheint unter UV-Licht in einem fluoreszierenden Grün. Das IKRK ETD wurde von Schreiner PrinTrust mit Sicherheits-Transfersiegeln ausgestattet, in die mehrere Sicherheits- und eindeutige Zuordnungsmerkmale integriert sind. Während das Dokument selbst ausreichend geschützt ist, stellt die sichere Lagerung der Blankodokumente „im Feld“ vor deren Ausfertigung das größte Sicherheitsrisiko dar.

Transfersiegel auf Notreisedokumenten oder Geburtsurkunden sind mit diversen Sicherheits- und Zuordnungsmerkmalen ausgestattet, unter anderem mit einer Seriennummer.

→ FAHRZEUGZULASSUNG - SICHERHEIT UND MEHRWERTE

Nicht ordnungsgemäß zugelassene Fahrzeuge verursachen weltweit hohe Schäden – von Steuerausfällen über Kfz-Diebstähle bis hin zu erhöhten Sicherheitsrisiken, wie der Umgehung von Zufahrtskontrollen. Das „Dritte Kfz-Kennzeichen“ ist ein Sicherheitsetikett, welches durch die Zulassungsbehörde beim Ausgabeprozess mit verschiedenen Daten (Versicherungsnachweis, Steuer-oder Abgabenachweis, eine Parkberechtigung, Mautkarte oder Zufahrtskontrolle) versehen wird. Es wird an der Innenseite der Windschutzscheibe verklebt und damit die bekannten Kennzeichenschilder aus Metall ergänzt. Denn: Die außen montierten Nummernschilder können leicht gestohlen, kopiert und unberechtigt weiterverwendet werden. Beim Sicherheitsetikett ist dies nicht ohne weiteres möglich, da es sich im Fahrzeuginnenraum befindet und mit Schutzmechanismen gegen Manipulation und Fälschung ausgestattet ist. Zusätzlich ließe sich auch ein RFID-Chip integrieren, der noch mehr individuell programmierbare Funktionen beinhaltet.

((rfid))-3rd License Plate: Sicherheitslabel zur Kennzeichnung und Identifizierung von Fahrzeugen.



Unter UV-Licht werden die mehrfarbigen Sicherheitsstrukturen sichtbar.

MANIPULATIONSSICHERE DOKUMENTE SIND AUCH IM ZEITALTER DER ZUNEHMENDEN DIGITALISIERUNG WICHTIG!

Der Einsatz von Dokumentenklebesiegeln macht den Manipulationsschutz im Behörden- und Unternehmensumfeld noch wirksamer und effektiver. Während sich Dokumente, die mit herkömmlichen Stempeln und Unterschriften versehen sind, relativ leicht fälschen lassen und Manipulationen für Laien und Kontrollbehörden nur schwierig zu erkennen sind, bieten Transfersiegel durch die Kombination verschiedener Sicherheitsmerkmale eine zuverlässige Echtheitsprüfung und hohe Fälschungssicherheit. Die mögliche Dokumentation der Abgabemengen durch Nummerierung und integrierte Kontrollziffern verhindert einen Missbrauch zuverlässig und ein versuchter Diebstahl ist sofort offensichtlich.

Dieser Artikel ist mit freundlicher Unterstützung von Dr. Kai Schnapauff, Leiter PrinTrust der Schreiner Group entstanden.

ÜBERSICHT DER SICHERHEITSMESSEN 2020

(Sicherheits-)Messen und Kongresse bieten die Möglichkeit, (Sicherheits-)Anbieter und (Sicherheits-)Produkte zu finden und die neuesten Entwicklungen sowie den Stand der Technik live zu erleben. In begleitenden Workshops oder bei Fachveranstaltungen werden die neuesten Themen und Herausforderungen ausgiebig diskutiert und Lösungen sowie Herangehensweisen anschaulich dargestellt. Bei uns finden Sie eine aktuelle Übersicht der Sicherheitsmessen 2020.

SICHER DURCHS JAHR 2020

01 JANUAR

- 14.01. BIS 16.01.2020

PERIMETER PROTECTION
Internationale Fachmesse für Perimeter-Schutz, Zauntechnik und Gebäudesicherheit
Nürnberg

03 MÄRZ

- 04.03. BIS 05.03.2020

LUFTSICHERHEITSTAGE
Treffen der Luftsicherheitsexperten
Potsdam

- 08.03. BIS 13.03.2020

INTERSEC BUILDING
Internationale Plattform für vernetzte Sicherheitstechnik
Frankfurt am Main

- 11.03. BIS 13.03.2020

9. SICHERHEITSGIPFEL DER DEUTSCHEN WIRTSCHAFT
BVSW Wintertagung 2020
Schliersee-Spitzingsee

- 25.03. BIS 26.03.2020

secIT
Treffpunkt für Security-Anwender und -Anbieter
Hannover

04 APRIL

- 21.04.2020

VSW-JAHRESTAGUNG
Erfahrungsaustausch zwischen Sicherheitsbehörden und Wirtschaft
Mainz

- 21.04. BIS 23.04.2020

GPEC
Internationale Fachmesse für Polizei- und Spezialausrüstung
Frankfurt am Main

05 MAI

- 13.05. BIS 14.05.2020

21. DATENSCHUTZKONGRESS
Berlin

- 26.05. BIS 27.05.2020

VFS-KONGRESS
Sicherheit und Sicherheitstechnik für Anwender
Kassel

06 JUNI

- 15.06. BIS 20.06.2020

INTERSCHUTZ
Weltleitmesse für Feuerwehr, Rettungswesen, Bevölkerungsschutz und Sicherheit
Hannover

- 24.06. BIS 25.06.2020

SICHERHEITSEXPO
Sicherheitstechnik live demonstriert
München

09 SEPTEMBER

- 22.09. BIS 25.09.2020

SECURITY ESSEN
Weltleitmesse für zivile Sicherheit
Essen

10 OKTOBER

- 06.10. BIS 08.10.2020

IT-SA
Messe und Kongress für IT-Security
Nürnberg

11 NOVEMBER

- 10.11. BIS 11.11.2020

PROTEKT
Konferenz und Fachausstellung für den Schutz kritischer Infrastrukturen
Leipzig

SICHERHEIT IST UNSERE STÄRKE

UNSERE LEISTUNGEN

- SICHERHEITSBERATUNG
- SICHERHEITSKONZEPTIONEN
- REISESICHERHEIT IM AUSLAND
- EXT. SICHERHEITSMANAGEMENT
- KRISEN- UND NOTFALLMANAGEMENT
- BUSINESS-CONTINUITY-MANAGEMENT
- SECURITY-AWARENESS VIA E-LEARNING

Besuchen Sie uns online:
www.sius-consulting.com

SIUS
Consulting

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.

KURZ VORGESTELLT

INITIATIVE WIRTSCHAFTSSCHUTZ

Mit der im Jahr 2016 gegründeten „Initiative Wirtschaftsschutz“ steht erstmals in Deutschland eine zentrale Anlaufstelle von Staat und Wirtschaft für alle Fragen zum Thema Wirtschaftsschutz zur Verfügung. Die Sicherheitsbehörden – koordiniert vom Bundesministerium des Innern, für Bau und Heimat – informieren gemeinsam mit den Wirtschafts- und Sicherheitsverbänden über vielseitige Gefahren für die Wirtschaft und machen das Thema gerade kleinen und mittelständischen Unternehmen zugänglich.

Mit einem umfassenden Schutzkonzept, welches sämtliche Informationen zum Wirtschaftsschutz bündelt, hat es sich die „Initiative Wirtschaftsschutz“ zum Ziel gesetzt, zentrale Unternehmenswerte für Deutschland und seine Wirtschaft zu schützen. Gemäß dem Leitmotiv „Prävention durch Dialog und Information“ steht die Initiative als Anlaufpunkt für Unternehmen, Institutionen, Verbände und öffentliche Stellen zur Verfügung.

Folgende Themen werden auf der Webseite der „Initiative Wirtschaftsschutz“ erläutert:

- Spionage/Sabotage
- Cyberabwehr/Cybercrime/IT-Sicherheit
- Proliferation
- Sicherheit auf Geschäftsreisen
- Politisch motivierte Kriminalität/Extremismus/Terrorismus
- Wirtschaftskriminalität
- Sicherheitslage International
- Wirtschaft International
- u. v. m.

Erfahren Sie jetzt mehr unter www.wirtschaftsschutz.info

TIPP

PODCAST „CYBERCRIME“ VON hr iNFO

Der Hessische Rundfunk hat in den letzten Jahren mehrere Folgen des Podcasts „Cybercrime“ produziert. Dieser soll Interessierten einen tiefgehenden und praxisnahen Einblick in die Welt des „Cybercrime“ ermöglichen. Die Dramatik um das Thema wird bewusst aufgegriffen und mit umfangreichen Hintergrundinformationen und Recherecheinblicken ergänzt:

- Ein international agierender Konzern wird von einem Hackerangriff bedroht.
- Erfahrungen aus einem Cyberangriff auf ein Krankenhaus.
- Eine Hackerin gibt spannende Einblicke in ihr „Arbeit“.
- Ein Cybercrime-Ermittler fahndet im Netz nach einer Person, die ein Kind missbraucht hat.

Alle beleuchteten Cybercrime-Themen, die auf realen Fällen und Personen beruhen, werden aus drei unterschiedlichen Perspektiven beleuchtet: die Ermittlersicht, die Täterperspektive und die Opfersituation. Erfahren Sie jetzt mehr unter www.hr-inforadio.de/podcast/cybercrime/

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.stock.adobe.com

SICHERHEIT. DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.