SICHERHEIT. DAS FACHMAGAZIN.

SICHERHEIT AUF DEN PUNKT GEBRACHT.

SIUS Consulting

KOMPETENZPARTNER

© frantzybex - stock.adobe.com

MEHRWERT

1

Sorglos zu spielen

hilft Kindern dabei, ihre Fähigkeiten voll zu entfalten.

2

Dafür brauchen

sie ein liebevolles, friedliches Zuhause. Genau das bieten wir Kindern in Not weltweit.

3

Nur so wachsen

sie zu mitfühlenden Persönlichkeiten heran, die diese Welt positiv verändern.

4

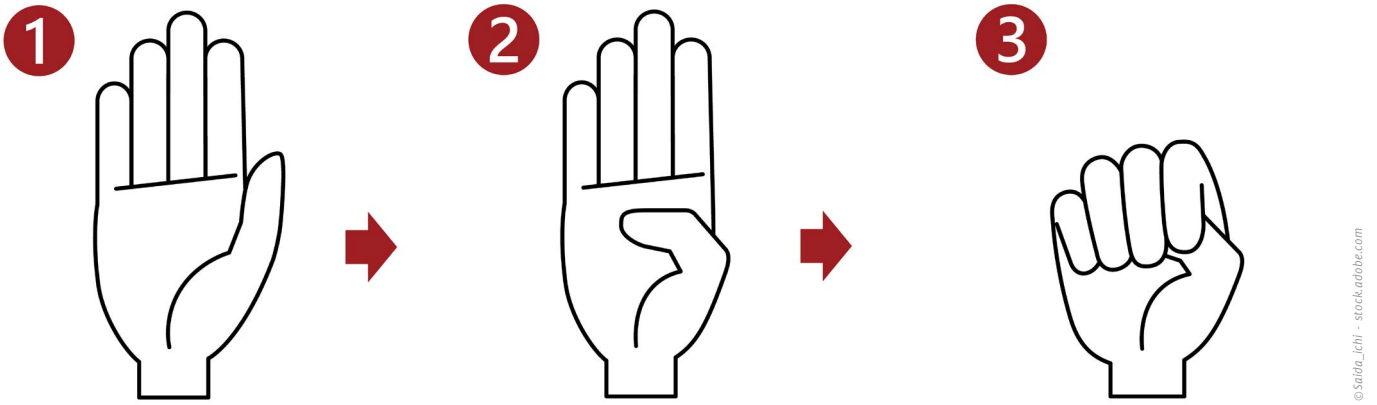
So schaffen wir

eine friedlichere Welt mit Mehrwert für alle. Unterstützen Sie uns dabei.

sos-kinderdoerfer.de

SOS KINDERDÖRFER WELTWEIT

Mit freundlicher Unterstützung von:
SIUS Consulting (www.sius-consulting.com)



©Saida_ichi - stock.adobe.com

1. HAND SENKRECHT NACH OBEN HEBEN. DIE FLACHE HAND ZEIGT MIT DER HAND-INNENFLÄCHE NACH VORNE.

2. DEN DAUMEN ZUR HANDFLÄCHE FÜHREN UND NACH INNEN KNICKEN, SODASS ER DIE HANDINNENFLÄCHE BERÜHRT.

3. DEN DAUMEN MIT DEN RESTLICHEN VIER FINGERN UMSCHLIESSEN, SODASS EINE FAUST MIT EINGESCHLOSSENEM DAUMEN ENTSTEHT.

EIN EINFACHES HANDZEICHEN, DAS JEDER KENNEN SOLLTE!

Signal For HELP

Die Opferzahlen häuslicher Gewalt sind in den vergangenen Jahren stets gestiegen. Für viele Betroffene ist es schwierig, auf ihre Situation aufmerksam zu machen, weil sie von ihren Peinigern z. B. beobachtet und kontrolliert werden oder in der jeweiligen Situation nicht offen sprechen können.

Aus diesem Grund hat die „Canadian Women's Foundation" ein Handzeichen ins Leben gerufen, welches international verstanden werden kann. Diese kleine, unauffällige, non-verbale und einhändige Geste soll Betroffenen helfen, einen Hilferuf abzusetzen und sich beispielsweise im persönlichen Kontakt, in Video-Chats, in Bilderfolgen oder in den sozialen Netzwerken bemerkbar zu machen.

! FÖRDERN AUCH SIE DEN BEKANNTHEITSGRAD DES HILFEZEICHENS – BEISPIELS-WEISE DURCH TEILEN IN DEN SOZIALEN NETZWERKEN #SIGNALFORHELP

VERHALTENSEMPFEHLUNG, WENN SIE EIN SOLCHES (HILFE-)ZEICHEN BEMERKEN

Sollten Sie dieses Zeichen bei einer Person erkennen, ist das ein klarer Hilferuf an Sie. Ein bedachtes und unauffälliges Handeln hat nun oberste Priorität, um sich und die betroffene Person nicht unnötig zu gefährden und den Täter auch nicht auf den Hilferuf aufmerksam zu machen.

Bereits die öffentliche Äußerung stellt ein hohes Risiko dar und ist somit ein großer Schritt für die Betroffenen. Stellen Sie möglichst behutsam Fragen, die mit „Ja" oder „Nein" beantwortet werden können, denn Sie wissen nicht, ob die Person allein ist oder Nachrichten beispielsweise mitgelesen werden. Bleiben Sie mit der Person möglichst in „unverfänglichem" Kontakt und alarmieren Sie bei der nächsten Gelegenheit unverzüglich die Polizei.

„Geht es den Kindern gut?"

„Soll ich mich später nochmal melden?"

„Kann ich vorbeikommen?"

„Soll ich jemanden anrufen, der dir helfen kann?"

KOSTENLOSE TELEFONNUMMERN VON BERATUNGSSTELLEN

FÜR BETROFFENE FRAUEN	FÜR BETROFFENE MÄNNER
0800 / 011 60 16	0800 / 123 99 00

© iStunningART - stock.adobe.com

RISIKOFAKTOR MENSCH: VON DER GEFAHR ZUR RESSOURCE!

„Wie kann ich meine Mitarbeiter davon abhalten, das Falsche zu tun?“. So oder so ähnlich lauten die Fragen, die sich Unternehmen stellen, die ihren Betrieb vor Cyberattacken schützen wollen. Der Mensch, also der oder die Mitarbeiter/-in, steht dabei oft als die Gefahrenquelle im Fokus. Schließlich sind es Menschen, die einen Link in einer Phishing-Mail öffnen. Es ist der Kollege, der unbedarft einen fremden USB-Stick ansteckt und es ist die Kollegin, die bereitwillig Passwörter über das Telefon weitergibt, nur weil das Gegenüber angibt, der Systemadministrator zu sein.

Es werden Anhänge geöffnet, Überweisungen getätigt, Sicherheitssysteme umgangen und das nicht aus dem Willen heraus, dem Unternehmen zu schaden. Dies passiert, weil wir Menschen gelernt haben, gesellschaftlichen Normen und Regeln zu folgen. So haben wir gelernt, Autoritäten zu folgen oder verspüren das Bedürfnis, uns für Gefallen zu revanchieren oder jemandem mit schwerer Last die Tür aufzuhalten. Derartige Handlungen vollbringen wir täglich viele Male und diese sind für uns so selbstverständlich, dass sie völlig automatisch und unbewusst ablaufen.

DER MENSCH ALS GEFAHR?!

Diese „hilfsbereiten" Automatismen sind tief in uns verankert. Wer die Trigger für solche gelernten und automatisierten Handlungsabläufe kennt, kann Menschen und ihre Handlungen beeinflussen und bewusst „auslösen". Da genügt es, ein großes und schwer wirkendes Paket in den Händen zu halten und die Wahrscheinlichkeit, die Tür aufgehalten zu bekommen, steigt (auch in einem eigentlichen gesicherten Bereich) signifikant. Bekannte Betrugsmaschen wie der sogenannte „CEO-Fraud", wo Mitarbeiter vom vermeintlichen Top-Manager des Unternehmens durch Autorität und Zeitdruck bewusst so unter Druck gesetzt werden, dass sie große Geldsummen ohne große Rückfragen freigeben, zeigen, wie gefährlich solche Manipulationstaktiken sind. Wie enorm das Schadenspotenzial solcher Taktiken ist, zeigen die Verluste, die Unternehmen aufgrund solcher Angriffe in den vergangenen Jahren verzeichneten. So kann davon ausgegangen werden, dass bereits 90 % der deutschen Unternehmen mindestens einmal von Datendiebstahl, Sabotage oder Spionage betroffen waren.

SCHÄDEN DURCH DATENDIEBSTAHL, SABOTAGE ODER SPIONAGE = MEHRERE MILLIARDEN EURO JÄHRLICH.

Es ist also durchaus berechtigt darüber nachzudenken, wie Unternehmen vor solchen Angriffen geschützt werden können. Genau an diesem Punkt kommt dann oft die zu Beginn gestellte Frage – wie Mitarbeitende davon abgehalten werden können, etwa aus unreflektierter Autoritätshörigkeit oder purer Höflichkeit Opfer eines solchen Angriffs zu werden.

Dabei ist nicht der Mensch an sich das Problem. Es ist vielmehr die Tatsache, dass diese Verhaltensweisen eben in den meisten Fällen unbewusst und unreflektiert ablaufen und ein „Ausbrechen" aus den gewohnten Mustern genauso wie das Melden solcher Vorfälle aufgrund einer negativen Fehlerkultur mit Scham und Angst vor Konsequenzen behaftet ist.

MIT WENIGEN ADAPTIONEN IM ARBEITSALLTAG KÖNNEN BEDEUTSAME (SICHERE) UNTERSCHIEDE ERZIELT WERDEN.

WIE HANDELN MITARBEITER IM SINNE DER INFORMATIONSSICHERHEIT?

AUTOMATISIERTE VERHALTENSWEISEN BEWUSSTMACHEN

Genau an dieser Stelle ist der Ansatzpunkt, solche Angriffe effektiv zu verhindern oder es den Angreifern zumindest so schwierig als möglich zu machen. Mitarbeiter müssen darin bestärkt werden, diese gewohnten und unreflektierten Verhaltensmuster abzulegen. Das geht nur, wenn Scham und Angst vor Konsequenzen abgebaut werden.

Die meisten Menschen kostet es zum Beispiel Überwindung, bei einer (scheinbaren) Autoritätsperson bei (vorgespieltem) Zeitdruck und trotz angedrohter Konsequenzen auf die Einhaltung der Sicherheitsbestimmungen zu bestehen. Es stellt sich also die Frage, wie den Mitarbeitenden dabei geholfen werden kann, aus diesen Automatismen auszubrechen, bewusst eine Handlung zu tätigen und Vorfälle im Anlassfall sofort zu melden.

Gemeint ist nicht, alle sozialen Normen, Umgangsformen und höfliches Handeln abzulegen. Es geht darum, dass sich Mitarbeiter ihre bisherigen automatisierten Handlungen bewusst und somit einer Reflexion zugänglich machen. Damit Mitarbeiter gewohnte Verhaltensweisen ablegen und durch bewusstes Handeln ersetzen, braucht es Rahmenbedingungen, die durch die Organisationsstruktur hergestellt werden können. ›››

1. NOTWENDIGE RESSOURCEN ZUR VERFÜGUNG STELLEN

Eine wichtige Voraussetzung ist, dass Mitarbeitern notwendige Ressourcen bereitgestellt werden, damit sie die von ihnen verlangten Maßnahmen auch umsetzen können. Gemeint sind zum einen Handlungsanleitungen und Policies, auf die sich Mitarbeiter berufen können und die ihnen Handlungssicherheit geben – auch entgegen gelernter sozialer Normen zu agieren. Mitarbeiter müssen darin bestärkt werden, auf Sicherheitsmaßnahmen zu bestehen und nicht etwa durch Führungskräfte dafür getadelt oder sogar bestraft werden. Zum anderen sind damit Ressourcen gemeint, die die Einhaltung von Sicherheitsmaßnahmen direkt unterstützen. So kann etwa das leidige Passwortthema schnell und sicher durch die Bereitstellung einer „Schlüsselbund-Applikation“ gelöst werden.

2. FEHLERKULTUR UND VORFALLMANAGEMENT

Es braucht eine Atmosphäre, in der beinah oder tatsächlich erfolgte Angriffe niederschwellig gemeldet werden können. So können Schwachstellen zeitnah behoben und bei Angriffen schnell reagiert werden. Das bedeutet zum einen das Melden von (Sicherheits-) Vorfällen zu bestärken und zum anderen eine Meldestelle einzurichten, wo die Meldungen von einer sachkundigen Stelle, die den Vorfall bewerten kann, entgegengenommen werden. Ein anonymes Meldesystem oder ein Ombudsmann könnten erste Maßnahmen sein. Eine weitere Entwicklungsmöglichkeit wäre der interne oder sogar interorganisationale Austausch über (beinah) Angriffe im Sinne eines „Lessons Learned Prozesses“.

3. BEDEUTSAMKEIT UND RELEVANZ DES HANDELNS WÜRDIGEN

Mitarbeiter müssen den Kontext und die Relevanz ihrer Handlungen für das Unternehmen verstehen und durch ihre Führungskraft als relevantes Element zum Schutz des Unternehmens verstanden, so behandelt und entsprechend wertgeschätzt werden.

> **„ES IST WEDER KOMPLIZIERT NOCH TEUER, AUS DEM „RISIKOFAKTOR MENSCH“ EINE RESSOURCE FÜR DIE INFORMATIONSSICHERHEIT EINES UNTERNEHMENS ZU MACHEN.**

Wenn Mitarbeiter einen Sinn darin sehen, verdächtige Situationen bewusst wahrzunehmen, sie die Relevanz ihrer Rolle im Kampf gegen solche Angriffe vermittelt bekommen und dafür die notwendigen Rahmenbedingungen zur Verfügung haben, ist die Wahrscheinlichkeit signifikant höher, dass solch ein Angriff erfolglos bleibt oder zumindest gemeldet wird und somit schnell reagiert werden kann. Diese drei Elemente lassen sich im Arbeitsalltag schnell und kostengünstig umsetzen und haben dabei ein enormes Potenzial, die Informationen und damit den Erfolg des Unternehmens nachhaltig zu schützen.

Dieser Artikel ist mit freundlicher Unterstützung von Teresa Allum entstanden.

WERBUNG

Sicher-Gebildet.de
Qualität bildet den Unterschied

SICHERHEITS-UNTERWEISUNGEN VIA E-LEARNING (24/7)

RECHTSSICHER + REVISIONSSICHER + ZERTIFIZIERT

www.Sicher-Gebildet.de

(DEN) UMGANG MIT VERDÄCHTIGEN GEGENSTÄNDEN UND POSTSENDUNGEN (FÖRDERN)!

HERRENLOSER KOFFER
UNBEAUFSICHTIGTE (HAND-)TASCHE
ABGELEGTE PLASTIKTÜTE
ALLEINSTEHENDER RUCKSACK
ABGESTELLTES PAKET
DEPONIERTES PÄCKCHEN
LIEGENGEBLIEBENER BRIEF
LIEGENGELASSENE KLEIDUNGS-STÜCKE

Das Auffinden eines verdächtigen Gegenstandes oder die Zustellung einer verdächtigen Postsendung können eine ernstzunehmende (Bedrohungs-)Situation darstellen, die eine unmittelbare Gefahr für Leib und Leben bedeutet, denn nicht immer handelt es sich „nur" um Attrappen. Viele Betroffene wissen im ersten Moment nicht, wie sie mit der Gefahrensituation umgehen sollen und welches Verhalten angemessen ist. Das eigene Verhalten im Umgang mit verdächtigen Gegenständen kann jedoch entscheidend für den weiteren positiven oder gar negativen Verlauf der Situation sein.

Bildquellen v. o.
© Photoiger - Gregory - stock.adobe.com
© Ivan Ismi - stock.adobe.com
© Sergey Klopotov - stock.adobe.com

i WAS IST EINE UNKONVENTIONELLE SPRENG- UND BRANDVORRICHTUNG?

Eine unkonventionelle Spreng- und Brandvorrichtung (kurz „USBV") ist eine selbst hergestellte, veränderte oder missbräuchlich benutzte Vorrichtung, die eine Explosion oder einen Brand herbeiführen kann und dadurch Leib und Leben von Menschen sowie Sachwerte gefährdet.

Bei Gegenständen, bei denen der begründete Verdacht besteht, dass es sich um eine scharfe (sprengfähige), handhabungs- und transportunsichere Vorrichtung handeln könnte, die bewusst Leib und Leben von Personen beeinträchtigen und beträchtliche Sachwerte beschädigen oder vernichten kann, handelt es sich um verdächtige Gegenstände.

Verdächtige Gegenstände können

- Sprengstoffe,
- Brandsätze, aber auch
- chemische, biologische, radioaktive oder nukleare Stoffe enthalten,

die nach dem äußeren Anschein in meist unverdächtigen Gegenständen deponiert werden.

Anhaltspunkte für einen verdächtigen Gegenstand können sein:

- die Beschaffenheit des Gegenstandes,
- eventuelle Geräusche aus dem Inneren sowie
- der Fundort, insbesondere allgemein zugängliche Bereiche wie z. B. Ein- und Ausfahrten, Ein- und Ausgänge, Eingangshallen, Flure, Treppenhäuser, Aufzüge, Toiletten usw.

Ein (offensichtlich) verdächtiger Gegenstand kann ggf. auch ein Ablenkungsmanöver für andere (Folge-)Taten sein. Gehen Sie daher grundsätzlich davon aus, dass es nicht der einzige Gegenstand ist und versetzen Sie das Unternehmen in Alarmbereitschaft. Grundsätzlich sollte sich beim Auffinden von verdächtigen Gegenständen immer die Frage gestellt werden:

- ⇨ WAS MACHT DIESER GEGENSTAND
- ⇨ ZU DIESEM ZEITPUNKT
- ⇨ AN DIESEM ORT UND
- ⇨ WIE IST ER DAHINGELANGT?

Gerade die Stärkung des Sicherheitsbewusstseins innerhalb der Belegschaft – insbesondere beim Empfang, Sicherheitsdienst oder dem Waren- und Posteingang – ist essenziell, um verdächtige Gegenstände oder Postsendungen möglichst frühzeitig zu erkennen und ein situationsgerechtes Verhalten im Alltag zu erreichen.

„DAS (RECHTZEITIGE) ERKENNEN VERDÄCHTIGER GEGENSTÄNDE/POSTSENDUNGEN KANN LEBEN RETTEN UND PERSONEN VOR SCHWEREN GESUNDHEITLICHEN BEEINTRÄCHTIGUNGEN BEWAHREN SOWIE SACHBESCHÄDIGUNGEN VERHINDERN.

WELCHE BEDROHUNGSARTEN GIBT ES?

Bei einer Bedrohung unterscheidet man zwischen 3 verschiedenen Arten der Bedrohung:

REELLE BEDROHUNG

Mit der reellen Bedrohung ist z. B. der klassische „Sprengstoffgürtel“ gemeint. Für jeden gut sichtbar, geht von einem Gegenstand oder einer Person die reelle Gefahr einer konkreten Bedrohung aus. Derartige Szenarien müssen immer als sehr ernst und realistisch eingestuft werden.

LATENTE BEDROHUNG

Bei der latenten Bedrohung handelt es sich z. B. um herrenlose Koffer, Taschen, Pakete und sonstige Gegenstände, die keinem eindeutigen Besitzer zugeordnet werden können und somit eine ernstzunehmende Bedrohung darstellen.

FIKTIVE BEDROHUNG

Die fiktive Bedrohung ist die am häufigsten auftretende Form der Bedrohung. Sie ist frei erfunden und hat keinen ernstzunehmenden Hintergrund. Grundsätzlich sollten Bedrohungen jedoch immer ernstgenommen werden, um Täter nicht unnötig zu provozieren.

VERHALTENSEMPFEHLUNGEN UND PERSÖNLICHE SCHUTZMASSNAHMEN

SO VERHALTEN SIE SICH RICHTIG:

1. Bewahren Sie Ruhe!
2. Verdächtige Gegenstände/Postsendungen müssen an Ort und Stelle verbleiben. Sie dürfen auf keinen Fall berührt, geschüttelt oder gar geöffnet werden – ebenso wenig ist daran zu riechen.
3. Verwenden Sie in der unmittelbaren Nähe ab sofort kein drahtloses Kommunikationsmittel mehr (z. B. Mobiltelefon oder Funkgerät). Verzichten Sie ebenso auf die Verwendung anderer elektronischer Geräte (z. B. Fotoapparat), da dies zum Auslösen des Zündmechanismus führen kann.
4. Fordern Sie alle anwesenden Personen dazu auf, die nähere Umgebung des verdächtigen Gegenstands bzw. der verdächtigen Postsendung unverzüglich zu verlassen und sichern Sie den Zutritt zum Bereich (z. B. Tür abschließen, Absperrband anbringen, Aufsichtsperson abstellen).
5. Verständigen Sie daraufhin unverzüglich:
   - die im Betrieb zuständigen Personen, z. B. Ihren Vorgesetzten, den Sicherheitsdienst oder das Facility Management sowie
   - die zuständige Polizeidienststelle und stellen Sie sich als Ansprechpartner/Zeuge zur Verfügung.
6. Sollten Sie in Kontakt mit dem Gegenstand bzw. der Postsendung gekommen sein, ziehen Sie sich die Oberbekleidung aus und bewahren Sie diese in einer Plastiktüte auf. Vermeiden Sie vorerst das Rauchen sowie Essen und Trinken.

WERBUNG

SICHERHEIT IST UNSERE STÄRKE!

SIUS
Consulting

SICHERHEITSBERATUNG.DE

KRISENMANAGEMENT.DE

SICHERE KOMMUNIKATION: „DER SCHLÜSSEL“ IN HERAUSFORDERNDEN GESPRÄCHSSITUATIONEN

Kennen Sie diese oder ähnliche Situationen? Ihr Kunde oder Gesprächspartner, möglicherweise sogar jemand aus dem eigenen Team, beginnt erregt auf Sie einzureden. Ohne dass Sie es wollen, entbrennt eine heftige Diskussion. Ein Wort folgt auf das andere. Es kommt zu Provokationen und Beleidigungen. Die gegenseitige Erregung steigt und es ist nicht klar, wohin dieses Gespräch führt oder wie es endet. Fest steht: Für beide Seiten ist dies ein unzufriedenstellendes Ergebnis!

Durch die Initiative und Erregung Ihres Gesprächspartners ist eine hohe Gesprächsdynamik entstanden, der Sie sich eigenständig nur schwer entziehen konnten. Dadurch ist die eigene Emotionalität gestiegen und Sie haben sich direkt in die Diskussion hereinziehen lassen. Dies verstärkt die Dynamik der Situation zusätzlich, besonders in Situationen, in denen Sie selber gestresst sind.

Eine derartige Eskalation von Gesprächssituationen lässt sich mit einer „sicheren“ Kommunikation – also der individuellen Aufmerksamkeit und den Blick für Stimmungen und situative Dynamiken – vermeiden. Kommunikatives Verhalten in kritischen Situationen ist Bestandteil von Deeskalationstrainings, die den Fokus auf extremere Formen eskalierter Situationen wie z. B. körperliche Übergriffe, Umgang mit alkoholisierten Personen etc. richten. Derartige Situationen müssen allerdings im „normalen“ Berufsalltag nicht erwartet werden, daher setzt eine „sichere“ Kommunikation weit vorher an.

Besonders prekär wird es, wenn Sie das Verhalten des Gesprächspartners nicht einschätzen können, beispielsweise aufgrund von kulturellen Unterschieden oder weil Ihr Gegenüber Ihnen einfach nur rätselhaft erscheint. In derartigen Situationen ist es wichtig, dass der Gesprächspartner nicht zusätzlich irritiert wird und insbesondere der Distanzbereich gewahrt bleibt (dies ist kulturell sehr unterschiedlich, von ca. 50 cm bis 2 m). Gehen Sie auf die offensichtlichen Unterschiede ein, erklären und begründen Sie Ihre Handlungen und Verhaltensweisen ggf. mehrmals. Geben Sie Ihrem Gesprächspartner die Möglichkeit, offensichtliche Schwierigkeiten zu artikulieren, indem Sie etwa sagen: „Bitte geben Sie mir Bescheid, wenn Ihnen etwas unangenehm ist.“ ›››

GESPRÄCHSPARTNER (GP)

Begrüßt Sie unhöflich.

EIGENES (UNGÜNSTIGES) ALLTAGSVERHALTEN

Sie lassen sich diesen Ton nicht gefallen. Sie sprechen unhöflich zurück. Sie erregen sich vielleicht sogar und werten Ihren Gesprächspartner ab.

Besseres Verhalten „SICHERE“ KOMMUNIKATION

Ruhe bewahren, mögliche Unklarheiten hinterfragen, weiterhin respektvoll kommunizieren und die Unklarheit auf sich beruhen lassen.

KOMMUNIKATIVE GRUNDREGEL: VERURTEILEN SIE IHREN GESPRÄCHSPARTNER BEI EINEM FEHLVERHALTEN NICHT GLEICH, SONDERN GEBEN SIE IHM IMMER EINE ZWEITE CHANCE.

Gelassen bleiben und auf den Anlass der Unterhaltung konzentrieren. Sollte sich tatsächlich eine provozierende Absicht herausstellen, ergründen Sie die Ursache.

„Ich habe den Eindruck, dass Sie sich über etwas ärgern. Wollen Sie mir den Grund dafür verraten?“

Sie fühlen sich durch Ihren GP provoziert, möglicherweise sogar vor Dritten.

Sie beginnen ein Streitgespräch, weil Sie sich bloßgestellt fühlen. Die Situation wird hektisch und sie geraten u. U. in eine isolierte Position, weil es Ihrem GP gelingt, stellvertretend für die anderen Anwesenden (Dritten) zu sprechen.

Eine (vermeintliche) Drohung wird ausgesprochen.

Sie übernehmen das Gesprächsniveau und reagieren mit einer Gegendrohung.

Ruhig und respektvoll bleiben und auf den eigentlichen Anlass Ihres Gespräches konzentrieren.

Sollte die Drohung ernst gemeint sein, zeigen Sie höflich die Konsequenzen auf (Beendigung des Gespräches, Hausrecht etc.)

Es kommt zu einem raschen und erregten Wortwechsel.

Sie lassen sich auf diesen Wortwechsel ein und fallen Ihrem GP ins Wort. Dabei verwenden Sie wiederholt „bessere“ Argumente.

Lassen Sie Zeit zu antworten. Vermeiden Sie hitzige Diskussionen. Kurze Gesprächspausen zulassen und weiterhin respektvoll und ruhig verhalten.

BLEIBEN SIE IMMER RUHIG, HÖFLICH UND RESPEKTVOLL.

Ihr GP hat Sie missverstanden und wirkt nun konsterniert und verärgert.

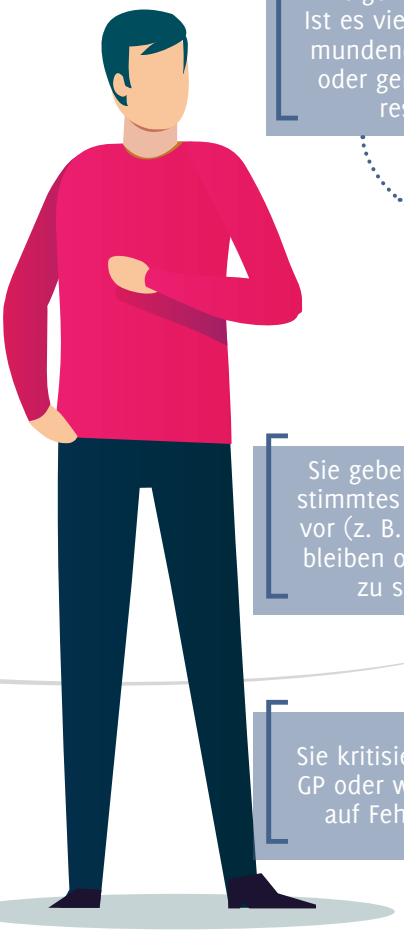
Sie nehmen das mangelnde Verständnis nicht ernst und sprechen deshalb ironisch und anspielungsreich. Womöglich kritisieren Sie ihn sogar dafür, dass er nicht gleich verstanden hat.

Respektvoll bleiben, die Erklärung möglichst unmissverständlich wiederholen und nach dem Verständnis des Sachverhaltes fragen.

Die Umgebung verunsichert den Gesprächspartner.

Sie ignorieren das Unbehagen und ändern Ihr Verhalten nicht.

Unbehagen ernst nehmen und ggf. Umgebungswechsel anbieten. Nach Vorschlägen für eine Erleichterung der Situation fragen.



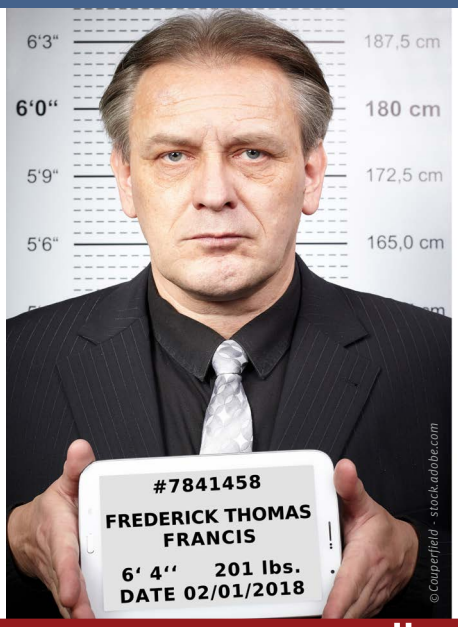
IHRE REAKTIONEN//IHR VERHALTEN	EIGENES (UNGÜNSTIGES) ALLTAGSVERHALTEN	Besseres Verhalten „SICHERE“ KOMMUNIKATION
Hinterfragen Sie Ihr eigenes Verhalten: Ist es vielleicht zu bevormundend, zu vorschnell oder generell zu wenig respektvoll?	Es ist Ihnen unangenehm, über Ihr Verhalten nachzudenken oder es überfordert Sie. Sie ändern Ihr Verhalten nicht, Ihr Ziel ist es, das Gespräch zu Ende zu bringen.	Sie zeigen sich aufmerksamer, entschuldigen sich ggf. und versuchen das Gespräch wieder auf Anfang zu setzen.
Sie geben ein bestimmtes Verhalten vor (z. B. sitzen zu bleiben oder ruhig zu sein).	Sie bestehen auf Ihre Grenzsetzungen, obwohl Sie bemerken, dass Ihr GP sichtlich Schwierigkeiten damit hat.	Verhalten rücksichtsvoller gestalten und ggf. einen Kompromiss finden.
Sie kritisieren Ihren GP oder weisen ihn auf Fehler hin.	Sie ziehen Ihre Kritik rücksichtslos durch und stellen Ihren GP ggf. vor Dritten bloß. Ihr GP fühlt sich dadurch gedemütigt oder verängstigt.	Kritik diskret und wertschätzend vortragen, dabei sachlich bleiben und Möglichkeit zur Erwiderung geben.
Eine Meinungsverschiedenheit mit Ihrem Gesprächspartner entwickelt sich zu einem Streitgespräch.	Sie haben (aus Ihrer Sicht) eindeutig Recht und setzen den Streit konsequent fort, indem Sie auf Ihrer Meinung beharren.	Ruhig bleiben, die eigene Position noch einmal verdeutlichen. Ggf. jedem seinen Standpunkt belassen. Findet sich keine Lösung, das Gespräch beenden.

1. **ES SCHWÄCHT IHRE POSITION NICHT, WENN SIE FEHLER, DIE SIE GEMACHT HABEN, IM GESPRÄCH EINGESTEHEN. ES STÄRKT TENDENZIELL SOGAR DIE VERTRAUENSWÜRDIGKEIT GEGENÜBER IHREM GESPRÄCHSPARTNER.**
2. **JE MEHR SIE IHREN GESPRÄCHSPARTNER GEGEN SEIN BEDÜRFNIS EINSCHRÄNKEN, DESTO MEHR WIDERSTAND WIRD ER LEISTEN.**
3. **IHR GESPRÄCHSPARTNER SOLLTE IMMER SEIN GESICHT WAHREN KÖNNEN!**

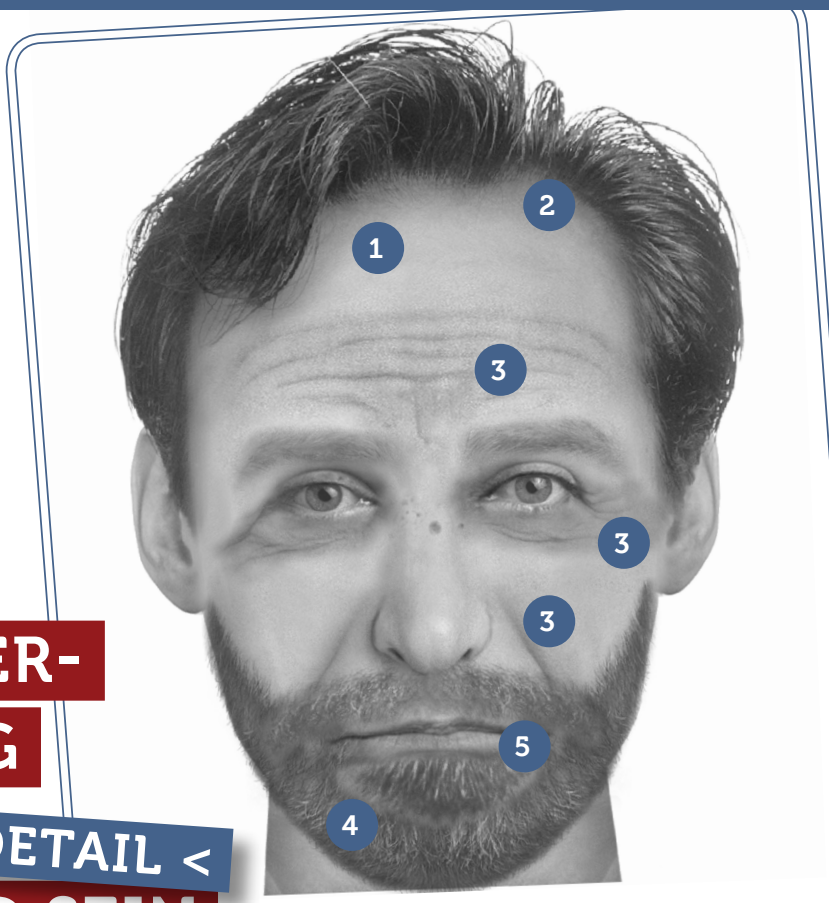
> RESPEKT UND WERTSCHÄTZUNG SOLLTEN EIN WESENTLICHER BESTANDTEIL DER INNEREN HALTUNG, INSBESONDERE IN HERAUSFORDERNDEN GESPRÄCHSSITUATIONEN SEIN.

Bei der „sicheren“ Kommunikation geht es um Respekt und aktive Wertschätzung, die die gesamte Dauer der Kommunikation umfasst. Egal wie sich Gesprächssituationen entwickeln, eine positive und konstruktive Haltung sowie sachliche Argumentation und ausreichend Informationen schätzt jeder Gesprächspartner. Jeder noch so hektischen Gesprächssituation lässt sich mit Ruhe begegnen, um die Dynamik herauszunehmen und handlungsfähig zu bleiben. Jede Person möchte gehört werden und Gehör finden. Daher ist es wichtig, Gesprächen aktiv zu folgen, Emotionen weitgehend außen vor zu lassen und erst bei Gesprächspausen einzusetzen.

Dieser Artikel ist mit freundlicher Unterstützung von Patrick Beham von der Personalentwicklung Beham-Berger entstanden.



BEI EINER TÄTER-BESCHREIBUNG KANN > JEDES DETAIL < ENTSCHEIDEND SEIN



1. Hoher Haaransatz
2. Seitenscheitel
3. Tiefe Stirn-/Augen-/Mundfalten
4. Vollbart
5. schmale Lippen

Verbrechen dauern meist nur einen Bruchteil von Sekunden: Täter tauchen auf, schlagen zu und sind ebenso schnell wieder weg, wie sie gekommen sind. Haben Sie eine Straftat beobachtet oder sind womöglich selbst zum Opfer geworden, ist es für die Aufklärungsarbeit der Strafverfolgungsbehörden essenziell, eine möglichst detaillierte Täterbeschreibung – also eine Beschreibung des Aussehens oder Verhaltens der Person, die der Straftat beschuldigt wird – abgeben zu können.

Sollte es keine Videoaufzeichnungen geben, die der Ermittlungsarbeit dienen, ist das Gedächtnis des Zeugen/Opfers zur Beschreibung des Täters enorm wichtig, um beispielsweise ein Phantombild zeichnen zu können.

EINE KURZE NOTIZ ODER EIN SPRACHMEMO (IM SMARTPHONE) NACH DER TAT KANN DEM GEDÄCHTNIS HELFEN, SICH SPÄTER DETAILLIERT ZU ERINNERN.

SOLLTE ES GEFAHRLOS MÖGLICH SEIN, IST EIN FOTO DES TÄTERS DER BESTE BEWEIS.

PERSONENBESCHREIBUNG UND KONKRETE TATMERKMALE

Wichtiger als ein allgemeiner (erster) Eindruck sind klare Beschreibungen des Aussehens und der äußeren Merkmale sowie besondere Auffälligkeiten. Alles was dazu dient, dass eine Person im Nachgang identifiziert werden kann, sollte beschrieben werden.

Insbesondere bei den Tatmerkmalen können kleine Nebensächlichkeiten ausschlaggebend sein, um einen Täter zu überführen. Daher können Aussagen

- zum Fluchtfahrzeug,
- zur Fluchtrichtung,
- der Bewaffnung,
- zur Beute sowie
- zu den verwendeten Hilfsmitteln

sehr wichtig sein.

>> CHECKLISTE <<
TÄTERBESCHREIBUNG

©SIUS Consulting - www.sius-consulting.com

GESCHLECHT: ☐ Mann / ☐ Frau

ALTER: ca. _____
☐ Erwachsener / ☐ Jugendlicher / ☐ Kind

GRÖSSE: ca. _____cm

KÖRPERFORM:
☐ schlank / ☐ dick / ☐ kräftig /
☐ sportlich/athletisch / ☐ auffallend dünn

GESICHTSFORM:
☐ oval / ☐ rund / ☐ eckig /
☐ herzförmig / ☐ trapezförmig

AUGENFARBE:
☐ blau / ☐ grün / ☐ braun /
☐ grau / ☐ bernsteinfarben

WEITERE GESICHTSBESCHREIBUNG:
Augenbrauen, und zwar: _____
Nase, und zwar: _____
Lippen, und zwar: _____
Ohren, und zwar: _____
Hals, und zwar: _____

☐ geschminkt / ☐ natürlich / ☐ verdeckt /
☐ schmutzig / ☐ unreine Haut

HAUTFARBE:
☐ weiß / ☐ rosa / ☐ hellbraun /
☐ dunkelbraun / ☐ schwarz

HAARFARBE:
☐ schwarz / ☐ blond / ☐ rot /
☐ grau / ☐ braun
☐ gefärbt, und zwar: _____
Besonderheiten, und zwar: _____

FRISUR:
☐ kurz / ☐ lang / ☐ gewellt / ☐ lockig /
☐ Afro / ☐ Glatze
☐ offen / ☐ halboffen / ☐ gebunden /
☐ hochgesteckt / ☐ gegelt

BRILLE:
☐ nein / ☐ ja, und zwar (Form): _____

BART:
☐ nein / ☐ ja, und zwar (Form, Farbe): _____

SPRACHE:
☐ hochdeutsch / ☐ Dialekt, und zwar: _____
☐ Fremdsprache, und zwar: _____

BEKLEIDUNG:
☐ Maske / ☐ Mütze / ☐ Kappe / ☐ Hut / ☐ Tuch
☐ Jacke / ☐ Pullover / ☐ T-Shirt / ☐ Hemd /
☐ Unterhemd
☐ Hose lang / ☐ Hose kurz / ☐ Kleid / ☐ Rock / ☐ Anzug
☐ Halbschuhe / ☐ Stiefel / ☐ Sandalen /
☐ Flip-Flops / ☐ barfuß
☐ Weiteres: _____

BESONDERHEITEN BEI DER BEKLEIDUNG:
☐ Farbe, und zwar: _____
☐ Aufdruck, und zwar: _____
☐ Abzeichen, und zwar: _____
☐ Löcher, und zwar: _____
☐ zerschlissen / ☐ neuwertig / ☐ getragen

SONSTIGE BESONDERHEITEN:
☐ Schmuck, und zwar: _____
☐ Tattoo, und zwar: _____
☐ Piercing, und zwar: _____
☐ Narben, und zwar: _____

12 HÄUFIGE SICHERHEITSIRRTÜMER (VERSTÄNDLICH) ENTLARVT

Überall werden Tipps zum „sicheren“ Surfen oder „richtigen“ Umgang mit E-Mails und IT-Sicherheit gegeben. Jedoch ist es für den Laien nicht immer einfach, nützliche Tipps von schlechten Mythen zu unterscheiden. Manche Tipps, die mittlerweile weit verbreitet sind, bergen mitunter sogar risikoreiche Handlungsansätze, die wiederum zu anderen Problemen führen können. In vielen Fällen hilft bereits eine Portion Skepsis und der Einsatz des gesunden Menschenverstands dabei, Betrugsversuchen und Hinterhalten frühzeitig auf die Schliche zu kommen.

INTERNET-SICHERHEIT

SICHERHEITSIRRTUM NR. 1: EIN SICHERES PASSWORT SCHÜTZT!?

Nein, denn sollte ein Onlinedienst gehackt und das Passwort gestohlen werden, sind alle mit diesem Passwort geschützten Dienste in Gefahr. Insbesondere bei der Verwendung von E-Mail-Adressen zur Authentifizierung lassen sich Nutzername und Passwort gut zuordnen. Daher ist ein gutes und sicheres Passwort unerlässlich – es sollte aber bei jedem Onlinedienst ein anderes Passwort gewählt werden. Besonders bei Diensten, die sensible Daten enthalten oder abfragen (z. B. Onlinebanking oder Onlineshopping), ist auf ein starkes und sicheres Passwort zu achten.

GRUNDSÄTZLICH SOLLTE EIN PASSWORT MIT EINER LÄNGE VON MINDESTENS 8 ZEICHEN, GROSS- UND KLEINBUCHSTABEN SOWIE SONDERZEICHEN UND ZIFFERN GEWÄHLT WERDEN. ZUDEM SOLLTEN PASSWÖRTER IN REGELMÄSSIGEN ZEITLICHEN ABSTÄNDEN GEÄNDERT, KEINESFALLS NOTIERT ODER MEHRFACH FÜR UNTERSCHIEDLICHE ONLINEDIENSTE GENUTZT WERDEN.

"Am liebsten trinke ich mein Wasser mit Eis und 1 Scheibe Zitrone."

Merken Sie sich nur den ersten Buchstaben eines jeden Wortes und Sie erhalten ein starkes und sicheres Passwort.

©Edler von Rabenstein - stock.adobe.com

SICHERHEITSIRRTUM NR. 2: DIE FIREWALL SCHÜTZT!?

Leider ist es nicht so einfach. Ohne die richtige Konfiguration bietet eine Firewall keinen optimalen Schutz vor Angriffen aus dem Internet. Die sogenannte „Personal Firewall“ kontrolliert den eingehenden und abgehenden Datenfluss, um den PC vor Schadprogrammen zu schützen. Angriffe aus dem Internet nutzen jedoch jede Sicherheitslücke in installierten und genutzten Programmen wie auch in der Firewall selbst aus.

WIE BEI JEDER SOFTWARE GILT DESHALB AUCH BEI DER FIREWALL: VOR ALLEM DIE KONFIGURATION IST ENTSCHEIDEND UND DIES GILT AUCH FÜR DIE FIREWALL VON INTERNET-ROUTERN. NUR MIT DEN RICHTIGEN FILTERREGELN UND EINSTELLUNGEN KANN DIE SICHERHEIT DES COMPUTERS GEWÄHRLEISTET WERDEN. EINSTELLUNGEN SOLLTEN REGELMÄSSIG ÜBERPRÜFT UND FILTERREGELN SO DEFINIERT WERDEN, DASS NUR UNBEDINGT NOTWENDIGE ZUGRIFFE ERLAUBT SIND. VERLANGT EIN NICHT BEKANNTES PROGRAMM ZUGRIFF AUF DAS INTERNET, SOLLTE DIES KRITISCH GEPRÜFT WERDEN.

©Pasko Maksim - stock.adobe.com

SICHERHEITSIRRTUM NR. 3: VERTRAUENSWÜRDIGE WEBSEITEN SIND SICHER!?

Anwender, die sich auf gängigen und bekannten Webseiten mit seriösem Inhalt bewegen, denken, sie „surfen“ auf sicherem Terrain. Leider können auch vertrauenswürdige seriöse Webseiten hin und wieder von Schadprogrammen befallen sein. Diese verstecken sich beispielsweise in Werbebannern oder in sogenannten „Drive-by-Downloads“, bei denen Inhalte ohne Zutun des Nutzers im Hintergrund heruntergeladen werden oder in schädlichen „Scripts“.

ES IST RATSAM, SICH NUR AUF VERTRAUENSWÜRDIGEN WEBSEITEN AUFZUHALTEN – DIES SCHÜTZT ABER NICHT AUSREICHEND VOR CYBER-ANGRIFFEN. EIN GRÜNDLICHER SCHUTZ DURCH ANTIVIRENPROGRAMME UND FIREWALLS SOWIE REGELMÄSSIGE SICHERHEITSUPDATES SIND TROTZ ALLER VORSICHT EMPFEHLENSWERT.

SICHERHEITSIRRTUM NR. 4: ANTIVIRENPROGRAMME SCHLAGEN BEI GEFAHR ALARM!?

Zwar ist ein Antivirenprogramm unerlässlich für sicheres Surfen im Internet – Updates für die genutzten Anwendungen sollten jedoch immer schnellstmöglich installiert werden. Jedes auf den eigenen Geräten installierte Programm birgt die potenzielle Gefahr, aus dem Internet angegriffen zu werden. Aktuelle Schadprogramme können bestehende Sicherheitslücken ausnutzen, bevor sie von Antivirenprogrammen erkannt werden. Die Angreifer nutzen dabei beispielsweise das Zeitfenster aus, in dem ein neu entwickeltes Schadprogramm von dem Antivirenprogramm noch nicht erkannt wird. Daher versuchen Softwarehersteller fortwährend, mit Updates und sogenannten „Patches“ (englisch für „Flicken“), Sicherheitslücken in ihren Programmen zu schließen.

MIT UPDATES UND PATCHES WIRD VERHINDERT, DASS SCHADPROGRAMME ÜBERHAUPT WIRKSAM WERDEN KÖNNEN. ANTIVIRENPROGRAMME SOLLTEN JEDERZEIT AKTUELL GEHALTEN WERDEN. DENN SIE BIETEN NUR DANN ZUSÄTZLICHEN SCHUTZ, WENN SIE MIT UPDATES AUF DEM NEUESTEN STAND GEHALTEN WERDEN.

©robert - stock.adobe.com
©Andrey - stock.adobe.com

Weiter auf der nächsten Seite. ›››

VIRTUELLES LIVE-EVENT
für die Kontrollraumbranche

Neue Impulse, kreative Lösungen und innovative Techniktrends. Eine Plattform, die aus der Kontrollraumbranche nicht mehr wegzudenken ist. Am **22. September** öffnet sich der Vorhang für den digitalen ko:mon – Kongress für Kontrollraumtechnik und Monitoring – erstmalig auf der virtuellen Bühne.

Auf Gäste dieses außergewöhnlichen **Live-Events** warten nicht nur exklusive Einblicke in eindrucksvolle, zukunftsorientierte Leitwarten-Konzepte. **Angesehene Experten** haben sich zudem mit Keynotevorträgen angekündigt, die zielsicher den Kern treffen, wenn es um die **Aussichten des Kontrollraumsektors** im Jahrzehnt des digitalen Wandels geht.

Jetzt kostenlos anmelden und bei der Premiere des virtuellen ko:mon dabei sein – „Power up your systems!“

KOSTENLOS ANMELDEN

22.09.2021
www.digital.ko-mon.de

- **„Update Zukunft – der Kontrollraum nach Corona“**
  – einen Blick in die Kristallkugel der Leitwartenwelt wagt Gesellschaftsforscher Michael Carl.
- **„Überleben in der digitalen Welt von morgen“**
  – darum geht es Mentalcoach Oliver Geisselhart, der zum „Survival-Training für das Gehirn“ einlädt.

COMPUTER-SICHERHEIT

SICHERHEITSIRRTUM NR. 5: DIE CLOUD IST SICHER!?

Das ist so nicht richtig. Zwar bietet die Datenspeicherung in der Cloud eine Reihe von Vorteilen: die vom Anbieter bereitgestellten Sicherheitsmechanismen, die Möglichkeit des Zugriffs auf die eigenen Daten jederzeit über das Internet und von jedem Gerät aus sowie das Einsparen von Speicherplatz vor allem auf mobilen Endgeräten. Es gibt Cloud-Dienste, deren Sicherheit und Verfügbarkeit hoch ist. Dennoch kann der Fall eintreten, dass der Nutzer nicht mehr auf seine Daten zugreifen kann. Technische Probleme, Ausfälle beim Dienstleister oder gar die Einstellung eines Cloud-Dienstes sind mögliche Gründe.

DURCH DIE NUTZUNG EINER CLOUD IST NICHT GARANTIERT, DASS DIE DATEN IMMER VERFÜGBAR SIND. ES IST ALSO UNERLÄSSLICH, WICHTIGE DATEN NICHT NUR AN EINEM ORT – WIE IN EINER CLOUD – ZU SPEICHERN, SONDERN REGELMÄSSIG BACKUPS, ALSO DUPLIKATE DER DATEN, AUF EINEM ANDEREN (EXTERNEN) SPEICHERMEDIUM ZU ERSTELLEN. DABEI SOLLTE BEDACHT WERDEN, DASS AUCH ANDERE GERÄTE, FESTPLATTEN UND SPEICHERMEDIEN UNERWARTET KAPUTT ODER VERLOREN GEHEN ODER GESTOHLEN WERDEN KÖNNEN.

SICHERHEITSIRRTUM NR. 6: GELÖSCHTE DATEN SIND NICHT WIEDERHERSTELLBAR!?

Falsch. Um Daten unwiederbringlich von einem Gerät oder Datenträger zu entfernen, sind zusätzliche Schritte nötig. Wenn Nutzer ein altes Gerät oder ein nicht mehr benötigtes externes Speichermedium entsorgen möchten, sollte sichergestellt werden, dass vorher alle Daten sicher gelöscht wurden. Das Verschieben von Dateien in den Papierkorb und das Leeren reicht dabei nicht aus. Einzig das Überschreiben von Daten lässt diese bei bestimmten Speichermedien auf Nimmerwiedersehen verschwinden.

UM DATEN ENDGÜLTIG UND SICHER ZU LÖSCHEN, SOLLTEN SPEZIELLE PROGRAMME ZUM EINSATZ KOMMEN. FALLS EIN GERÄT ODER SPEICHERMEDIUM SICH NICHT ÜBERSCHREIBEN LÄSST, SOLLTE ES PHYSIKALISCH ZERSTÖRT WERDEN. NUR SO KANN EINE WIEDERHERSTELLUNG DER DATEN UNMÖGLICH GEMACHT WERDEN.

SICHERHEITSIRRTUM NR. 7: ALS NUTZER HABE ICH NICHTS ZU VERBERGEN!?

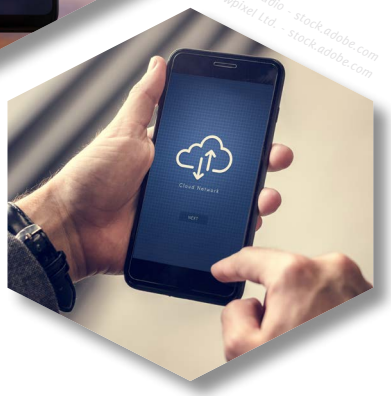
Diese Ansicht ist grundlegend falsch, da Kriminelle alle Daten für ihre Zwecke nutzen können. Das sind nicht unbedingt die gespeicherten Urlaubsfotos, Korrespondenzen oder andere private Dokumente. Von einem weitgehend ungeschützten Rechner können Kriminelle gespeicherte oder ins Internet übertragbare Zugangs-, Konto- und Kreditkartendaten leicht stehlen und missbrauchen. Spätestens bei „Ransomware-Angriffen“, bei denen Daten verschlüsselt werden und nur gegen eine Lösegeldzahlung wieder frei verfügbar sind, stellen viele Nutzer fest, dass es doch zahlreiche schützenswerte Daten gibt. Unzureichend abgesicherte Geräte können ebenfalls Bestandteil eines Botnetzes werden und somit für kriminelle Zwecke missbraucht werden.

JEDER, DER MIT EINEM UNGESCHÜTZTEN GERÄT IM INTERNET SURFT, EINKAUFT ODER ONLINEBANKING BETREIBT, NUTZT UND HINTERLÄSST EINE VIELZAHL AN DATEN, FÜR DIE SICH KRIMINELLE INTERESSIEREN.

SICHERHEITSIRRTUM NR. 8: SCHADPROGRAMME MACHEN SICH BEMERKBAR!?

Nicht immer kann ein Anwender feststellen, ob sich auf seinem Computer ein Schadprogramm eingenistet hat. Es gibt verschiedenste Arten von Schadprogrammen, die Angreifer auf unterschiedlichen Wegen einschleusen können. Viele Schadprogramme verfügen bspw. über Funktionen zum Identitätsdiebstahl. Diese verfolgen das Ziel, den Nutzer auszuspähen, also beispielsweise Zugangs-, Konto- und Kreditkartendaten auszuspionieren. Vollkommen unauffällig verhalten sich auch solche Schadprogramme, die einem Angreifer die Fernsteuerung von infizierten Geräten ermöglicht. Diese Art von Schadprogramm wird beispielsweise durch E-Mail-Anhänge, das Öffnen einer speziell manipulierten Webseite oder den Klick auf einen infizierten Werbebanner geschleust.

ES GIBT KEINEN HUNDERTPROZENTIGEN SCHUTZ VOR DIESEN BEDROHUNGEN. ANWENDER KÖNNEN JEDOCH MIT MASSNAHMEN WIE EINEM ANTIVIRENPROGRAMM UND EINER FIREWALL SOWIE DER REGELMÄSSIGEN NUTZUNG VON SOFTWARE-UPDATES UND EINEM SENSIBLEN UMGANG MIT E-MAIL-ANHÄNGEN DEN SCHUTZ MASSGEBLICH ERHÖHEN. ANWENDER SOLLTEN IM ZWEIFEL STETS DARAUF VERZICHTEN, SOFTWARE ODER ANDERE DATEN AUS UNBEKANNTEN QUELLEN HERUNTERZULADEN ODER ZU INSTALLIEREN.



Bildquellen v. o.:
©WrightStudio - stock.adobe.com
©Rawpixel Ltd. - stock.adobe.com

Weiter auf der nächsten Seite. ›››

Und? Können wir Ihnen helfen? Sicher!

Wer schützt Ihre Verwaltung, Ihren Betrieb oder Ihre Produktionsstätte? Wer unterstützt Sie bei der Sicherstellung von reibungslosen Abläufen? Wir sind einsatzbereit!
Als Qualitätsanbieter für Sicherheitsdienstleistungen mit über 3.600 Mitarbeiter*innen deutschlandweit sind wir jederzeit für Sie da. Zu unserem Team gehören übrigens auch 110 top geschulte Wachbegleithunde.

Unsere Mitarbeiter*innen – auch die vierbeinigen – werden in der Klüh-eigenen Sicherheitsschule, die bereits seit 1981 besteht, perfekt auf ihre Einsatzgebiete vorbereitet.
So hat sich Klüh Security in über sechs Jahrzehnten großes Vertrauen und eine erstklassige Reputation erarbeitet.

Wir sichern Großveranstaltungen, Ausstellungen und Messen, betreuen VIPs, stellen Sicherheitskräfte an Flughäfen und sind seit vielen Jahren starker Partner der sicherheitssensiblen Finanzbranche. Auch die Bundeswehr vertraut seit Jahrzehnten unserer Kompetenz. Wir übernehmen Verantwortung aus Überzeugung und bieten gern auch Ihnen zuverlässigen Schutz und Sicherheit!

www.klueh.de

klüh MULTISERVICES

E-MAIL-SICHERHEIT

© fizkes - stock.adobe.com

SICHERHEITSIRRTUM NR. 9: DER ABSENDER EINER E-MAIL IST KLAR ERKENNBAR!?

Das ist falsch, denn Absenderadressen von E-Mails können mit geringem Aufwand beliebig gefälscht werden. Hinter dem in einer E-Mail angezeigten Namen einer Person oder Organisation kann sich ein anderer Absender verbergen – dies ist üblicherweise bei illegalen Aktivitäten der Fall, wie Spam-Versand oder dem Versuch, den Computer eines Nutzers mit einem Schadprogramm zu infizieren. Einen ersten Hinweis auf den Absender gibt das Rüberfahren mit der Maus über den angezeigten Namen, so wird die – angeblich – verwendete E-Mail-Adresse angezeigt.

BEI E-MAIL-ABSENDERADRESSEN SOLLTE IMMER GENAU HINGESEHEN WERDEN (RECHTSCHREIBUNG, DOMAIN, MAUSZEIGERNUTZUNG). AUCH BEI E-MAILS VON SCHEINBAR BEKANNTEN ABSENDERN KANN ES SICH UM SPAM HANDELN. HIER HILFT EIN BLICK AUF DIE BETREFFZEILE, UM ZU BEURTEILEN, WIE WAHRSCHEINLICH ES IST, DASS GERADE DIESE PERSON EINE ENTSPRECHENDE FORMULIERUNG VERWENDET.

SICHERHEITSIRRTUM NR. 10: EINE E-MAIL NUR ZU ÖFFNEN BIRGT NOCH KEINE RISIKEN!?

Das trifft leider nicht zu. Viele E-Mails werden heute im HTML-Format verschickt. Im Gegensatz zu reinen Text-E-Mails sind diese oftmals farbig, mit verschiedenen Schriften und Grafiken gestaltet. Im sogenannten Quellcode einer HTML-formatierten E-Mail lauert die Gefahr: ein schädlicher Code, der bereits beim Öffnen der E-Mail auf dem Computer des Empfängers ausgeführt wird, ohne dass dafür ein Anhang angeklickt werden muss.

NUTZER SOLLTEN IM E-MAIL-PROGRAMM DIE ANZEIGE VON E-MAILS IM HTML-FORMAT DEAKTIVIEREN. DIE E-MAILS WERDEN DANN ZWAR NUR IM REINTEXT ANGEZEIGT UND KÖNNEN SCHLECHT LESBAR UND UNVOLLSTÄNDIG ERSCHEINEN. BEI VERTRAUENSWÜRDIGEN ABSENDERN KANN DER EMPFÄNGER DIE HTML-ANSICHT DER E-MAIL PER KLICK AUF EINE SCHALTFLÄCHE AKTIVIEREN UND DIE INHALTE VOLLSTÄNDIG BETRACHTEN.

© Nicolas Herrbach - stock.adobe.com

© Nokhoog - stock.adobe.com

SICHERHEITSIRRTUM NR. 11: PHISHING-VERSUCHE FALLEN SOFORT AUF!?

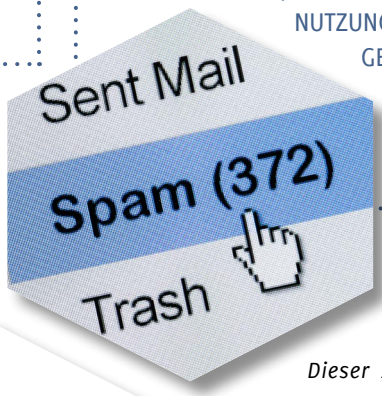
Das Ziel von Phishing ist es, den Opfern Zugangsdaten zu Onlineshops, Onlinebanking, E-Mail-Konten oder anderen Internetdiensten zu entlocken. Eine der beliebtesten Methoden dabei ist, E-Mails von bekannten Diensten zu fälschen und den Empfänger darin aufzufordern, einem Link zu folgen, um dort beispielsweise Stornierungen oder eine angeblich sicherheitsrelevante Bestätigung der Nutzerdaten vorzunehmen. Die Aufmachung solcher E-Mails und der hinterlegten Webseiten sehen den Originalen oftmals täuschend ähnlich.

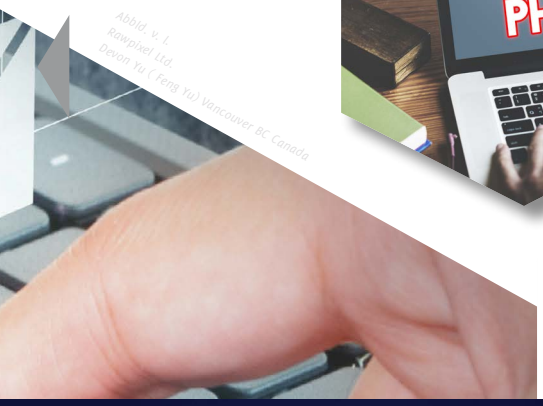
VERDÄCHTIGE E-MAILS SOLLTEN NICHT GEÖFFNET WERDEN. LINKS IN SOLCHEN E-MAILS DÜRFEN NICHT ANGEKLICKT WERDEN! IM ZWEIFEL KÖNNEN NUTZER DIE SEITE DES ANBIETERS MANUELL IM BROWSER AUFRUFEN UND SICH DIREKT AUF DER DORTIGEN PLATTFORM EINLOGGEN, UM SICH IM HINBLICK AUF DIE ECHTHEIT ZU VERGEWISSERN.

SICHERHEITSIRRTUM NR. 12: MAN KANN SICH VON SPAM-E-MAILS ABMELDEN!?

Unter dem Begriff „Spam“ werden verschiedene Arten unerwünschter E-Mails zusammengefasst. Dazu gehören unaufgefordert zugesandte Werbung für teilweise zweifelhafte Produkte und Dienstleistungen, Nachrichten mit merkwürdigen Inhalten und so genannte Phishing-E-Mails. Egal, um welche Art unaufgeforderter E-Mail es sich handelt, sollten Empfänger diese ignorieren und umgehend löschen, am besten, ohne sie zuvor überhaupt zu öffnen. Auf keinen Fall sollten Nutzer Verlinkungen folgen, die vermeintlich dazu führen, dass die Empfängeradresse aus der Liste gelöscht wird. Sobald Sie als Empfänger auf solch eine E-Mail reagieren, weiß der Versender, dass Ihre Adresse gültig und aktiv ist. Die Folge ist ein umso höheres Aufkommen an unerwünschten E-Mails.

DAS ABMELDEN VON SPAM-E-MAILS FÜHRT HÄUFIG ZU NOCH MEHR SPAM. ES EMPFIEHLT SICH, EINE ZWEITE E-MAIL-ADRESSE FÜR DIE NUTZUNG VON ONLINEDIENSTEN ANZULEGEN. SO KÖNNEN SPAM-E-MAILS ZUMINDEST AUS DEM HAUPT-E-MAIL-POSTFACH FERNGEHALTEN WERDEN.

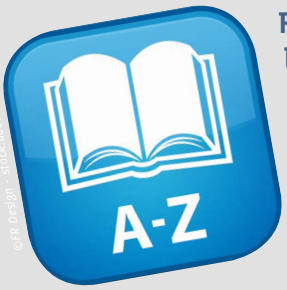




Dieser Artikel ist mit freundlicher Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik entstanden. Erfahren Sie jederzeit mehr unter: www.bsi.bund.de.

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.

TIPP



FACHJARGON: EIN CYBER-GLOSSAR BIETET WERTVOLLE HILFESTELLUNG

Als Laie ist es schwierig, Wörter und ihre Bedeutung immer im richtigen Kontext zu verwenden. Dies kann insbesondere bei Anfragen oder Gesprächen mit Experten zu Missverständnissen führen.

Daher kann ein Glossar hilfreich sein, um Fachausdrücke kurz und prägnant zu erläutern. Insbesondere in der Cyberwelt existieren viele Anglizismen, die „richtig“ übersetzt werden müssen, um sie zu verstehen und eine einheitliche Begriffsbildung herzustellen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat auf seiner Webseite ein deutschsprachiges Cyber-Glossar zur Verfügung gestellt. Von „A“ wie „Access Point“ über „F“ wie „Fail-Over“ und „R“ wie „Repeater“ bis „Z“ wie „Zwei-Faktor-Authentisierung“ werden verschiedene Begriffe aus dem Cyberumfeld in ihrer Bedeutung erläutert.

Erfahren Sie jetzt mehr unter: www.bsi.bund.de

BUCHEMPFEHLUNG

NOTFALL-/KRISENVORSORGE: DAS GROSSE BUCH DER ÜBERLEBENSTECHNIKEN

Dieses „Survival Standardwerk“ von Gerhard Buzek schafft ein Bewusstsein für verschiedene Problemlagen und Notsituationen und stellt detailliert Lösungen mit den unterschiedlichsten zur Verfügung stehenden Ressourcen dar.

Verirren in der Natur, Flucht mit dem Fahrzeug, Geiselnahme, Brand, Verschüttung, unsichere Gegenden oder Flugzeugabsturz – weil Notlage nicht gleich Notlage ist, werden drei Szenarien betrachtet und die jeweiligen Risiken sowie der Umgang damit skizziert.

- Überleben in Extremsituationen
- Überleben in der Natur
- Überleben in der Zivilisation

Vor allem abseits der Zivilisation lauern Gefahren, derer sich die wenigsten bewusst sind. So manche Wanderung endete schon in der Wildnis. Daher ist die Kenntnis lebenswichtiger Techniken und Fertigkeiten essenziell, auch wenn man kein Superheld ist.

Mehr zum Thema unter www.youtube.com/SIUSconsulting

„GEEIGNET FÜR ALLE, DIE SICH BESSER VORBEREITEN WOLLEN UND SEHR BELIEBT IM OUTDOOR-BEREICH!

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
Alle bei SICHERHEIT. Das Fachmagazin. erschienenen Artikel sind urheberrechtlich geschützt. Alle Rechte sind vorbehalten. Reproduktionen gleich welcher Art sind nur mit schriftlicher Zustimmung erlaubt.
Alle Angaben in SICHERHEIT. Das Fachmagazin. wurden mit äußerster Sorgfalt recherchiert und geprüft. Sie unterliegen jedoch der steten Veränderung. Eine Gewähr kann deshalb nicht übernommen werden.

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.