DATENSCHUTZAKTUELL
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH
OKT 2026
Schweiz

SCHUTZ VOR CYBERCRIME: STÄRKEN SIE DIE ERSTE VERTEIDIGUNGSLINIE

AWARENESS
Zukunftstag am 12.11.2026: Geben Sie wichtige Tipps 1–2

DATENSCHUTZ-ORGANISATION
USB-Sticks: Beugen Sie mit 10 Regeln Datenpannen vor 6

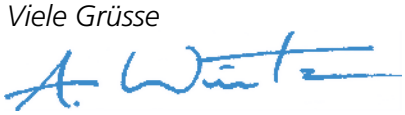
Kein Datenschutz ist auch keine Lösung

Liebe Leserin, lieber Leser,

Datenschutz ist schon immer ein heiss diskutiertes und hoch umstrittenes Thema – vielleicht auch in Ihrem Unternehmen. Und auch in der Politik gibt es Stimmen, die als Massnahme zum Bürokratieabbau den Datenschutz zurückfahren wollen.

Natürlich liesse sich manche gesetzliche Anforderung erheblich vereinfachen. Das werden Sie als Datenschutzberater sicher auch so sehen. Wichtig ist jedoch, dass Sie die Grundidee verteidigen. Nicht jeder soll mit Personendaten machen dürfen, was er will. Schliesslich hat jeder das Recht auf Schutz seiner Daten. Und dieses Recht muss erhalten bleiben.

Viele Grüsse



Andreas Würtz,
Rechtsanwalt und Chefredaktor

Ihr Experte für Datenschutz
Andreas Würtz verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz pragmatisch umsetzen lässt.

Inhalt

Awareness
Nationaler Zukunftstag am 12.11.2026: Geben Sie wichtige Tipps Seiten 1–2

Datenschutzorganisation
Schauen Sie bei der Datenverfügbarkeit genauer hin Seite 3

Awareness
Schutz vor Cybercrime: Stärken Sie die erste Verteidigungslinie Seiten 4–5

Datenschutzorganisation
USB-Sticks: Beugen Sie mit 10 Regeln Datenpannen vor Seite 6

Fragen an die Redaktion
Ist eine etwas zu lange Videoaufzeichnung vertretbar? Seite 7

Müssen wir vertauschte Lieferscheine als Panne melden? Seite 7

Urteil aus dem Ausland
Werbevideos nur ohne erkennbare Personen erlaubt Seite 8

Zu Ihrem Onlinebereich:
https://kurzlink.ch/privacy

Live-Talk:
https://kurzlink.ch/live-talk

Expertenhotline:
https://kurzlink.ch/kontakt-wuertz

Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Michael Schrader, Bonn

V.i.S.d.P.: Michael Jodda (Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredaktor:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | Tomasz Zajda; Seite 1: Adobe Stock | grafikplusfoto

Erscheinungsweise: 17-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Helfen Sie beim Suchen junger Mitarbeiter – datenschutzgerecht.

Zukunftstag am 12.11.2026: Geben Sie wichtige Tipps

Geeignete junge Mitarbeiter oder Auszubildende zu finden wird für viele Unternehmen zunehmend zum Problem. Daher setzt vielleicht auch Ihr Unternehmen auf den 12.11.2026. An diesem Tag findet in der Schweiz wieder der „Nationale Zukunftstag" statt. Das ist nicht nur eine gute Gelegenheit, um junge Menschen für bestimmte Berufe zu begeistern. Ihr Unternehmen kann sich als attraktiver Arbeitgeber in Szene setzen.

Sorgen Sie für Sensibilität bei den Kollegen

Natürlich ist es wichtig, den Zukunftstag für Mädchen und Jungen interessant und abwechslungsreich zu gestalten. Schliesslich gibt es auch für Ihr Unternehmen keine zweite Chance für einen ersten guten Eindruck bei den Teilnehmern. Allerdings werden in der einen oder anderen Form wohl auch Personendaten eine Rolle spielen. Daher sind auch Sie als Datenschutzberater gefragt. Schliesslich können Sie nicht einfach die Augen verschliessen und den Datenschutz sein lassen. Denn Patzer und Pannen im Datenschutz sind auch an einem Aktionstag ganz schlecht.

Nutzen Sie die nächsten Wochen

Bis zum Zukunftstag ist es noch einige Wochen hin. Das bedeutet aber nicht, dass Sie die Hände in den Schoss legen sollten. Werden Sie frühzeitig aktiv. Sorgen Sie für erhöhte Sensibilität bei Organisatoren oder bei den am Aktionstag teilnehmenden Kollegen. Dazu haben Sie beispielsweise folgende Möglichkeiten:

- **Kommen Sie mit den zuständigen Kollegen ins Gespräch**
  Laden Sie zu einem kurzen Gespräch ein, gerade mit den Organisatoren oder der Ausbildungsleitung. Hier können Sie schnell in Erfahrung bringen, was angedacht ist.
- **Klären Sie Handlungs- und Unterstützungsbedarf**
  Identifizieren Sie die Situationen und Fälle, in denen auch der Schutz von (persönlichen) Informationen von Bedeutung ist.
- **Loten Sie die Möglichkeiten für Ihr Thema aus**
  Auch das kann eine Idee sein: Werden am Aktionstag Berufe und Tätigkeiten vorgestellt, können Sie auch Ihren Job in den Fokus rücken. Diese Imagepflege wirkt nicht nur nach aussen. Auch im Unternehmen wird Ihr Beitrag mit Sicherheit wahrgenommen. Alternativ können Sie anbieten, dass Sie ein oder zwei Teilnehmern einen Einblick in Ihren Arbeitsalltag geben.
- **Informieren Sie und geben Sie Tipps**
  Um Pannen und Patzer zu vermeiden, können Sie den zuständigen Kollegen einige Tipps geben.

Grundlage für Ihren Entwurf kann das folgende Muster sein:

Muster: Tipps zum Nationalen Zukunftstag 2026

Liebe Kollegin, lieber Kollege,

am 12.11.2026 findet wieder der Nationale Zukunftstag statt, der berufliche Informationstag für Mädchen bzw. für Jungen. Das Ziel dieses Tages ist schnell erklärt: Unter dem Motto Seitenwechsel soll bei Mädchen oder Jungen Interesse für Berufe geweckt werden, die häufiger vom anderen Geschlecht ergriffen werden. Auch unser Unternehmen will dazu beitragen, dass klassische Rollenbilder in der Berufswelt aufgebrochen werden. Zudem ist wichtig: Unser Unternehmen braucht dringend Nachwuchs. Der Nationale Zukunftstag 2026 ist eine gute Gelegenheit für unser Unternehmen, sich als attraktiver Arbeitgeber bzw. Ausbildungsbetrieb zu empfehlen. Diese Chance sollten wir unbedingt nutzen.

Bestimmt wollen Sie den Zukunftstag interessant und kurzweilig für die Teilnehmenden gestalten. Damit der Tag ein voller Erfolg wird, sollten Sie sich die folgenden Tipps zu Herzen nehmen:

Beachten Sie alles, was sonst auch gilt

Auch wenn bei solchen Aktionstagen manches anders läuft als üblich, dürfen Sie gerade beim Thema Datenschutz nicht nachlässig werden. Denn: Geht etwas im Zusammenhang mit Personendaten schief, taugt ein Aktionstag nicht als Rechtfertigung. Daher: Orientieren Sie sich beim Umgang mit Personendaten an den Regeln und Massstäben, die auch an allen anderen Tagen in unserem Unternehmen gelten. Kommen Teilnehmer mit Personendaten in Kontakt, etwa weil diese einen Mitarbeiter bei der Arbeit begleiten, sollten Sie daran denken, die Teilnehmer auf deren Pflicht zur Wahrung der Vertraulichkeit aufmerksam zu machen.

Gestalten Sie die Anmeldung datenschutzfreundlich

Wahrscheinlich gibt es eine Anmeldung für den Aktionstag bzw. Interessierte müssen sich vorab mit den Fachabteilungen in Verbindung setzen. Hier ist wichtig, dass Sie eine Anmeldung oder auch das Einfordern von Informationen so gestalten, dass der Datenschutz passt. Sind Sie sich hier unsicher, sprechen Sie mit den Organisatoren des Aktionstags, der Personalabteilung oder dem Datenschutzberater.

Setzen Sie auf das Minimalprinzip

Damit fahren Sie immer gut. Klären Sie für sich immer, ob dies oder jenes wirklich erforderlich ist. Das gilt für das Erfassen von Informationen bei Teilnehmern. Aber auch hinsichtlich Informationen, die Teilnehmer zur Kenntnis nehmen können, sollten Sie immer hinterfragen: Ist die Kenntnis persönlicher Informationen, etwa von Kunden, wirklich nötig?

Stimmen Sie Bearbeitungen von Personendaten rechtzeitig ab

Wollen Sie Personendaten von Teilnehmern bearbeiten, muss so einiges im Datenschutz beachtet werden. Auch bei unscheinbaren Vorhaben, etwa einem Gewinnspiel, kann manch wichtiger Aspekt leicht übersehen werden. Klären Sie also frühzeitig mit dem Datenschutzberater, worauf es in Ihrem Fall ankommt und was zu tun ist.

Achten Sie bei Präsentationen und Vorträgen auf den Datenschutz

Vermeiden Sie Personenbezug, wenn dieser nicht erforderlich ist, etwa wenn Sie Beispiele bringen. Natürlich können Sie auf Ansprechpartner oder Kollegen im Unternehmen verweisen, wenn das für das Verständnis erforderlich ist. Bauen Sie Screenshots ein oder schildern Sie Fälle, achten Sie auf ausreichende Anonymisierung. Dann gibt es keine Probleme mit dem Persönlichkeitsrecht oder dem Datenschutz.

Bestimmte Bereiche sind tabu

Schauen Sie vorab, inwieweit Teilnehmer Zutritt brauchen bzw. diese in Bereiche gelangen könnten, die tabu sind. Das kann beispielsweise unsere Entwicklungsabteilung sein. Klären Sie ggf. mit den zuständigen Kollegen, inwieweit Besucherausweise oder eingeschränkte Zutrittsrechte vergeben werden müssen.

Setzen Sie Clean Desk und Clear Screen konsequent um

Auch an Ihrem Arbeitsplatz oder in Ihrer näheren Umgebung sollten Sie den Datenschutz ernst nehmen. Sperren Sie den Computer bei Abwesenheit, lassen Sie Sensibles oder Schützenswertes nicht unbeaufsichtigt herumliegen. Prüfen Sie kritisch, inwieweit es etwas gibt, das nicht für die Augen oder Ohren eines Teilnehmers bestimmt ist.

Geben Sie Spielregeln zur Smartphonenutzung vor

Gerade bei jungen Menschen wird das Erlebte gerne im Bild oder Video festgehalten und irgendwo „gepostet". Das kann ein Problem für den Datenschutz oder die Geschäftsgeheimnisse unseres Unternehmens sein. Legen Sie daher Spielregeln für die Nutzung des Smartphones durch die Teilnehmer fest. Im Bedarfsfall können Sie auch fordern, dass die Geräte ausgeschaltet werden oder am Empfang hinterlegt werden.

Gestalten Sie Foto- und Videoaufnahmen rechtssicher

Wollen Sie selbst Fotos oder Videos machen, etwa um diese für einen Bericht auf der Webseite oder in einem sozialen Netzwerk zu veröffentlichen, heisst es Augen auf. Meist ist hier die Einwilligung des Abgebildeten erforderlich. Bei Minderjährigen gibt es hier jedoch besondere Anforderungen. Klären Sie also im Vorfeld alles rechtlich Relevante, damit eine Veröffentlichung nicht zum Problem wird.

Instruieren Sie betreuende und begleitende Mitarbeiter

Auch das kann passieren: Sie wollen sich um die Teilnehmer selbst kümmern. Am Aktionstag sind sie jedoch krank oder müssen einen wichtigen Termin wahrnehmen. Informieren und instruieren Sie frühzeitig Kollegen, die für Sie einspringen. Damit leisten Sie einen wichtigen Beitrag, dass dem Vertreter die Vertretung leichter fällt. Und manches kann dann erst gar nicht schiefgehen.

Löschen Sie nach der Veranstaltung alles nicht mehr Erforderliche

Unter Umständen bearbeiten Sie im Zusammenhang mit dem Aktionstag Personendaten. Ist der Tag vorbei, sollten Sie zeitnah prüfen, inwieweit relevante Informationen für den verfolgten Zweck noch erforderlich sind. Ist das nicht der Fall, sollten Sie nicht mehr benötigte Informationen löschen. Bei Fragen: Melden Sie sich einfach. Eventuell kommen bei der Vorbereitung des oder am Aktionstag Fragen mit Datenschutzbezug auf. Warten Sie dann nicht lange ab und treffen Sie keine Entscheidungen aus dem Bauch heraus. Kontaktieren Sie mich, Ihren Datenschutzberater. Ich wünsche Ihnen viel Erfolg und gutes Gelingen

Ihr Eddi Kett

Schauen Sie bei der Datenverfügbarkeit genauer hin

Daten sind der Treibstoff für den Motor Ihres Unternehmens. Doch wenn Daten nicht mehr verfügbar sind, weil sie etwa verloren gegangen sind, passiert das Gleiche wie bei einem Verbrennungsmotor: Erst kommt es zum Stottern und dann bleibt er stehen. Umso wichtiger ist für Ihr Unternehmen, dass es dafür sorgt, dass (Personen-) Daten stets verfügbar sind.

Verfügbarkeit dient der Sicherheit der Bearbeitung

Schauen Sie in Art. 8 Abs. 1 Bundesgesetz über den Datenschutz (DSG) und Art. 5 Buchst. h DSG finden Sie dort die Sicherheitsziele. Eines ist, dass Ihr Unternehmen dafür sorgen muss, dass Personendaten nicht verlorengehen dürfen. Typisch sind hier ausreichend dimensionierte Technik, Redundanzsysteme und Datenspiegelungen in RAID-Systemen. Doch gerade kleinere Unternehmen werden vor allem auf Back-ups setzen. Wie es um die Datenverfügbarkeit in Ihrem Unternehmen steht, können Sie in einem Beratungsgespräch herausfinden. Setzen Sie auf diese Checkliste:

Checkliste: Wichtige Aspekte bei Datenverfügbarkeit und Back-up

Aspekt	Darauf kommt es an	In Ordnung?
Inwieweit sind Personendaten Daten betroffen?	› Geht es auch um Personendaten, greifen insbesondere die Vorgaben des DSG. › Besonders relevant sind die Festlegungen des Art. 8 i.V.m. Art. 5 Buchst. h DSG. Zu den Schutzzielen zählt es auch sicherzustellen, dass Personendaten nicht unbeabsichtigt oder widerrechtlichverlorengehen.	○ Ja ○ Nein
Gibt es einen Überblick bzw. eine Bewertung dazu, welche Daten wie verfügbar sein müssen?	› Eine solche Bewertung ist unerlässlich. Schliesslich ist sie Ausgangspunkt für alles Weitere, etwa zu Datenspiegelungen und Back-ups, zu Wiederherstellungsprozessen oder tolerablen Ausfall- bzw. Wiederherstellungszeiten. › Nicht alle Daten sind gleich sicherungswürdig. Klar ist jedoch: Je verfügbarer Daten sein müssen, desto mehr Aufwand muss bezüglich Redundanzsystemen oder Back-ups getrieben werden.	○ Ja ○ Nein
Welche Prozesse greifen, wenn Daten nicht verfügbar sind?	› Es sollte klare Vorgaben geben, wie etwa Notfallpläne, Prozessbeschreibungen und Checklisten. › Hinterfragen Sie, inwieweit das Funktionieren der Festlegungen getestet wurde. Nur wenn das passiert ist, ist wahrscheinlich, dass alles auch im Fall der Fälle klappt.	○ Ja ○ Nein
Gibt es eine Risikoanalyse?	› Insbesondere die Schutzmassnahmen nach Art. 8 Abs. 1 DSG müssen risikoangemessen sein. › Grundlegendes Vorgehen: Gefahren identifizieren, möglichen Schaden und Eintrittswahrscheinlichkeit abschätzen, Risiken bewerten und mit geeigneten Massnahmen behandeln.	○ Ja ○ Nein
Inwieweit gibt es Datenspiegelungen und Redundanzsysteme?	› Gerade wenn es um Hochverfügbarkeit geht, können Datenwiederherstellungen aus Back-ups zu lange dauern. Unter Umständen sind Datenspiegelungen oder Redundanzsysteme die bessere Wahl. › Klären Sie auch den Aspekt der Verfügbarkeit bzw. der Möglichkeit zur Weiterarbeit an einem anderen Standort. Brennt der Hauptstandort ab, ist hier auch eine Weiterarbeit unmöglich.	○ Ja ○ Nein
Welche Daten werden auf welche Weise gesichert?	› Lassen Sie sich das Vorgehen erläutern. So muss klar werden, welche Daten in welchen Abständen, wie und auf welchen Medien gesichert werden. › Abgedeckt sein sollten auch Betriebssysteme, Software, Datenbanken und Server. › Achten Sie darauf, dass das Ihnen Erläuterte auch zu den Festlegungen in einem Sicherheitskonzept oder Betriebshandbuch passt. › Prüfen Sie zudem: Entsprechen das Vorgehen und die eingesetzten Methoden dem Stand der Technik?	○ Ja ○ Nein
Wo werden die gesicherten Daten aufbewahrt?	› Besprechen Sie die physische Aufbewahrung von Sicherungen. In einem Gebäude sollte das in unterschiedlichen Brandabschnitten erfolgen. › Bedenken Sie aber auch andere Gefahren, wie Naturereignisse oder einen Wasserschaden. › Haben Sie zudem ein Auge darauf, dass unbefugter Zugriff ausgeschlossen sein muss.	○ Ja ○ Nein
Werden bei automatisierten Sicherungen Protokolle ausgewertet?	› Automatische Sicherungen bringen den Vorteil, dass nicht vergessen wird, sie durchzuführen. Allerdings kann es dennoch zu Fehlern oder Abbrüchen kommen. › Bringen Sie in Erfahrung, wer wann welche Checks durchführt.	○ Ja ○ Nein
Sind Datensicherungen vor Schadprogrammen geschützt?	› Die beste Sicherung bringt nichts, wenn Schadprogramme auch dort aktiv werden können. › Klären Sie, wie das verhindert wird, etwa durch eine Trennung der Datenverbindungen.	○ Ja ○ Nein
Sind Dienstleister datenschutzkonform eingebunden?	› Setzt Ihr Unternehmen auf Services von anderen Unternehmen, etwa Cloud-Angebote, muss ggf. einiges zum Datenschutz bedacht werden. › Häufig liegt eine Auftragsbearbeitung vor, die zu regeln ist. Ist der Anbieter in einem Drittstaat ansässig, kommen die Anforderungen aus Art. 16 DSG hinzu.	○ Ja ○ Nein
Wie geht man mit Anfrage von betroffenen Personen um?	› Legen Sie hier vor allem den Fokus auf das Recht auf Löschung. Grundsätzlich greift das auch bei Datensicherungen. › Lassen Sie sich das Vorgehen erklären. Wird in einer Sicherung nicht gelöscht, muss das zumindest bei der Datenwiederherstellung erfolgen.	○ Ja ○ Nein

Schutz vor Cybercrime: Stärken Sie die erste Verteidigungslinie

Cyberkriminelle haben es auf Ihr Unternehmen abgesehen. Und weil niemand ausschliessen kann, dass dem so ist, muss vorgesorgt werden. Schliesslich sollen sich Cyberkriminelle am besten an Ihrem Unternehmen die Zähne ausbeissen. Damit das gelingt, kommt es entscheidend auf die Beschäftigten an.

Sensibilisieren Sie die Mitarbeiter

Ihr Unternehmen kann noch so viel in technische Schutzmassnahmen investieren. Alles ist für die Katz, wenn ein Beschäftigter unbedacht einen E-Mail-Anhang mit Schadcode öffnet. Um dem vorzubeugen, ist entscheidend, dass die Beschäftigten wissen, worauf es ankommt. Um das nötige Wissen zu vermitteln und richtiges Handeln zu fördern, können Sie z. B. eine Awareness-E-Mail verschicken.

Muster: Awareness-E-Mail zu den Maschen von Cyberkriminellen

Betreff: So haben Cyberkriminelle bei Ihnen keine Chance

Liebe Kolleginnen und Kollegen.

bestimmt ist auch Ihnen bewusst: Cyberkriminalität ist schon lange keine Randerscheinung mehr. Inzwischen ist Internetkriminalität mitten im Leben angekommen. Und die Machenschaften von Cyberkriminellen stellen für Sie wie auch für unser Unternehmen ein grosses Risiko dar, und zwar nicht nur wirtschaftlich, sondern auch was den Datenschutz angeht. Geraten schützenswerte Informationen, etwa Personendaten oder Geschäftsgeheimnisse, in die Hände von Cyberkriminellen, ist gewaltiger Ärger vorprogrammiert. Seien Sie sich sicher: Cyberkriminelle haben es nicht nur auf grosse Konzerne abgesehen. Auch unser Unternehmen steht als mittelständisches Unternehmen im Fokus. Denn Cyberkriminelle hoffen, dass bei kleineren Unternehmen die Schutzmassnahmen weniger hoch und die Sensibilität der Beschäftigten eher gering sind.

Es fängt meist harmlos an

Die meisten erfolgreichen Angriffe von Cyberkriminellen beginnen mit einer E-Mail, einem Anruf, einer Messenger-Nachricht oder einer SMS. Hinzu kommt, dass der Empfänger nicht genau hinschaut, nicht nachdenkt oder im falschen Moment unaufmerksam ist. Schnell kann es dann passiert sein. Da bringen auch die besten technischen Lösungen wie Firewall oder Virenscanner kaum noch etwas, wenn den Cyberkriminellen Tür und Tor geöffnet wird.

Cyberkriminelle sind keine Anfänger

E-Mails mit vielen Schreibfehlern, die leicht als Phishing zu erkennen waren, kommen nun weniger oft vor. Inzwischen gehen Cyberkriminelle hochprofessionell vor. Sie nutzen KI, etwa um perfekte E-Mail-Fälschungen herzustellen. Deepfakes werden erzeugt, um die Stimme des Chefs oder Videos für die Onlinekonferenz zu klonen. Zudem recherchieren sie Informationen in sozialen Netzwerken oder sammeln diese auf Webseiten.

Sie sind die wichtigste Verteidigungslinie

Egal, wo Sie arbeiten und auf welcher Hierarchiestufe Sie tätig sind: Jeder kann ins Fadenkreuz der Cyberkriminellen geraten. Dabei darf es nicht zu einem unbedachten Klick, einer achtlosen Weitergabe von Anmeldeinformationen oder einer übereilten Überweisung kommen. Damit Sie Cyberkriminellen nicht auf den Leim gehen, ist es wichtig, dass Sie insbesondere die folgenden fünf Maschen kennen.

Masche Nr. 1: Phishing per E-Mail

Was passiert? Bei Ihnen landet eine E-Mail im Postfach, die scheinbar von einem vertrauenswürdigen und ggf. auch bekannten Absender kommt. Das kann etwa eine Bank, eine Behörde, ein Paketdienst oder eine Servicenachricht von einem sozialen Netzwerk sein. Auch kann die Mail scheinbar von einem Kollegen, Vorgesetzten oder Geschäftspartner stammen. Ziel des Ganzen: Geschickt will man Sie dazu bringen, dass Sie schnell handeln, nicht nachdenken und etwa auf einen Link klicken. Der führt Sie auf eine täuschend echt aussehende Webseite. Dort sollen Sie Anmeldedaten eingeben oder eine Datei öffnen. Die eingegebenen Daten werden dann missbraucht. Die Datei enthält Schadsoftware.

Woran erkennen Sie es? Typischerweise gibt es noch eine unpersönliche oder unpassende Anrede. Zudem wird Handlungsdruck erzeugt, etwa mit einer „letzten Mahnung", einer „Kontosperrung" oder einem „Strafverfahren" gedroht. Manchmal gibt es noch Rechtschreibfehler, auch wenn diese in Phishing-E-Mails dank KI weniger werden. Enthalten sind oft Links zu einer Webseite, bei der erst auf den zweiten Blick auffällt, dass sie nicht das „Original" ist. Beigefügt sind gerne auch Anhänge, z. B. Rechnungen oder Angebote etwa als .docx-, xlsx- oder Zip-Datei.

Masche Nr. 2: Voice Phishing (Vishing)

Was passiert? Sie erhalten einen Anruf. Am anderen Ende der Leitung ist eine freundliche Person. In perfektem Deutsch gibt sie sich als Mitarbeiter der IT-Hotline oder des Supports unseres Unternehmens oder von Microsoft & Co. aus. Manchmal gibt man auch vor, Mitarbeiter einer

Behörde, einer Bank oder eines Geschäftspartners zu sein. Der Anrufer schildert ein Problem, etwa einen Sicherheitsvorfall, ein technisches Problem oder eine verdächtige Zahlung. Und genau Sie – nur Sie – können dabei helfen, das Problem zu lösen. Sie sollen etwa eine Wartungssitzung mit Zugriff auf Ihren Computer erlauben, Passwörter preisgeben oder von einer Webseite ein Update herunterladen. Letzteres enthält natürlich Schadcode. Woran erkennen Sie es? Werden Sie bei unangekündigten Anrufen von angeblichen IT-Spezialisten, Support-Mitarbeitern oder Behördenvertretern immer stutzig. Diese rufen in der Regel nie unaufgefordert an. Druck wird aufgebaut und Sie sollen sofort handeln. Zudem fordert man Sie auf, eine Webseite aufzurufen, einen Zugriff zu erlauben oder einen zugesendeten Anhang zu öffnen. Alternativ sollen Sie Anmeldeinformationen mitteilen. Auch werden mit KI geklonte vertraute Stimmen genutzt, um Sie in die Falle zu locken.

Masche Nr. 3: Der Chef-Trick (CEO-Fraud)

Was passiert? Sie erhalten vom Chef eine E-Mail oder einen Anruf. Doch das ist schon der Trick. Das stimmt natürlich nicht. Man gaukelt Ihnen nur vor, dass der Geschäftsführer Sie, ja gerade Sie, ins Vertrauen zieht. Es geht regelmässig um eine ganz eilige und streng vertrauliche Aktion, etwa einen noch geheimen Unternehmenszukauf. Nur Sie können dafür sorgen, dass nichts schiefgeht. Dazu sollen Sie ganz dringend eine Überweisung tätigen oder sensible Informationen weitergeben. Meist sollen Sie dabei auf bestehende Anweisungen oder Prozesse keine Rücksicht nehmen. Doch alles ist erstunken und erlogen.

Woran erkennen Sie es? Die Sache ist immer höchst eilig und absolut geheim. Nur Sie dürfen von der Sache wissen, auch wenn das gar nicht zu Ihrer Tätigkeit passt oder in Ihrer Entscheidungskompetenz liegt. Zudem wird Druck aufgebaut. Machen Sie nicht das Geforderte, soll grosser Schaden entstehen. Vorgeschriebene Prozesse oder etablierte Checks (z. B. Vier-Augen-Prinzip") sollen Sie ignorieren. E-Mail-Adressen weichen kaum erkennbar von der echten Adresse ab. Mit Deepfakes erzeugte Stimmen klingen zwar vertraut, aber irgendwie passt etwas nicht.

Masche Nr. 4: Schocknachrichten

Was passiert? Sie erhalten einen Anruf oder eine Sprachnachricht, etwa per Messenger. Der Inhalt erscheint dramatisch. Ein Kollege ist verunglückt oder wurde wegen einer erheblichen Straftat ins Gefängnis gesteckt. Oder es ist von einer Abmahnung, einem Ermittlungsverfahren bzw. einem drohenden Bussgeldbescheid gegen das Unternehmen die Rede. Nur mit schnellem Handeln kann das Schlimme noch abgewendet werden. Das Ziel: Sie sollen in dieser Schrecksituation unbedacht handeln und etwa Geld überweisen, sensible Informationen preisgeben oder einen Link anklicken.

Woran erkennen Sie es? Die Botschaft soll Sie schockieren. Dazu setzt man auf Angst, Sorge Pflichtgefühl oder Schuldgefühle. Es wird Druck aufgebaut und Sie müssen schnell handeln, um Schaden abzuwenden. Nur Sie sind in der Lage, das Unheil abzuwenden. Sie werden aufgefordert, die Sache geheim zu halten. Meist sollen Zahlungen in einer Form erfolgen, die unüblich ist, etwa als Auslandsüberweisung oder in Kryptowährung.

Masche Nr. 5: „Der Enkeltrick" im Unternehmen

Was passiert? Ältere Menschen werden gerne über den Tisch gezogen, weil sich der angeblich in Not geratene Enkel meldet und dringend Hilfe braucht. Aus Verbundenheit, Pflichtgefühl und Hilfsbereitschaft werden dann oft Geldbeträge an den „falschen Enkel" gegeben, eben die Kriminellen. Das funktioniert auch im Unternehmen. Es meldet sich etwa ein Kollege, der dringend Ihre Hilfe braucht. Sie sollen ihm bestimmte Dateien zur Verfügung stellen. Allerdings kann das auch am Eingang zum Gebäude passieren, wenn angeblich die Zutrittskarte vergessen wurde.

Woran erkennen Sie es? An sich wirken die Anfragen harmlos, das Ziel ist jedoch meist, dass Sie Daten herausgeben oder den Zugang gestatten. Die Person ist Ihnen eigentlich unbekannt. Gerne kommt es auch zu „Namedropping", sprich, man bezieht sich auf andere Stellen oder bekannte Personen wie z. B. „Herr Meier, unser Geschäftsführer, schickt mich". Um Vertrauen zu schaffen, kommt man ins Plaudern oder es regnet Komplimente.

So verhalten Sie sich richtig

Damit all diese Maschen ins Leere gehen, ist entscheidend, dass Sie sich richtig verhalten. Machen Sie Folgendes:

- **Bevor Sie handeln: zweimal nachdenken.** Zeitdruck ist ein wichtiger Erfolgsfaktor für Cyberkriminelle. Nehmen Sie sich immer die Zeit, um die nächsten Schritte gut zu überlegen.
- **Machen Sie nicht das, was in einer verdächtigen Situation gefordert wird.** Klicken Sie nicht auf Links, geben Sie nichts Sensibles preis und öffnen Sie keine Anhänge.
- **Weichen Sie nie von geltenden Regeln und Prozessen ab.** Gerade das Vier-Augen-Prinzip, Freigabeprozesse und Sicherheitsregeln gelten immer und ausnahmslos.
- **Nehmen Sie Ihr Bauchgefühl ernst.** Kommt Ihnen etwas seltsam vor, dann trifft das in den meisten Fällen tatsächlich zu.
- **Halten Sie im Zweifel immer Rücksprache.** Fragen Sie Kollegen, Vorgesetzte oder andere relevante Stellen im Unternehmen. Auch können Sie den Datenschutzberaterten ansprechen.
- **Bestätigen Sie die Echtheit über bekannte Wege:** Nutzen Sie nie Links oder Kontaktinformationen aus der E-Mail. Setzen Sie auf unser Firmenadressbuch oder offizielle Quellen.

Und wenn trotzdem etwas schiefgeht?

Fehler können jedem passieren. Doch auch dann sollten Sie das Richtige tun: Warten Sie nicht lange und melden Sie die Sache sofort der IT-Abteilung bzw. dem Datenschutzberater. Wird nämlich schnell gehandelt, kann Schlimmeres verhindern helfen. Melden Sie sich gerne auch bei erfolglosen Angriffsversuchen. Bleiben Sie auf der Hut!

Wir zählen auf Sie! Ihr Datenschutzberater

Heinz Elmann

USB-Sticks: Beugen Sie mit 10 Regeln Datenpannen vor

Meist sind sie das Mittel der Wahl, wenn Daten transportiert oder von einer Person zu einer anderen weitergegeben werden sollen. Die Rede ist von mobilen Datenträgern, wie z. B. USB-Sticks, Speicherkarten oder externen Festplatten. Was so praktisch ist, birgt aber auch so manches Datenschutzrisiko. Schärfen Sie also die Sinne der Mitarbeiter.

So gut wie alle Mitarbeiter wollen im Job nichts falsch machen. Denn Fehler sorgen regelmässig für Stress und Ärger. Und den will sich jeder vom Hals halten. Doch USB-Sticks & Co. bringen Risiken mit sich, die hier und da aus Unkenntnis oder im Eifer des Gefechts ausser Acht gelassen werden. Dem können Sie vorbeugen. Machen Sie den Mitarbeitern den richtigen Umgang mit Datenträgern leichter. Sorgen Sie dafür, dass bei der Ausgabe des Datenträgers durch die IT-Abteilung auch ein Merkblatt ausgehändigt wird.

Merkblatt: 10 goldene Sicherheitsregelung für USB-Sticks & Co.

Liebe Kollegin, lieber Kollege,

Sie haben heute von der IT-Abteilung einen externen Datenträger erhalten, beispielsweise einen USB-Stick oder eine Festplatte. So praktisch diese kleinen Datenträger sind: Umso grösser sind die Risiken, etwa durch Verlust oder Diebstahl des Datenträgers. Auch können sie Schadprogramme einschleppen. Damit nichts schiefgeht, müssen Sie die folgenden zehn goldenen Regeln beachten:

1. Verwenden Sie nur den vom Unternehmen bereitgestellten Datenträger

Für dienstliche Zwecke verwenden Sie bitte nur den von der IT-Abteilung erhaltenen Datenträger. Nutzen Sie ihn nicht für Privates, etwa um Dateien zu übertragen. Das kann Risiken bergen, etwa für das Einschleppen von Viren oder Schadprogrammen über Privatgeräte.

2. Ohne Wenn und Aber: Setzen Sie auf Verschlüsselung

Verschlüsselung ist beim Transport von Daten eine zwingende Massnahme. Ist der Datenträger nicht hardwareverschlüsselt, nutzen Sie etwa die bordeigene Verschlüsselung BitLocker von Microsoft Windows. Einzelne Dateien können Sie mit einem starken Passwort vor unbefugtem Zugriff schützen. Für mehrere Dateien können Sie auch eine verschlüsselte Zip-Datei erstellen.

3. Achten Sie auf ein starkes Passwort

Dieses sollte mindestens zwölf Zeichen umfassen und aus Gross-/Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Nutzen Sie ein individuelles Passwort, das Sie nicht anderswo verwenden. Halten Sie das Passwort nicht auf einem Zettel fest, denn auch den können Sie verlieren oder er kann mit dem Datenträger geklaut werden. Besser ist ein Passwortmanager.

4. Besonders Schützenswertes müssen Sie mehr schützen

Müssen Sie besonders sensible oder schützenswerte Daten transportieren, setzen Sie am besten auf mehrere Schutzmassnahmen. Lassen Sie sich von der IT-Abteilung einen hardwareverschlüsselten Datenträger geben. Verschlüsseln Sie zusätzlich die darauf befindlichen Daten. Vergeben Sie hier unterschiedliche Passwörter.

5. Nutzen Sie den Datenträger nicht als Dateiablage

Ein solcher Datenträger ist nur für den Transport bzw. den Austausch von Dateien gedacht und das eben nur temporär. Dateien legen Sie dort ab, wo sie hingehören. Das sind die zentral gemanagten Dateiablagen Ihrer Abteilung.

6. Löschen Sie den Datenträger regelmässig, und zwar sicher

Räumen Sie den Datenträger nach der Nutzung auf. Löschen Sie beispielsweise alte Angebote. Achten Sie beim Löschen darauf, dass die Daten nicht nur im Papierkorb landen. „Schreddern" Sie die Daten digital. Die entsprechende Funktion finden Sie über das Kontextmenü im Dateiexplorer. Ein Rechtsklick auf die Datei genügt.

7. Bewahren Sie den Datenträger immer sicher auf

Tragen Sie den Datenträger nach Möglichkeit immer bei sich. Lassen Sie ihn nicht offen herumliegen. Schliesslich gilt: Gelegenheit macht Diebe. Auch im Hotel sollten Sie allen „Gelegenheiten" vorbeugen. Schliessen Sie den Datenträger sicher weg, etwa im Tresor.

8. Geben Sie den Datenträger nicht an Dritte weiter

Am besten ist, wenn Sie den Datenträger nie aus der Hand geben bzw. aus den Augen lassen. Auch „nette Menschen" können Böses im Schilde führen. Für das Kopieren unsichtbarer Schadprogramme reichen wenige Sekunden aus.

9. Prüfen Sie Erhaltenes auf Herz und Nieren

Nutzen Sie den Datenträger, um von anderen Personen Daten zu übertragen, sollten Sie direkt beim Anstecken des Datenträgers den Virenscanner für einen Check der Dateien nutzen. Das geht ruckzuck und Sie reduzieren das Schadensrisiko erheblich.

10. Pannen & Co. müssen Sie unbedingt melden

Haben Sie den Datenträger verloren oder wurde er gestohlen, gilt: Melden Sie das sofort bei der IT-Abteilung und beim Datenschutzberater. Hier müssen schnell Massnahmen eingeleitet werden, um mögliche Schäden abzuwenden.

Ist eine etwas zu lange Videoaufzeichnung vertretbar?

FRAGE: Ich betreue ein kleines Unternehmen. Weil es schon Diebstähle im Ladengeschäft gab, kommt dort eine Videoüberwachung zum Einsatz. Die ist schon etwas betagt. Auf den Datenspeicher passen Bilddaten für ca. vier Tage. Ist der Speicher voll, werden die ältesten Aufnahmen überschrieben. Von dem EDÖB wird eine Aufzeichnungsdauer von 72 Stunden, sprich drei Tage, meist problemlos akzeptiert. Die alte Anlage speichert also eigentlich etwas zu lange. Ist das dennoch irgendwie vertretbar?

ANTWORT: Unter Umständen wird vom zuständigen EDÖB auch eine viertägige Speicherdauer akzeptiert bzw. toleriert. Will man hier auf der sicheren Seite sein, kann sich die Nachfrage beim EDÖB lohnen.

Grundsätzlich müssen diejenigen technischen und organisatorischen Massnahmen ergriffen werden, damit eine Bearbeitung im Einklang mit dem Bundesgesetz über den Datenschutz (Art. 7 Abs. 1 DSG). In Betracht zu ziehen sind solche Massnahmen, die entweder für eine kürzere Speicherdauer sorgen oder eine erhöhte Beeinträchtigung des Persönlichkeitsrechts auf andere Weise kompensieren. Denken Sie also beispielsweise an folgende Möglichkeiten:

- Eine Festplatte kann ggf. durch eine kleinere Festplatte ersetzt werden, sodass schlichtweg weniger gespeichert werden kann.
- Eventuell lassen sich in der genutzten Software Parameter so ändern, dass die Festplatte schneller voll ist, etwa weil Daten weniger komprimiert werden. Ggf. lässt sich die Speicherdauer auch generell reduzieren.
- Organisatorisch kommen strenge Zugriffsbeschränkungen in Betracht, sodass ein Zugriff auf die Daten nur bei Vorliegen bestimmter Voraussetzungen möglich ist. Zudem kann das Unternehmen auch ein manuelles Löschen in Erwägung ziehen. Letzteres muss jedoch auch tatsächlich passieren. Stellen Sie das sicher.

Müssen wir vertauschte Lieferscheine als Panne melden?

FRAGE: Wir haben nur Geschäftskunden. In der Logistik kam es kürzlich zu einer Panne. Es wurden in vier Pakete die falschen Lieferscheine gepackt. Auf diesen sind bei Lieferanweisungen auch Personendaten zu finden. Wir haben die Empfänger gebeten, die falsch erhaltenen Lieferscheine zu vernichten. Wir fragen uns noch: Müssen wir diese Panne nach Art. 24 Bundesgesetz über den Datenschutz (DSG) melden?

ANTWORT: Folgende Dinge sind im Zusammenhang mit der Meldung von Datenpannen stets entscheidend. Ihr Unternehmen muss

1. die Risiken bewerten, die sich aus der „Panne" für die betroffene Person ergeben. Die Panne muss zu einem hohen Risiko für die betroffenen Person führen. Sie müssen also das Risiko für die betroffene Person einschätzen. Berücksichtigen Sie dabei etwa drohende (finanzielle) Schäden, Rufschädigung oder der Verlust der Kontrolle.
2. die Risken bewerten, die sich aus der Panne für die Grundrechte der betroffenen Person ergeben. Es gibt Datenschutzverletzungen bei denen die Grundrechte anderer Menschen betroffen sind. Das könnte zum Beispiel der Fall sein, wenn Gesundheitsdaten offengelegt werden oder wenn beispielsweise genetische oder biometrische Daten entwendet worden sind.

Kommt Ihr Unternehmen zum Ergebnis, dass nach der Abwägung ein hohes Risiko für die betroffenen Personen besteht oder sie sogar in ihren Grundrechten verletzt sind, darf Ihr Unternehmen nicht zögern. In einem solchen Fall muss die Meldung so rasch als möglich erfolgen.

Risiken eher gering

Bei vernünftiger Betrachtung des Sachverhalts wird man in Ihrem Fall nicht von einem hohen Risiko ausgehen müssen.

Erstens ging es nur um eine kleine Zahl betroffener Personen. Zweitens waren die Daten eher unkritisch. Zudem sind keine Schäden aus der Kenntnisnahme der Daten zu erwarten. Insofern ist eine Meldung nicht erforderlich. Die engen Voraussetzungen des Art. 24 DSG liegen nicht vor, denn der EDÖB verlangt keine Meldung bei nur niedrigem Risiken.

Werbevideos nur ohne erkennbare Personen erlaubt

Viele Unternehmen setzen auf soziale Medien, und zwar auch für Werbung mithilfe von Videos. Sind darauf jedoch auch Unbeteiligte erkennbar, kann das gegen die Datenschutz-Grundverordnung (DSGVO) verstossen. Und dagegen kann die Datenschutzaufsicht zu Recht vorgehen, meint das Verwaltungsgericht (VG) Düsseldorf in Deutschland (Beschluss vom 5.3.2026, Az. 29 L 4014/25).

Das führte zum Streit vor Gericht

Ein Reiseveranstalter, der spätere Kläger, vermittelte Reisen, etwa auf Kreuzfahrtschiffen. Bei Facebook betrieb das Unternehmen eine Seite. Auf dieser wurden auch von Mitarbeitern erstellte Videos veröffentlicht, die deren Reiseeindrücke wiedergeben sollten. So war es auch bei einem Video, das den auch bei Influencern beliebten Aura-Skypool in Dubai zeigte. Im Video waren auch zahlreiche andere Personen zu sehen, teilweise nur in Badekleidung.

Betroffener reicht Beschwerde ein

Das auf der Facebook-Seite veröffentlichte Video blieb nicht unbemerkt. Ein Betroffener entdeckte sich im Video vom Skypool und beschwerte sich bei der Datenschutzaufsichtsbehörde, der späteren Beklagten. Die Behörde ging der Beschwerde nach. Sie forderte das Unternehmen auf, die Videos auf der Facebook-Seite zu prüfen und ggf. zu löschen. Das wollte das Unternehmen nicht.

Nachdem eine erste Anordnung der Aufsichtsbehörde gerichtlich aufgehoben wurde, erliess die Aufsichtsbehörde im Herbst 2025 eine neue Anordnung. Darin forderte die Behörde das Unternehmen erneut dazu auf, alle Videos auf der Facebook-Seite so zu verändern, dass eine Identifizierung der abgebildeten Personen nicht möglich ist. Das wäre nur dann nicht erforderlich, wenn die Einwilligungen der abgebildeten Personen vorlägen. Verbunden war die Anordnung unter anderem mit einer Zwangsgeldandrohung. Zudem wurde die sofortige Vollziehbarkeit angeordnet.

Behörde: Videos verstossen gegen DSGVO

Aus Sicht der Aufsichtsbehörde fehle es an einer Rechtsgrundlage, etwa der Einwilligung. Auch ein überwiegendes berechtigtes Interesse sei nicht gegeben. Genau das sah der Reiseveranstalter anders. Also klagte er gegen den Bescheid und forderte in einem weiteren Verfahren, dass die sofortige Vollziehung ausgesetzt wird. Aus seiner Sicht wäre der Bescheid rechtswidrig. Es gäbe in Sachen DSGVO nichts zu beanstanden. So überwiege sein Interesse an der Verarbeitung. Zudem gehe es nicht nur um Werbung. Die Veröffentlichung sei auch Ausdruck der Meinungsfreiheit. Ausserdem ginge es um eine Örtlichkeit, die bei Influencern beliebt wäre. Die abgebildeten Personen hätten also erwartet, dass dort Videos angefertigt und diese auch veröffentlicht würden.

So entschied das VG Düsseldorf

Das Gericht gab dem Reiseveranstalter nur zu einem geringen Teil recht. Es ordnete lediglich die aufschiebende Wirkung bezüglich des im Behördenbescheid angedrohten Zwangsgelds an. Bezüglich der Anordnung des Sofortvollzugs wegen der sonstigen Regelungen des Bescheids der Aufsichtsbehörde hatte das Gericht nichts zu beanstanden.

Aus Sicht des Gerichts gab es gegen die Anordnung des sofortigen Vollzugs keine formellen oder materiellen Bedenken. Die Aufsichtsbehörde durfte auch eine entsprechende Anordnung treffen. Schliesslich verstösst der Reiseveranstalter mit der Veröffentlichung des Videos gegen Art. 5 Abs. 1 Buchst. a DSGVO.

Rechtsgrundlagen sind keine gegeben

So liegen weder Einwilligungen vor, noch lässt sich die Veröffentlichung auf ein überwiegendes berechtigtes Interesse stützen. Zwar mag der Reiseveranstalter ein wirtschaftliches Interesse verfolgen. Allerdings ist hierfür keine Veröffentlichung von Videos erforderlich, bei denen unbeteiligte Personen zu erkennen sind.

Gerade bei der Abwägung mit den Interessen der Betroffenen muss das unternehmerische Interesse hinter diejenigen der Betroffenen zurücktreten. Diese befinden sich im Urlaub und in ihrer Freizeit. Hier muss niemand davon ausgehen, dass er ohne Kenntnis und Einwilligung für Werbezwecke aufgenommen wird. Zudem besteht keinerlei Verbindung zwischen Reiseveranstalter und diesen Personen, sodass eine Verarbeitung für die Personen auch nicht absehbar wäre. Dass es sich um eine bei Influencern beliebte Örtlichkeit handelt, ist unbeachtlich.

KUG spielt keine Rolle

Auch kann sich der Reiseveranstalter nicht auf eventuelle Ausnahmen des Kunsturhebergesetzes (KUG) berufen. Dieses greift nämlich nicht. Hierzu hätte der Reiseveranstalter journalistische Zwecke im Sinne von Art. 85 Abs. 2 DSGVO verfolgen müssen. Die Veröffentlichungen dienten jedoch ausschliesslich Werbezwecken.

Das können wir in der Schweiz folgern

Bei uns hätten Gerichte nicht anders entschieden. Für das Werbevideo müssen entweder Einwilligungen der erkennbaren Personen vorliegen oder diese müssen unkenntlich gemacht werden. Man kann sich nicht darauf berufen, dass dies zu aufwendig, die Sache von der Meinungsfreiheit gedeckt wäre oder betroffene Personen am jeweiligen Ort mit einer Aufnahme/Veröffentlichung hätten rechnen müssen.

PRIVACYXPERTS

IT- & INFORMATIONS-SICHERHEIT UPDATE

SICHER. AKTUELL. PRAXISNAH.

NAVIGIEREN SIE SOUVERÄN DURCH DEN DSCHUNGEL AUS IT-RECHT, CYBERSICHERHEIT UND COMPLIANCE.

CYBER COMPLIANCE-KOMPASS
24 ARBEITSHILFEN FÜR MEHR COMPLIANCE

IHR WEGWEISER FÜR COMPLIANCE, SICHERHEIT UND BUSINESS-KONTINUITÄT

Mit dem 24-teiligen Cyber-Compliance-Kompass und dem E-Magazin „IT- & Informationssicherheit Update" haben Sie das Wissen und die Werkzeuge,die Sie jetzt brauchen.

IHRE VORTEILE

Immer aktuell
Wichtige Entwicklungen und neue Richtlinien verständlich aufbereitet.

Praxisnah umsetzen
Checklisten, Vorlagen und Anleitungen direkt für Ihren Arbeitsalltag.

Über 100 Arbeitshilfen
Exklusive Inhalte im Premiumbereich – für nachhaltige Umsetzung.

Digital & mobil
Mobiloptimiert, durchsuchbar und überall verfugbar.

Webinare & Experten
Regelmäßige Live-Webinare und Aufzeichnungen mit Experten.

Mehr Sicherheit
Stärken Sie Ihre Cyber-Resilienz und erfüllen Sie alle Anforderungen.

HIGHLIGHTS AUS DEM CYBER-COMPLIANCE-KOMPASS

- E-Book: Navigieren im Dschungel des IT-Rechts
- Protokollierungskonzept IT-Systeme & Anwendungen (Excel)
- Soll-Ist Abgleich nach ISO 27001
- Checkliste: Bausteine der KRITIS Verordnung umsetzen
- Entscheidungsbaum: Ist es ein Security Incident?
- Checkliste: Uberprüfung IT-Dienstleister
- 12 Best Practices für Endpoint-Security
- Sicherheitsmaßnahmen für Outlook & Excel
- Anforderungen der Informationssicherheit an das Notfallmanagement
- Cyberversicherung-Fragenkatalog
- Mobile Device Management nach BS
- Muster-Richtlinie: Umgang mit Daten je Vertraulichkeitsklasse
- Richtlinien der Informationssicherheit (Übersicht)
- Checkliste: Cyber-Resilienz
- Checkliste: Backup-Konzept
- und viele weitere Arbeitshilfen, Vorlagen und Anleitungen ...

JETZT GRATIS TESTEN

Testen Sie das E-Magazin 30 Tage kostenlos. Inklusive Cyber-Compliance-Kompass und zahlreicher Arbeitshilfen.

https://t1p.de/it-kompass

DAS EXPERTEN TEAM AN IHRER SEITE

ANDREAS HESSEL
Chief Information Security Officer
Langjähriger Leiter Informationssicherheit Risikomanagement einer Bank. Externer Datenschutzbeauftragter und Berater für Cybersicherheit. Fachautor.

MICHAEL ROHRLICH
Rechtsanwalt
Fachautor, Dozent und Video-Trainer für IT-Recht, Datenschutz und e-Commerce. Autor fur diverse Print- und Online-Publikationen.

MARC OLIVER THOMA
IT-Sicherheitstrainer & Berater
Experte für IT-Sicherheit, Datenschutz und Kommunikation. Linkedin-Learning-Trainer und externer Datenschutzbeauftragter für KMU.

GUT INFORMIERT. PRAXISNAH. SOFORT UMSETZBAR. **www.privacyxperts.de**

Erstellt für Schweizer Datenschutzberater
und für alle mit Aufgaben im Datenschutz
in der Schweiz von:

PRIVACYXPERTS

Telefon: +49 2 28 95 50 150
Fax: +49 2 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: kurzlink.ch/privacy

Ein Unternehmensbereich des VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Strasse 2–4
53177 Bonn, Deutschland

Vorschau:

Neue Mitarbeiter:
Setzen Sie auf die Führungskräfte

Nutzen Sie Merkblätter,
um den Datenschutz vorwärtszubringen