8/25

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER

SOCIAL ENGINEERING

Wie der Mensch im Jahr 2025 zum Ziel von Kriminellen wird

URLAUBSZEIT ...

... gleich Angriffszeit? Warum der Datenschutz nicht mit in die Ferien darf

powered by
PRIVACYXPERTS

Der Mensch im Fokus – Sicherheitsrisiken im digitalen Alltag

Liebe Leserin, lieber Leser,

technologische Fortschritte haben in den letzten Jahren für deutlich mehr Sicherheit in unseren digitalen Infrastrukturen gesorgt. Firewalls, Verschlüsselung, Zugriffskontrollen – all das funktioniert heute besser denn je. Doch Kriminelle denken mit: Wo Systeme stabiler werden, rückt der Mensch ins Visier.

In dieser Ausgabe werfen wir deshalb einen genaueren Blick auf zwei aktuelle Bedrohungsszenarien, die weniger mit Technik, dafür umso mehr mit menschlichem Verhalten zu tun haben.

Im ersten Beitrag beleuchten wir die Methoden des Social Engineering. Angreifer nutzen hier gezielt psychologische Tricks, um Mitarbeiter zu manipulieren und so an vertrauliche Informationen zu gelangen – ganz ohne technische Hürden. Ob per E-Mail, Telefon oder im persönlichen Gespräch: Wer sich sicher fühlt, ist oft besonders anfällig.

Passend zur Jahreszeit widmen wir uns im zweiten Beitrag den Gefahren, die sich in der Urlaubszeit einschleichen. Wenn Führungskräfte abwesend sind, Vertretungen improvisiert agieren und der Arbeitsmodus auf „Sommerleicht" gestellt wird, nutzen Angreifer die Gelegenheit. Besonders im mobilen Arbeiten – etwa aus dem Homeoffice am Meer – wird Datenschutz schnell zur Nebensache.

Zwei Beiträge, ein gemeinsames Thema: Sicherheit beginnt beim Menschen. Wir zeigen Ihnen, wie Sie sich und Ihr Unternehmen schützen – ob im Alltag oder auf der Sonnenliege.

Viel Spaß beim Lesen – und bleiben Sie wachsam mit unseren Tipps!

SEBASTIAN TAUSCH
ARBEITET ALS SELBSTSTÄNDIGER IT-BERATER UND UNTERSTÜTZT KLEINE UND MITTLERE UNTERNEHMEN PRAXISNAH IM BEREICH DATENSCHUTZ. NACH EINER KAUFMÄNNISCHEN AUSBILDUNG SAMMELTE ER VIELE JAHRE PRAKTISCHE IT-ERFAHRUNG.

ANDREAS HESSEL
IST ALS CHIEF INFORMATION SECURITY OFFICER LANGJÄHRIGER LEITER DES BEREICHES INFORMATIONSSICHERHEIT UND RISIKOMANAGEMENT EINER LANDESBANK. DANEBEN ARBEITET ER ALS EXTERNER DATENSCHUTZBEAUFTRAGTER UND BERATER IM BEREICH CYBERSECURITY.

SOCIAL ENGINEERING: WIE DER MENSCH IM JAHR 2025 ZUM ZIEL VON KRIMINELLEN WIRD

Die technischen Sicherheitsmaßnahmen in Unternehmen wurden in den vergangenen Jahren immer besser. Deshalb versuchen die Angreifer, das vermeintlich schwächste Glied in der Kette anzugreifen: den Menschen bzw. die Beschäftigten des Unternehmens. Bei Social-Engineering-Angriffen verfolgen die Angreifer also nicht das Ziel, technische Sicherheitslücken in Systemen auszunutzen, sondern Menschen!

Das versteht man unter Social Engineering

Beim Social Engineering werden Manipulationstechniken eingesetzt. Mithilfe dieser Techniken sollen Menschen oftmals dazu gebracht werden, den Angreifern

- sensible Daten oder Dokumente zu übermitteln,
- Geld oder andere Vermögenswerte zu transferieren,
- zu helfen, technische Schutzmaßnahmen zu umgehen.

Die Angreifer nutzen dazu die unterschiedlichsten Kommunikationswege und Methoden sowie Kombinationen, um an ihr Ziel zu gelangen. Mögliche Opfer sind sowohl Unternehmen und andere Organisationen als auch Privatpersonen.

Phishing, Smishing und Quishing

Üblicherweise senden die Angreifer beim Phishing eine Nachricht per E-Mail (Phishing), SMS (Smishing) oder Messenger. Es werden aber auch andere Kommunikationskanäle genutzt, wie Chats in Online-Plattformen oder QR-Codes (Quishing). Das Ziel eines Phishing-Angriffs ist es eigentlich, Zugangsdaten zu erbeuten. Oft werden aber auch andere sensible Daten über diese Kommunikationskanäle erbeutet, etwa Kreditkartendaten. Die Absender geben sich als Bank, Behörde oder große Plattform aus. QR-Codes von Kriminellen wurden unter anderem auf Ladesäulen für Elektroautos und auf angeblichen Strafzetteln gefunden.

Achtung: Die große Herausforderung ist zunehmend, Nachrichten auch als Phishing zu erkennen. Denn diese werden immer besser!

Durch den Einsatz von Automatisierung und künstlicher Intelligenz (KI) sowie erbeuteten und veröffentlichten Daten sind die Angreifer zunehmend in der Lage, individualisierte Phishing-Nachrichten mit echten Daten zu übermitteln. Statt also Nachrichten einer „Sparkasse“ zu versenden, enthalten diese Nachrichten dann die jeweils korrekte Bezeichnung der Sparkasse und sogar die richtige Kontonummer bzw. einen Teil davon.

Pretexting und die Chef-Falle

Beim sogenannten Pretexting nehmen die Angreifer eine falsche Identität an und entwickeln ein mehr oder weniger glaubhaftes Szenario.

So gibt es sehr schlichte Varianten, bei denen die Angreifer nahezu wahllos ihre potenziellen Opfer kontaktieren und sich etwa als Mitarbeiter von Microsoft ausgeben. In dieser Rolle versuchen diese dann, ihr Opfer dazu zu bringen, dass es einen Fernwartungszugang öffnet oder eine Schadsoftware installiert.

In anderen Fällen recherchieren die Angreifer ausführlicher und können damit realistisch wirkende Geschichten erfinden. Hier gibt sich der Angreifer dann etwa als bekannte Person des beauftragten IT-Dienstleisters aus, bezieht sich z. B. auf ein gerade durchgeführtes Software-Projekt, weiß, dass der IT-Leiter im Urlaub ist, und bittet um Fernwartungszugang wegen eines wichtigen Problems.

Als einen speziellen Pretexting-Angriff kann die sogenannte Chef-Falle (CEO-Fraud) angesehen werden. Hierbei geben sich die Angreifer als Chef oder Vorgesetzter aus und versuchen, ihre potenziellen Opfer dazu zu bringen, Finanztransaktionen durchzuführen.

Enkeltrick, Schockanrufe, Honeytrap und Erpressung

Social-Engineering-Angriffe zielen nicht nur auf Unternehmen ab. Einige Kriminelle haben speziell Senioren im Visier und geben sich als Enkel in Not, etwa wegen eines Unfalls im Urlaub, aus. Andere setzen Familienmitglieder unter Schock, etwa indem sie sich als Beamte oder Mitarbeiter eines Krankenhauses ausgeben und behaupten, dass ein Familienmitglied einen schweren Unfall hätte oder in eine kriminelle Handlung verwickelt sei.

>

> Mit der Honeytrap-Strategie versuchen Angreifer, eine romantische oder sexuelle Beziehung zum potenziellen Opfer aufzubauen, um im Anschluss um Geld zu bitten oder – etwa nach der vorherigen Übermittlung intimer Bilder – dieses zu erpressen.

Baiting

Beim Baiting (englisch für Ködern) stellen die Kriminellen ihren potenziellen Opfern einen kostenfreien oder stark vergünstigten Gegenstand oder eine Dienstleistung bzw. Belohnung in Aussicht. Teilweise wird auch versucht, die Neugier zu wecken. Dies wurde – insbesondere früher – etwa dadurch erreicht, dass USB-Sticks mit Schadsoftware „zufällig" verloren wurden.

Heute locken die Angreifer eher mit angeblich teuren gewonnenen Artikeln, wie Smartphones, oder stellen kostenfreie oder stark vergünstigte Software oder Dienstleistungen, wie Musik- oder Video-Streaming, in Aussicht. Im Regelfall zielen die Angriffe darauf ab, dass die Opfer sensible Daten übermitteln oder eine Schadsoftware installieren.

Tailgating/Piggybacking

Beim Tailgating (etwa dicht auffahren/dicht folgen), auch Piggybacking (etwa Huckepack) genannt, versuchen Angreifer, sich Zugang zu einem Bereich, Gebäude oder Raum zu verschaffen. Sehr vereinfacht lassen sich die Angreifer durch eine berechtigte Person mitnehmen oder sich von dieser die Türe aufhalten. Schlussendlich wird hier die Hilfsbereitschaft ausgenutzt.

In der Praxis gibt sich der Angreifer etwa als Lieferant, Paketbote, Handwerker oder Reinigungskraft aus. Er läuft dann einfach einer Person hinterher, welche in den gewünschten Bereich geht, und bittet ihn etwa, die Türe aufzuhalten – sofern das nicht ohnehin automatisch erfolgt.

Am Ziel angelangt, kann die Person dann je nach Situation und Ziel z. B. Dokumente oder Daten einsehen, kopieren oder entwenden und Geräte manipulieren, entwenden sowie eigene Geräte, etwa für einen Zugriff von außen, installieren.

So schützen Sie sich vor Social-Engineering-Angriffen

Beim Social Engineering nutzen die Angreifer Manipulationstechniken, um ihre potenziellen Opfer dazu zu bringen, eine Handlung auszuführen. Dazu wird entweder Neugier geweckt, eine Belohnung oder ein hoher Rabatt in Aussicht gestellt, auf die Hilfsbereitschaft der Person gesetzt oder Druck aufgebaut und mit möglichen Konsequenzen Angst erzeugt. Dies sind somit zumindest erste Indizien für einen Social-Engineering-Angriff. Deshalb:

1. Seien Sie skeptisch bei ungewöhnlichen Anfragen

Besonders dann, wenn Druck aufgebaut wird („dringend", „sofort", „Chef hat's beauftragt") oder Daten/Zugänge eingefordert werden: Fragen Sie lieber einmal mehr nach – etwa direkt bei Ihrer Führungskraft, der IT oder den jeweiligen Verantwortlichen.

2. Prüfen Sie Absender, Links und Anhänge

Klicken Sie nicht ohne vorherige Prüfung auf Links oder beigefügte Anhänge, wenn Ihnen die Nachricht seltsam vorkommt. Dies gilt auch, wenn der Absender augenscheinlich bekannt ist!

Bitte bedenken Sie bei Ihrer Prüfung, dass die Angreifer mithilfe von Schadsoftware oder einer vorherigen erfolgreichen Phishing-Attacke möglicherweise auch Zugriff auf das Postfach des Absenders haben. Fragen Sie bei Zweifeln beim vorgegebenen Absender nach

und verwenden Sie hierfür andere, bekannte Kommunikationskanäle.

3. Lassen Sie sich nicht unter Druck setzen

Dringlichkeit ist ein typisches Mittel zur Manipulation. Sie kennen das sicherlich bereits aus Phishing-Nachrichten, in denen Ihnen als Konsequenz aufgezeigt wird, dass etwa das betroffene Bank- oder Benutzerkonto unwiderruflich gesperrt wird oder hohe Kosten entstehen.

Je nach Kontext des Angriffs werden die Angreifer erhebliche Konsequenzen in Aussicht stellen. Um solche Drohungen ins Leere laufen zu lassen, sollten im Vorfeld interne Regelungen und Absprachen getroffen werden, etwa zu Zuständigkeiten, Vertretungen, oder auch Authentifizierungsnachweise, wenn eine Person nicht persönlich vor Ort ist.

4. Lassen Sie Ihre Hilfsbereitschaft nicht ausnutzen

Natürlich hilft man anderen Personen gerne und hält diesen etwa die Türe auf, gerade wenn diese „die Hände voll“ haben. Nur wissen das leider auch Kriminelle. Finden Sie im Bedarfsfall heraus, wie Besucher und Dienstleister in Ihrem Unternehmen empfangen und begleitet werden, sodass keine Person Bereiche oder Räume betritt, welche für sie nicht vorgesehen sind.

5. Lassen Sie sich nicht täuschen

Die Angreifer recherchieren im Vorfeld oder nutzen geleakte, veröffentlichte Daten, um möglichst glaubwürdig zu erscheinen.

Machen Sie es den Angreifern so schwer wie möglich, Sie zu täuschen! Nutzen Sie unterschiedliche Zugangsdaten für verschiedene Dienste oder wenn möglich das Passkey-Verfahren. Prüfen Sie je nach Bedarf, ob die Person, die Sie kontaktiert hat, wirklich bei dem jeweiligen Unternehmen oder der Behörde arbeitet, und versuchen Sie, diese über einen anderen Kontaktweg zu erreichen.

Fazit:

Social Engineering ist keine abstrakte Bedrohung – es ist Alltag. Mit einem gesunden Maß an Skepsis, technischem Schutz und dem Bewusstsein für Manipulationstechniken lassen sich entsprechende Angriffe erkennen und abwehren.

Bei Fragen oder Unsicherheiten stehen Ihnen Ihre Vorgesetzten oder Ansprechpartner zum Thema Sicherheit und Datenschutz sicherlich gerne zur Verfügung. (ST)

URLAUBSZEIT – ANGRIFFSZEIT? WARUM DER DATENSCHUTZ NICHT MIT IN DIE FERIEN DARF

Endlich Urlaub! Die Sonne lacht, das Handy bleibt aus – zumindest fast. Während Sie gedanklich schon mit den Zehen im Sand spielen, beginnt für Angreifer die Hochsaison. Denn wenn Führungskräfte länger abwesend sind, Vertretungen eilig geregelt werden und der E-Mail-Verteiler großzügig gefüllt ist, dann öffnen sich oft kleine Türen, durch die große Risiken schlüpfen.

Auch wenn die Aussicht aus dem Homeoffice auf Sardinien atemberaubend ist, brauchen Datenschutz und IT-Sicherheit auch im mobilen Arbeiten mehr als nur gutes WLAN. In dieser Ausgabe zeigen wir Ihnen, wie Sie Ihre Erholung genießen können, ohne dass Ihr Unternehmen dabei baden geht.

Datenschutz macht keinen Urlaub: 5 Punkte für ein sicheres „Büro-Bye-Bye“

Urlaub fängt im Kopf an, aber beim Datenschutz bitte schon im Kalender. Denn wer einfach so den Laptop zuklappt und sich in die Ferien verabschiedet, hinterlässt oft mehr als nur seine Kaffeetasse.

Gerade in der Urlaubszeit entstehen Sicherheitslücken nicht durch böse Absicht, sondern durch fehlende Planung. Damit das nicht passiert, finden Sie nachfolgend Ihre Datenschutz-Checkliste vor dem Abflug:

1. Vertretung klar regeln – aber bitte mit Köpfchen

Überlegen Sie genau, wer Ihre Aufgaben übernimmt und vor allem auf welche Daten diese Person tatsächlich zugreifen muss. Ein „Ich habe dir mal alles weiter- >

> geleitet“ mag gut gemeint sein, verletzt aber schnell den Grundsatz der Datenminimierung. Zugriffe auf personenbezogene Daten dürfen nur dann erfolgen, wenn sie für die Vertretung unbedingt nötig sind.

Mein Tipp:
Temporäre Zugriffsrechte einrichten. Am besten befristet und dokumentiert.

2. E-Mail-Autoantworten mit Verstand

„Ich bin bis zum Soundsovielten nicht erreichbar. Bitte wenden Sie sich an …“ – so weit, so gut. Aber bitte keine halbe Personalakte in die Abwesenheitsnotiz. Vermeiden Sie persönliche Informationen und geben Sie als Kontaktperson möglichst eine allgemeine Funktionsadresse an, z. B. datenschutz@unternehmen.de oder team@firma.de. Das schützt nicht nur die Privatsphäre, sondern erschwert auch Social Engineering durch Dritte.

3. Gemeinsame Kalender? Nur wenn’s nötig ist

Wer darf sehen, wo Sie sind, und müssen das wirklich alle Kolleginnen und Kollegen wissen? Schützen Sie Ihre Kalendereinträge vor neugierigen Blicken. In vielen Tools können Sie einstellen, ob nur „abwesend“ oder auch Details wie „Reha“, „Klinik“ oder „Weltreise mit Route“ angezeigt werden. Tragen Sie solche Details besser nicht ein.

Mein Tipp:
Weniger ist im Datenschutz meistens mehr.

4. Keine offenen Baustellen

Daten, die nicht mehr gebraucht werden, gehören gelöscht oder archiviert und das möglichst vor dem Urlaub. Besonders dann, wenn Kolleginnen oder Kollegen Ihre Projekte übernehmen, sollte klar sein, wo sich welche Informationen befinden und wie damit umzugehen ist. Ein unstrukturierter Schreibtisch oder chaotischer Dateispeicher sind wie eine Einladung zum Datenschutz-Desaster.

5. Der Klassiker: Bildschirm sperren, Laptop verstauen

Auch wenn’s banal klingt: Ein unbeaufsichtigter Rechner im Büro ist ein offenes Scheunentor. Sorgen Sie dafür, dass Ihr Arbeitsplatz sauber hinterlassen wird – digital und physisch.

Mein Tipp:
Alles, was vertraulich ist, wird weggeschlossen oder passwortgeschützt abgelegt. Und das Handy nicht auf dem Schreibtisch liegen lassen, auch nicht „nur für zwei Wochen“.

Fazit: Mit ein paar durchdachten Handgriffen vor dem Urlaub stellen Sie sicher, dass Ihr Datenschutz nicht ins Schwitzen kommt und Sie ganz ohne „Bauchgrummeln“ abschalten können.

Wenn Angreifer Urlaubsgrüße fälschen – Social Engineering hat Hochsaison

Urlaubszeit ist Angriffszeit, vor allem für Cyberkriminelle, die es auf Unternehmen abgesehen haben. Denn während im Büro die Telefone stiller klingen und viele Kolleginnen und Kollegen abwesend sind, wittern Betrüger ihre Chance. Besonders beliebt sind Social-Engineering-Attacken per E-Mail oder Anruf, die genau auf solche Situationen zugeschnitten sind.

Ein typisches Szenario per E-Mail

Eine Nachricht landet in der Buchhaltung. Absender: Der Geschäftsführer persönlich – zumindest sieht es auf den ersten Blick so aus. Betreff: „Dringende Zahlung – bitte heute noch überweisen.“ Die Mail ist knapp formuliert, der Ton ist autoritär, aber plausibel. Und weil die Assistenz im Urlaub ist, springt ein Kollege ein und führt die Überweisung aus. Später stellt sich heraus: Der Chef sonnt sich gerade auf Kreta und hat von der Mail nichts gewusst. Der Absender war ein Krimineller, der Name im Absenderfeld war gefälscht.

Doch es bleibt nicht bei E-Mails – auch das Telefon wird zur Angriffsfläche

Ein Anruf geht im Sekretariat ein. Die Stimme klingt freundlich, professionell. Der Anrufer erklärt, er arbeite im Auftrag von Frau Müller aus dem Vertrieb, die ja derzeit in Urlaub sei, was auch brav in der Abwesenheitsnotiz steht, die der Angreifer zuvor erhalten hat. Man müsse dringend an Kundendaten, um ein laufendes Projekt zu retten. Die neue Kollegin, die erst seit letzter Woche im Team die Urlaubsvertretung macht, will hilfsbereit sein und nennt die gewünschten Informationen. Nachfragen bei Frau Müller? Leider unmöglich. Die liegt gerade im Funkloch der Toskana.

Was macht diese Tricks so gefährlich? Das müssen Sie beachten

Angreifer nutzen gezielt das Informationsleck, das viele Abwesenheitsnotizen hinterlassen: Wer ist weg, wie lange, wer vertritt?

Mit diesen Puzzlestücken bauen sie glaubwürdige Lügengeschichten und hoffen, dass gerade im Sommer der gesunde Zweifel in Flipflops unterwegs ist.

Was können Sie konkret tun?

- **Vermeiden Sie unnötige Details in Abwesenheitsnotizen**

  Wer im Urlaub ist, muss nicht die ganze Welt wissen. Es reicht oft: „Ich bin aktuell nicht erreichbar. Ihre Nachricht wird nicht weitergeleitet."

- **Lassen Sie sich nicht unter Zeitdruck setzen – weder per Mail noch am Telefon**

  Seriöse Geschäftspartner haben Verständnis, wenn eine kurze Prüfung nötig ist.

- **Verifizieren Sie Aufträge und Identitäten**

  Fragen Sie über bekannte Nummern oder Kanäle zurück – nicht über die Nummer, die Ihnen genannt wurde.

- **Sprechen Sie im Team über mögliche Angriffsversuche**

  Je wachsamer das gesamte Team, desto geringer das Risiko, dass ein Einzelner getäuscht wird.

Mein Tipp:

Eins ist sicher, Kriminelle machen keinen Urlaub. Sie planen ihn mit Ihren Daten.

Sonne, Sand und sensible Daten – Arbeiten im Urlaub birgt Risiken

Klingt verlockend, morgens eine Videokonferenz, nachmittags Strandbar. Doch wer im Urlaub arbeitet, riskiert mehr als nur einen Sonnenbrand. Denn ein Hotelzimmer ist kein Büro und der Flughafen keine vertrauliche Besprechungszone. Öffentliches WLAN, neugierige Blicke und fehlender physischer Schutz machen mobile Arbeit unterwegs zu einem echten Risiko für den Datenschutz.

Besonders heikel sind Dienstgeräte auf Reisen ins Ausland. In einigen Ländern, z. B. den USA, darf der Zoll bei der Einreise elektronische Geräte durchsuchen und dabei auch auf gespeicherte Unternehmensdaten zugreifen. Und zwar ganz legal. Wer hier keine klare Trennung von privat und dienstlich hat oder sensible Informationen unverschlüsselt mitführt, läuft Gefahr, dass mehr mitreist als geplant.

Mein Tipp:

Wenn Sie im Urlaub wirklich arbeiten müssen, klären Sie vorher mit Ihrer IT, welche Sicherheitsvorkehrungen nötig sind. Noch besser wäre es, sich und Ihren Daten mal eine Pause zu gönnen. Beide werden es Ihnen danken. (AH)

WUSSTEN SIE SCHON,

dass ein einzelner USB-Stick Ihr ganzes Unternehmen in Schwierigkeiten bringen kann?

Was aussieht wie ein harmloser Speicherzwerg, ist in Wahrheit ein echtes Risiko. Denn USB-Sticks sind nicht nur Träger von Präsentationen und Urlaubsfotos, sie sind auch ein beliebtes Einfallstor für Schadsoftware. Kriminelle legen z. B. gezielt manipulierte USB-Sticks auf Firmenparkplätzen, in Tiefgaragen oder in der Nähe von Eingängen aus. Weil der Mensch von Natur aus neugierig ist, landet so ein Fundstück schnell im nächsten Firmenrechner.

„Mal kurz schauen, wem der gehört" – genau dieser Impuls ist es, auf den Angreifer setzen. Denn beim Einstecken kann sich eine Schadsoftware sofort selbstständig ausführen, ohne dass man etwas davon merkt.

Manche USB-Sticks tarnen sich sogar als Tastatur oder Netzwerkgerät und schleusen unbemerkt Skripte ein, die Passwörter abgreifen oder Hintertüren öffnen.

Was Sie daraus mitnehmen sollten:

- Geben Sie solche Fundstücke an die IT weiter.
- Benutzen Sie keine privaten USB-Sticks im Unternehmensnetzwerk – auch nicht „nur mal eben schnell".

Fazit:

Finger weg von unbekannten Sticks, auch wenn sie hübsch glänzen. Im Zweifel ist der Inhalt gefährlich. (AH)

KI IM UNTERNEHMEN SICHER EINFÜHREN

Künstliche Intelligenz – kurz KI (engl. AI) – ist längst keine abstrakte Zukunftstechnologie mehr. Viele Anwendungen und Apps, die wir täglich nutzen, beinhalten bereits KI-Funktionen: automatische Sortierungen in E-Mail-Programmen, Übersetzungshilfen in Schreibprogrammen, automatische Bildverbesserung etc. Dabei wird deutlich: KI ist kein Projekt „für später", sondern bereits Teil des Arbeitsalltags. Unser Video unterstützt Sie mit den wichtigsten Erkenntnissen. Scannen Sie einfach den QR-Code.

Ich habe die Ausgabe von Privacy@Work gelesen:

Name, Vorname, Abteilung	Unterschrift

Bei Fragen im Bereich Datenschutz wenden Sie sich bitte an Ihre Datenschutzbeauftragte oder Ihren Datenschutzbeauftragten!

Impressum:

PRIVACYXPERTS

PrivacyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, D-53177 Bonn; Großkundenpostleitzahl: D-53095 Bonn; Handelsregister: HRB 8165, Registergericht: Amtsgericht Bonn, Vertreten durch den Vorstand: Richard Rentrop, ISSN: 1614 – 5674; Kontakt: Telefon: 0228 – 9 55 01 60 (Kundendienst); Telefax: 0228 — 3 69 64 80, E-Mail: kundendienst@privacyxperts.de, Internet: https://www.privacyxperts.de, Umsatzsteuer: Umsatzsteuer-Identifikationsnummer gemäß §27a Umsatzsteuergesetz: DE 812639372, V.i.S.d.P.: Michael Jodda; Theodor-Heuss-Straße 2–4; D-53177 Bonn, Herausgeber: Michael Jodda, Bonn, Autoren: Andreas Hessel, Sebastian Tausch, Produktmanagement: Lisa Suchy, Bonn, Layout & Satz: Bettina Pour-Imani, BB-Design, Birken-Honigsessen, Bildrechte Seite 1: Yuliia, ketkata, S. 4 Yuliia, S. 4 PureSolution – alle AdobeStock.com, Druck: Warlich Druck Meckenheim GmbH, Meckenheim

Erscheinungsweise: 16-mal pro Jahr; Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird. Alle Angaben in Privacy@Work wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier