3/26

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER

MULTI-FAKTOR-AUTHENTIFIZIERUNG

Stark – aber in 2026 nicht unknackbar

WARUM NICHT JEDER ALLES SEHEN MUSS

Das Prinzip der minimalen Berechtigung

powered by
PRIVACYXPERTS

Liebe Leserinnen und Leser,

IT-Sicherheit beginnt nicht bei der Technik, sondern bei uns selbst. Moderne Schutzmaßnahmen wie die Multi-Faktor-Authentifizierung (MFA) verhindern täglich unzählige unberechtigte Zugriffe.

Doch Angriffe entwickeln sich weiter. Kriminelle setzen zunehmend auf Stress, Gewohnheit und menschliche Reaktionen statt auf technische Schwachstellen. MFA ist ein starkes Werkzeug – aber kein Freifahrtschein.

Ähnlich verhält es sich mit Zugriffsrechten im Arbeitsalltag. Über Jahre gewachsene Berechtigungen, geteilte Ordner und große Verteiler entstehen meist aus Pragmatismus, nicht aus böser Absicht. Dennoch erhöhen sie das Risiko für Datenabflüsse und Fehler – und betreffen damit nicht nur das Unternehmen, sondern auch jede einzelne Person.

Beide Themen zeigen: Sicherheit ist kein einmal eingerichteter Zustand, sondern ein fortlaufender Prozess. Aufmerksamkeit, kritisches Hinterfragen und klare Regeln sind dabei genauso wichtig wie technische Lösungen.

Die folgenden Beiträge sollen sensibilisieren, nicht verunsichern. Sie erklären typische Angriffsmethoden, zeigen Risiken im Alltag auf und geben konkrete Hinweise, wie jede und jeder zur Sicherheit beitragen können. Denn wirksam ist IT-Sicherheit nur dann, wenn Technik und verantwortungsvolles Handeln zusammenwirken.

Herzliche Grüße,

Ihr Redaktionsteam von „Privacy@Work“

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.

MULTI-FAKTOR-AUTHENTIFIZIERUNG: STARK – ABER IN 2026 NICHT UNKNACKBAR

Die Multi-Faktor-Authentifizierung (MFA) gehört bislang mit zu den wichtigsten Schutzmaßnahmen für Onlinezugänge. Sie stellt sicher, dass für den Zugriff auf ein Benutzerkonto nicht mehr nur Benutzername und Passwort ausreichen, sondern ein zusätzlicher Faktor erforderlich ist. Auch wenn Kriminelle die Zugangsdaten kennen, scheitert deren Zugriff in vielen Fällen genau an dieser zweiten Hürde.

Doch so wirksam MFA auch ist: Sie ist nicht unknackbar. Vor allem dann nicht, wenn Angreifer gezielt den Menschen angreifen – und nicht die Technik.

Wie MFA funktioniert

Bei der Anmeldung wird nach Benutzername und Passwort ein weiterer Faktor abgefragt. Dabei handelt es sich um etwas, das man besitzt – in der Praxis meist das Smartphone. Die MFA besteht somit aus Wissen (Benutzername und Passwort) und Besitz, etwa das Smartphone.

Je nach System muss

- ein Einmalcode eingegeben werden, der per App erzeugt oder per SMS empfangen wird, oder
- eine Anmeldung aktiv über eine App bestätigt werden.

Erst wenn dieser zweite Faktor korrekt bestätigt wurde, ist der Log-in erfolgreich.

Abbildung 1: Beispiel einer MFA-Anmeldeanforderung mit zusätzlichem Bestätigungscode per SMS

Große Onlineanbieter stellen häufig mehrere Varianten für den zweiten Faktor zur Verfügung. Dazu zählen beispielsweise per SMS übermittelte Codes, die Code-Generierung über eine allgemeine Authenticator-App, Bestätigungen über eine eigene Anbieter-App oder auch automatisierte Telefonanrufe.

Um den Anmeldeprozess im Alltag zu vereinfachen, erlauben einige Anbieter zudem, den jeweils genutzten Browser in Verbindung mit dem verwendeten Gerät – oft zeitlich befristet – als „vertrauenswürdig“ zu hinterlegen. In diesen Fällen ist bei späteren Anmeldungen nicht bei jedem Log-in eine erneute MFA-Abfrage erforderlich.

Einfach betrachtet, übernimmt der Browser auf dem konkreten Gerät dann die Rolle eines zusätzlichen Faktors, da der Zugriff voraussetzt, dass sich der Nutzer im Besitz dieses Geräts befindet.

Woher haben Angreifer meine Zugangsdaten?

Ein weitverbreiteter Irrtum ist die Annahme, Kriminelle müssten Benutzername und Passwort erst mühsam erraten. Tatsächlich werden im Internet und im sogenannten Darknet große Mengen kompromittierter Zugangsdaten gehandelt – teilweise kostenpflichtig, teilweise sogar frei zugänglich.

Diese Daten stammen aus früheren Datenpannen, Phishing-Angriffen oder Schadsoftware-Infektionen. Besonders problematisch ist dabei, dass viele Nutzer dieselben Zugangsdaten für mehrere Dienste verwenden. Gelingt es Angreifern, eine Kombination aus E-Mail-Adresse und Passwort zu erlangen, wird diese automatisiert bei zahlreichen Plattformen ausprobiert.

Ist ein Konto zusätzlich mit MFA geschützt, bleibt der Zugriff zunächst blockiert – doch genau hier setzen die weiteren Angriffsmethoden an.

MFA-Bombing: Wenn Bestätigungen zur Belastung werden

Beim sogenannten MFA-Bombing (auch Push-Fatigue) verfügen Angreifer bereits über gültige Zugangsdaten, scheitern jedoch am zweiten Faktor. Um dieses Hindernis zu überwinden, starten sie immer wieder neue Log-in-Versuche.

Jeder Versuch löst eine neue MFA-Anfrage auf dem Smartphone des Betroffenen aus. Besonders anfällig >

> hierfür sind MFA-Lösungen, die entsprechende Push-Meldungen auf dem Smartphone auslösen.

Die Hoffnung der Angreifer:

- Die Vielzahl der Meldungen nervt,
- es wird ein technischer Fehler vermutet oder
- die Anfrage wird aus Stress oder Gewohnheit bestätigt.

Erhalten Sie MFA-Anfragen oder Codes, obwohl Sie sich gerade nirgendwo anmelden, ist das ein klares Warnsignal. Solche Anfragen dürfen nicht bestätigt werden. Stattdessen sollte der Vorfall umgehend über die vorgesehenen internen Meldewege – etwa an die IT-Abteilung – weitergegeben werden.

Der „MFA-Reset"-Trick: Social Engineering statt Technik

Bleibt das MFA-Bombing erfolglos, folgt häufig der nächste Schritt: der direkte Kontakt zum Opfer. Dabei geben sich Angreifer beispielsweise als IT-Support aus und verweisen auf die zuvor aufgetretenen MFA-Meldungen.

Sie bieten an, die MFA „zurückzusetzen" oder neu einzurichten. Nach mehreren störenden Anfragen klingt dieses Angebot oft plausibel.

Tatsächlich fordern die Angreifer dabei jedoch

- die Bestätigung einer MFA-Anfrage oder
- die Weitergabe eines per SMS empfangenen Codes.

Mit dieser Bestätigung wird die MFA nicht neu eingerichtet, sondern der Zugriff für die Angreifer freigegeben.

MFA-Codes oder Bestätigungen dürfen niemals telefonisch, per E-Mail oder Chat weitergegeben werden.

Passwort- und MFA-Phishing in Echtzeit

Eine besonders professionelle Angriffsmethode kombiniert mehrere Schritte. Ziel ist es, Benutzername, Passwort und den zweiten Faktor nahezu zeitgleich abzugreifen.

Häufig beginnt der Angriff mit einer täuschend echten E-Mail, etwa mit dem Hinweis auf eine angeblich freigegebene Datei über OneDrive oder SharePoint. Der enthaltene Link führt jedoch auf eine nachgebaute Anmeldeseite.

Im Hintergrund kommen dabei spezialisierte kriminelle Werkzeuge zum Einsatz. Solche Phishing-Seiten sind oft Teil fertiger Angriffspakete, die inklusive Hosting, Vorlagen und automatisierter Weiterleitung angeboten werden. Die eingegebenen Zugangsdaten werden in Echtzeit an die Angreifer weitergeleitet, die parallel versuchen, sich auf der echten Plattform anzumelden.

Bestätigen Betroffene zusätzlich die MFA-Anfrage, wird der Zugriff unmittelbar freigegeben. Diese Angriffe erfolgen nicht nur per E-Mail. Auch Messenger-Dienste, Kollaborationstools oder Telefonanrufe werden genutzt – teilweise vollständig automatisiert.

Abbildung 2: Bestätigung einer Anmeldung über einen per SMS zugesendeten Code

Credential-Stuffing und professionalisierte Angriffsdienstleistungen

Gelangen Kriminelle an Kombinationen aus E-Mail-Adresse und Passwort, werden diese Daten häufig automatisiert weiterverwendet. Bei sogenannten Credential-Stuffing-Angriffen testen Angreifer bekannte Zugangsdaten systematisch bei einer Vielzahl von Onlinediensten. Hintergrund ist, dass viele Nutzer identische Passwörter für unterschiedliche Konten verwenden.

Solche Angriffe erfolgen nicht manuell, sondern mit speziell entwickelter Software. Diese Programme prüfen innerhalb kurzer Zeit Tausende oder sogar Millionen von Zugangsdaten gegen verschiedene Plattformen. Treffer werden automatisch weiterverarbeitet oder weiterverkauft.

Parallel dazu hat sich ein regelrechter Markt für professionalisierte Angriffsdienstleistungen entwickelt. Im Internet und in geschlossenen Foren kann man fertige Werkzeuge, Phishing-Kits und komplette Angriffspakete finden.

Teilweise werden diese Dienstleistungen sogar als Abonnement angeboten, inklusive Support, Updates und Anleitungen. Dadurch können auch technisch weniger versierte Täter komplexe Angriffe durchführen.

Was im Ernstfall zu tun ist

Wenn Sie unsicher sind oder vermuten, auf einen solchen Angriff hereingefallen zu sein:

- Informieren Sie sofort Ihre zuständigen Ansprechpartner,
- lassen Sie aktive Sitzungen beenden und
- setzen Sie Zugangsdaten zurück.

Je schneller reagiert wird, desto geringer sind bestenfalls die möglichen Schäden.

Fazit:

Die MFA bleibt eine zentrale Sicherheitsmaßnahme und verhindert täglich zahlreiche unberechtigte Zugriffsversuche. Gleichzeitig gilt: Je attraktiver ein Ziel ist, desto mehr Aufwand betreiben Angreifer – und desto professioneller werden die kriminellen Methoden.

Wer typische Angriffe wie MFA-Bombing, Support-Tricks oder kombinierte Phishing-Angriffe kennt, kann diese frühzeitig identifizieren und richtig reagieren. Aufmerksamkeit bleibt damit ein entscheidender Sicherheitsfaktor.

Einige Anbieter setzen inzwischen ergänzend oder alternativ auf sogenannte Passkeys. Dabei wird vollständig auf klassische Passwörter verzichtet. Die Anmeldung erfolgt stattdessen gerätegebunden, beispielsweise per Fingerabdruck, Gesichtserkennung oder Gerätesperre.

Passkeys gelten daher als ein vielversprechender Ansatz, um bestimmte Angriffsmethoden deutlich zu erschweren. (ST)

WARUM NICHT JEDER ALLES SEHEN MUSS – DAS PRINZIP DER MINIMALEN BERECHTIGUNG IM ARBEITSALLTAG

Stellen Sie sich vor, Sie bekommen einen neuen Schlüssel. Er öffnet nicht nur Ihr Büro, sondern auch die Personalabteilung, die Buchhaltung und den Serverraum. Praktisch? Vielleicht. Aber auch beunruhigend. Denn was passiert, wenn dieser Schlüssel verloren geht?

Genauso verhält es sich mit Zugriffsrechten in unseren IT-Systemen. Manchmal haben Mitarbeitende Zugang zu weit mehr Daten und Anwendungen, als sie für ihre tägliche Arbeit benötigen. Das ist selten böse Absicht. Es passiert einfach. Über die Jahre. Schleichend. Und meistens unbemerkt.

Deshalb möchte ich Ihnen heute ein wichtiges Prinzip vorstellen. Es heißt Least Privilege. Auf Deutsch: das Prinzip der minimalen Berechtigung. Und es schützt nicht nur unser Unternehmen, sondern auch Sie persönlich.

Was bedeutet das Prinzip der minimalen Berechtigung?

Die Idee ist einfach. Jeder Mitarbeitende erhält nur die Zugriffsrechte, die er für seine Arbeit tatsächlich braucht. Nicht mehr und nicht weniger. Denken Sie an ein Hotel. Als Gast bekommen Sie eine Schlüsselkarte für Ihr Zimmer. Vielleicht noch für den Fitnessraum oder die Tiefgarage. Aber sicher nicht für alle 200 Zimmer im Haus. Das wäre absurd. Und gefährlich.

Genauso sollte es bei uns funktionieren. Sie haben Zugriff auf die Ordner Ihrer Abteilung. Auf die Anwendungen, die Sie nutzen. Auf die Kundendaten, die Sie betreuen. Aber eben nicht auf die Gehaltslisten der Personalabteilung oder die Vertragsunterlagen des Vorstands.

Mein Tipp:

Fragen Sie sich einmal ehrlich: Haben Sie Zugriff auf Bereiche, die Sie eigentlich gar nicht brauchen? Falls ja, ist das ein guter Moment, dies der IT zu melden.

Wie entsteht eigentlich dieser Wildwuchs bei Berechtigungen?

Die Antwort ist meistens: aus Hilfsbereitschaft und Zeitdruck. Niemand plant, ein Sicherheitsrisiko zu schaffen. Es passiert einfach.

>

> Ein klassisches Beispiel: Ihre Kollegin geht in Elternzeit. Sie übernehmen vorübergehend einige ihrer Aufgaben. Dafür brauchen Sie Zugriff auf bestimmte Ordner und Systeme. Die IT richtet das ein. Schnell und unkompliziert.

Dann kommt Ihre Kollegin zurück. Alles ist wieder beim Alten. Aber Ihre zusätzlichen Zugriffsrechte? Die bleiben. Niemand denkt daran, sie wieder zu entziehen. Warum auch? Es funktioniert ja.

Oder Sie wechseln die Abteilung. Neue Aufgaben, neue Systeme, neue Berechtigungen. Aber die alten Zugänge? Die werden selten gelöscht. Nach ein paar Jahren haben Sie Zugriff auf Bereiche, von denen Sie längst vergessen haben, dass es sie gibt.

Und dann gibt es noch den Klassiker: Der Kollege braucht dringend eine Datei, hat aber keinen Zugriff. Sie teilen ihm kurz Ihre Zugangsdaten mit. Nur dieses eine Mal. Aber aus einmal wird zweimal. Und plötzlich kennt die halbe Abteilung Ihr Passwort.

Mein Tipp:
Wenn Sie feststellen, dass Sie auf Bereiche zugreifen können, die mit Ihrer aktuellen Tätigkeit nichts mehr zu tun haben, melden Sie das. Das ist kein Petzen. Das ist verantwortungsvolles Handeln.

Was kann ich selbst tun?

Die gute Nachricht: Sie können aktiv dazu beitragen, dass unser Berechtigungsmanagement sauber bleibt. Hier sind einige konkrete Punkte:

- Hinterfragen Sie Ihre Zugriffsrechte. Schauen Sie sich gelegentlich an, auf welche Ordner und Systeme Sie Zugriff haben. Brauchen Sie das alles wirklich? Wenn nicht, melden Sie es.
- Geben Sie keine Zugangsdaten weiter. Auch nicht aus Hilfsbereitschaft. Auch nicht nur kurz. Wenn ein Kollege Zugriff auf ein System braucht, muss er einen eigenen Zugang bekommen. Alles andere ist ein Sicherheitsrisiko.
- Prüfen Sie geteilte Ordner. Wer hat eigentlich Zugriff auf den Teamordner? Sind dort noch ehemalige Kollegen berechtigt? Gibt es Unterordner, die eigentlich nicht für alle sichtbar sein sollten?
- Achten Sie auf E-Mail-Verteiler. Der große Verteiler mit 50 Empfängern mag praktisch sein. Aber muss wirklich jeder jede Information erhalten? Weniger ist oft mehr.
- Melden Sie Auffälligkeiten. Wenn Sie bemerken, dass Sie auf Daten zugreifen können, die Sie nichts angehen, sprechen Sie die IT an. Das ist kein Fehler, den Sie gemacht haben. Aber Sie können helfen, ihn zu beheben.

Geteilte Ordner und Verteiler – die unterschätzten Risiken

Lassen Sie uns über ein Thema sprechen, das in fast jedem Unternehmen für Kopfzerbrechen sorgt: geteilte Ordner und E-Mail-Verteiler.

Der Teamordner. Seit Jahren wächst er vor sich hin. Niemand weiß mehr genau, was drin ist. Und wer eigentlich alles darauf zugreifen kann. Irgendwann wurde der Praktikant freigeschaltet. Der ist längst weg, aber sein Zugang vermutlich nicht.

Oder der Projektordner. Am Anfang waren drei Personen beteiligt. Im Laufe des Projekts kamen immer mehr dazu. Am Ende hatten 20 Leute Zugriff. Das Projekt ist seit einem Jahr abgeschlossen. Der Ordner existiert noch. Mit allen Berechtigungen.

E-Mail-Verteiler sind ähnlich tückisch. Sie werden angelegt, wachsen über die Jahre und werden selten aktualisiert. Ehemalige Mitarbeitende sind noch drin. Neue fehlen. Und bei jedem Versand geht die Information an Personen, die sie vielleicht gar nicht erhalten sollten.

Mein Tipp:
Wenn Sie für einen geteilten Ordner oder einen Verteiler verantwortlich sind, nehmen Sie sich einmal im Jahr Zeit für eine Bestandsaufnahme. Wer hat Zugriff? Wer braucht ihn noch? Das dauert eine halbe Stunde und kann viele Probleme verhindern.

Warum weniger Rechte auch Sie selbst schützen

Vielleicht denken Sie jetzt: „Das klingt nach mehr Einschränkungen. Nach weniger Flexibilität. Nach mehr Bürokratie."

Aber lassen Sie mich einen anderen Blickwinkel anbieten. Eingeschränkte Zugriffsrechte schützen auch Sie persönlich.

Wenn Sie keinen Zugriff auf sensible Personaldaten haben, können Sie diese auch nicht versehentlich an den falschen Empfänger schicken. Wenn Sie nicht in der Buchhaltung arbeiten, können Sie keine Zahlungsdaten versehentlich löschen. Wenn Sie keinen Zugang zum Archiv haben, können Sie dort auch nichts

durcheinanderbringen. Mit anderen Worten: Weniger Zugriffsrechte bedeuten weniger Gelegenheiten für Fehler. Und damit weniger Risiko, selbst in eine unangenehme Situation zu geraten.

Ihre Checkliste für den Alltag

1. Prüfen Sie regelmäßig, auf welche Ordner und Systeme Sie Zugriff haben.	○
2. Melden Sie nicht mehr benötigte Zugriffsrechte an die IT.	○
3. Geben Sie niemals Ihre Zugangsdaten an Kollegen weiter.	○
4. Hinterfragen Sie die Berechtigungen in geteilten Ordnern.	○
5. Überprüfen Sie E-Mail-Verteiler auf Aktualität.	○
6. Teilen Sie Dokumente nur mit Personen, die sie wirklich benötigen.	○

Mein Tipp:
Betrachten Sie minimale Zugriffsrechte als das, was sie sind – ein Schutzmechanismus. Nicht nur für das Unternehmen, sondern auch für Sie.

Fazit: Gemeinsam für klare Verhältnisse

Das Prinzip der minimalen Berechtigung ist kein Misstrauensvotum. Es ist ein vernünftiger Ansatz, um Risiken zu minimieren. Für unser Unternehmen, für unsere Kunden und für jeden Einzelnen von uns.

Sie müssen kein IT-Experte sein, um dazu beizutragen. Es reicht, aufmerksam zu sein. Zugriffsrechte zu hinterfragen. Auffälligkeiten zu melden. Und Zugangsdaten für sich zu behalten.

Wenn Sie unsicher sind, ob Sie auf bestimmte Daten zugreifen sollten, fragen Sie nach. Lieber einmal zu viel gefragt als einmal zu wenig. Ich helfe Ihnen gerne weiter. (AH)

WUSSTEN SIE SCHON? WARUM DER PRAKTIKANT MANCHMAL MEHR SIEHT ALS DER ABTEILUNGSLEITER

Es klingt absurd, passiert aber regelmäßig. Ein Praktikant hat Zugriff auf vertrauliche Unternehmensdaten, während sein Abteilungsleiter diese gar nicht sehen kann. Wie kommt das?

Die Erklärung ist meistens banal: Der Praktikant wurde in der IT-Abteilung eingesetzt. Dort bekam er für ein kleines Projekt Administratorrechte. Das Projekt dauerte zwei Wochen. Die Rechte blieben.

Oder der Praktikant unterstützte die Personalabteilung bei einer Auswertung. Dafür brauchte er Zugriff auf Mitarbeiterdaten. Die Auswertung ist längst fertig. Der Zugriff besteht weiter.

Studien zeigen, dass in vielen Unternehmen mehr als 20 % aller Zugriffsrechte veraltet sind. Das bedeutet: Jeder fünfte Zugang existiert, obwohl er nicht mehr benötigt wird. Bei großen Unternehmen können das Tausende von unnötigen Berechtigungen sein.

Besonders kritisch wird es bei Mitarbeitenden, die häufig die Abteilung wechseln oder in verschiedenen Projekten arbeiten. Mit jedem Wechsel kommen neue Rechte hinzu. Aber die alten werden selten entfernt. Nach einigen Jahren haben diese Personen ein Sammelsurium an Zugängen, das niemand mehr überblickt.

Die gute Nachricht: Regelmäßige Überprüfungen der Zugriffsrechte, sogenannte Access Reviews, können dieses Problem lösen.

Dabei wird systematisch geprüft, ob jeder Zugang noch benötigt wird. Viele Unternehmen führen solche Reviews einmal im Jahr durch. Die besten machen es quartalsweise.

Und Sie können dabei helfen. Wenn Sie bei der nächsten Überprüfung gefragt werden, ob Sie bestimmte Zugänge noch brauchen, antworten Sie ehrlich. Jeder nicht mehr benötigte Zugang, der entfernt wird, macht unser Unternehmen ein Stück sicherer. (AH)

KURZFILM: KONTEXTMANIPULATION

Der Einsatz Künstlicher Intelligenz (KI) nimmt stetig zu. Neben bekannten KI-Systemen wie ChatGPT, Gemini, Grok, Le Chat und Copilot wird KI-Technologie auch zunehmend in Anwendungen integriert.

Wie bei nahezu jeder eingesetzten Technologie gibt es auch hier Personen, die versuchen, Ergebnisse zu ihren Gunsten zu beeinflussen. In diesem Video wollen wir uns die Prompt Injection ansehen oder in Deutsch – die Kontextmanipulation.

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 S. 1: madedee – AdobeStock.com, Druck: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 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