9/25

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER

VOM BÜRO-PC BIS ZUR CLOUD

Wo und wie werden Ihre Daten gespeichert und geschützt?

OPFER VON ANGRIFFEN

Plötzlich sind alle Daten eines Betriebs online einsehbar ... auch Ihre?

powered by
PRIVACYXPERTS

Daten unterwegs – und oft im Visier

Liebe Leserin, lieber Leser,

Daten sind das Rückgrat moderner Unternehmen – sie verbinden Prozesse, Abteilungen, Geräte und Menschen. Doch wie oft machen wir uns wirklich Gedanken darüber, wo sich unsere Daten eigentlich befinden, wenn wir eine E-Mail senden, ein Dokument speichern oder einen Cloud-Dienst nutzen? Im Beitrag „Sag mir, wo deine Daten sind – vom Büro-PC bis zur Cloud" werfen wir einen Blick hinter die Kulissen der täglichen Datenreise in Unternehmen. Denn wer die Wege der eigenen Informationen kennt, kann auch besser für Sicherheit sorgen.

Und Sicherheit ist dringlicher denn je. Der zweite Beitrag zeigt eindrücklich, was passiert, wenn dieser Schutz fehlt: Jeden Monat geraten Hunderte Unternehmen weltweit ins Visier von Ransomware-Gruppen – mit dramatischen Folgen. Wenn plötzlich alle internen Daten öffentlich einsehbar sind, ist der Schaden nicht nur finanziell, sondern auch reputativ oft kaum zu reparieren.

Unsere Beiträge zeigen: Zwischen harmloser Dateispeicherung und digitaler Katastrophe liegt nur ein schmaler Grat – und der lässt sich mit Wissen, Transparenz und klaren Sicherheitsstrategien besser absichern.

Bleiben Sie wachsam – und gut informiert.

Mit freundlichen Grüßen

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.

SAG MIR, WO DEINE DATEN SIND – VOM BÜRO-PC BIS ZUR CLOUD

Ein kleiner Blick hinter die Kulissen der Datenreise im Unternehmen

Sie tippen gerade einen Bericht, speichern ein Dokument auf dem Server oder schicken eine E-Mail an einen Kunden? Dann bewegen Sie sich – ohne es zu merken – mitten durch ein komplexes Datennetzwerk. Vom Arbeitsplatz-PC über mobile Endgeräte bis hin zur Cloud: Ihre Daten sind ständig unterwegs. Die spannende Frage ist dabei nicht nur wo, sondern auch wie sie gespeichert, verarbeitet und geschützt werden.

Hier lauern oft die unsichtbaren Risiken. Wer speichert was wo? Wer hat Zugriff? Und was passiert, wenn mal etwas schiefgeht? In diesem Artikel nehmen wir Sie mit auf eine kleine Entdeckungsreise durch die Stationen Ihrer Daten – vom Büro bis in die digitale Wolke. Und Sie bekommen konkrete Tipps, wie Sie mit wenigen Handgriffen die Sicherheit auf jeder Etappe verbessern können. Bringen Sie Ihr digitales Gepäck in Ordnung – wir zeigen Ihnen, wie.

Datenreise durch 5 Stationen. So schützen Sie unsere Daten

Station 1: Der Büroarbeitsplatz – die erste Haltestelle der Daten

Hier beginnt alles: Ein Angebot wird geschrieben, ein Formular geöffnet, ein Kundendatensatz aktualisiert. Ihr Arbeitsplatz ist die Startrampe für viele sensible Informationen.

Das sind die Risiken:

- Dateien werden lokal gespeichert und geraten so außerhalb zentraler Sicherheitsmaßnahmen.
- Bildschirme sind für Kollegen, Reinigungskräfte oder Besucher einsehbar.
- Offene USB-Anschlüsse oder private Geräte bringen Daten außer Kontrolle.

Was Sie tun können:

- Speichern Sie keine sensiblen Daten lokal auf dem Rechner – nutzen Sie zentrale Speicherorte.
- Sperren Sie Ihren Bildschirm, wenn Sie den Platz verlassen (Windows-Taste + L).
- Verwenden Sie nur zugelassene Geräte und keine privaten USB-Sticks.
- Achten Sie auf Papierausdrucke – was aus dem Drucker kommt, sollte nicht liegen bleiben.

Mein Tipp:
Ihr Rechner ist keine Schatztruhe – sensible Daten gehören in den Datensafe, nicht ins Schreibtischkästchen.

Station 2: Der Server – das Rückgrat der Datenorganisation

Ihre Daten landen im besten Fall auf einem Server und das ist gut so. Denn hier greifen Back-ups, Zugriffsrechte und andere Schutzmaßnahmen. Aber auch der beste Server nützt wenig, wenn er falsch genutzt wird.

Das sind die Risiken:

- Unübersichtliche Ordnerstrukturen führen dazu, dass sensible Daten falsch abgelegt werden.
- Fehlende Rechtevergabe sorgt für unnötige Zugriffe durch Unbefugte.
- Alte Daten bleiben ewig liegen – auch nach Mitarbeiterwechseln.

Was Sie tun können:

- Verwenden Sie klare, strukturierte Ordnerbezeichnungen – und keine kryptischen Abkürzungen.
- Achten Sie darauf, dass Daten nur in dafür vorgesehenen Bereichen gespeichert werden.
- Löschen oder archivieren Sie Daten, die nicht mehr gebraucht werden – aber bitte datenschutzgerecht.
- Melden Sie falsche Zugriffsrechte, wenn neue Kollegen kommen oder gehen.

Mein Tipp:
Der Server ist kein Dachboden – wer aufräumt, findet schneller, was er sucht. Und schützt es besser.

Station 3: Das mobile Gerät – Datenschutz zum Mitnehmen

Ob Laptop, Smartphone oder Tablet – mobile Endgeräte sind heute unverzichtbar. Aber unterwegs gelten eigene Regeln: Wer hier nicht aufpasst, lädt potenziell Fremde zur Datenparty ein.

Das sind die Risiken:

- Geräte gehen verloren oder werden gestohlen.
- Öffentliche WLANs laden zum Datenklau ein.
- Messenger-Apps oder private E-Mail-Accounts vermischen Berufliches und Privates.

>

> **Was Sie tun können:**
- Schützen Sie Geräte durch starke Bildschirmsperren und Verschlüsselung.
- Vermeiden Sie öffentliche WLANs ohne VPN – oder nutzen Sie mobile Daten.
- Speichern und versenden Sie keine dienstlichen Daten in WhatsApp, Signal oder privaten E-Mail-Konten.

Halten Sie die Geräte und Tools auf dem neuesten Stand.

Mein Tipp:
Mobile Geräte sind wie Zahnbürsten – man gibt sie nicht aus der Hand und nutzt sie nur für sich selbst.

Station 4: Die Cloud – praktisch, aber nicht wolkenlos

Cloud-Dienste sind bequem, ermöglichen Zusammenarbeit und sorgen für ortsunabhängigen Zugriff. Doch auch hier ist der Schutz der Daten kein Selbstläufer.

Das sind die Risiken:
- unklare Speicherorte (Drittlandtransfer!, unseriöse Anbieter usw.)
- unbekannte Back-up-Verfahren
- unklare Verschlüsselung
- Synchronisation mit privaten Geräten
- unzureichende Zugriffssteuerung bei geteilten Dokumenten

Was Sie tun können:
- Nutzen Sie nur freigegebene Cloud-Dienste unseres Unternehmens – keine privaten Dropbox- oder Google-Drives.
- Prüfen Sie Freigabelinks – wer darf was sehen oder bearbeiten? Arbeiten Sie nie aus Gewohnheit mit privaten Geräten oder unsicheren Apps.
- Löschen Sie Cloud-Daten, wenn sie nicht mehr gebraucht werden – nicht nur lokal.

Mein Tipp:
Clouds sind keine Wolken, die alles verschlucken – auch hier braucht es Ordnung und klare Grenzen.

Station 5: Die E-Mail – schnell verschickt, aber nicht immer sicher

Kaum ein Kommunikationsmittel wird so oft genutzt und so oft unterschätzt. Mit einem Klick geht eine E-Mail auf die Reise, manchmal mit mehr Informationen als beabsichtigt. Besonders kritisch wird es bei Anhängen, personenbezogenen Daten und falschen Empfängern.

Das sind die Risiken:
- falscher Adressat durch Autovervollständigung
- personenbezogene oder vertrauliche Daten unverschlüsselt versendet
- Anhänge mit sensiblen Informationen weitergeleitet oder gespeichert
- Mails mit Kundendaten im Papierkorb statt im Archiv

Was Sie tun können:
- Prüfen Sie jeden Empfänger vor dem Absenden – besonders bei „Allen antworten".
- Verwenden Sie bei sensiblen Inhalten eine Verschlüsselung oder sichere Portale.
- Hängen Sie keine personenbezogenen Daten ungeschützt an.
- Löschen Sie E-Mails nicht einfach, wenn sie geschäftsrelevant sind – sondern archivieren Sie diese datenschutzkonform.
- Vorsicht bei Weiterleitungen: Fragen Sie sich, ob der neue Empfänger wirklich alle Inhalte sehen darf.

Mein Tipp:
Eine unverschlüsselte bzw. ungeschützte E-Mail ist wie eine Postkarte – jeder auf dem Weg könnte mitlesen. Vertrauliches gehört in den Umschlag.

Angekommen – und jetzt? Ihre Rolle als Datenschützer im Alltag

Sie sehen, dass die Reise Ihrer Daten abwechslungsreich ist. An jeder Station liegt es auch an Ihnen, wie sicher die Route verläuft. Dabei braucht es keine komplizierten Programme oder stundenlange Schulungen. Meist sind es kleine Handgriffe und bewusste Entscheidungen, die den Unterschied machen.

Ob am Schreibtisch, unterwegs oder in der Cloud – jede Datei mit vertraulichen Informationen hat ein Recht auf Schutz. Und Sie als Mitarbeitende sind die wichtigste Schnittstelle zwischen Technik, Organisation und gesunder Vorsicht.

Nutzen Sie die Tipps aus diesem Artikel, um die nächste Datenschutzpanne zu verhindern, bevor sie passiert. Melden Sie sich, wenn Sie unsichere Speicherorte entdecken oder Fragen haben. Und denken Sie daran:

Datenschutz ist kein Ziel – sondern eine Reise, die jeden Tag neu beginnt. Und das Beste daran: Sie sitzen selbst am Steuer. (AH)

PLÖTZLICH SIND ALLE DATEN EINES UNTERNEHMENS ONLINE EINSEHBAR … AUCH IHRE?

Ein Blick etwa auf ransomware.live zeigt: Jeden Tag werden Organisationen weltweit Opfer von Angriffen von Ransomware-Gruppen. Laut dem Portal wurden allein im Juli 2025 rund 500 Organisationen erfolgreich angegriffen. Bis Juli 2025 verzeichnet das Portal etwas über 4.500 Opfer für das aktuelle Jahr.

Verschlüsselung und Veröffentlichung

Diese kriminellen Banden verschlüsseln aber oftmals nicht mehr „nur" die Daten ihrer Opfer. Da viele Unternehmen ihre Datensicherungen angepasst haben, veröffentlichen einige Ransomware-Gruppen die Daten ihrer Opfer, wenn diese kein „Lösegeld" bezahlen. Um den Druck auf die Verantwortlichen zu erhöhen, wird die Veröffentlichung der Daten teilweise sogar mit einem Countdown versehen.

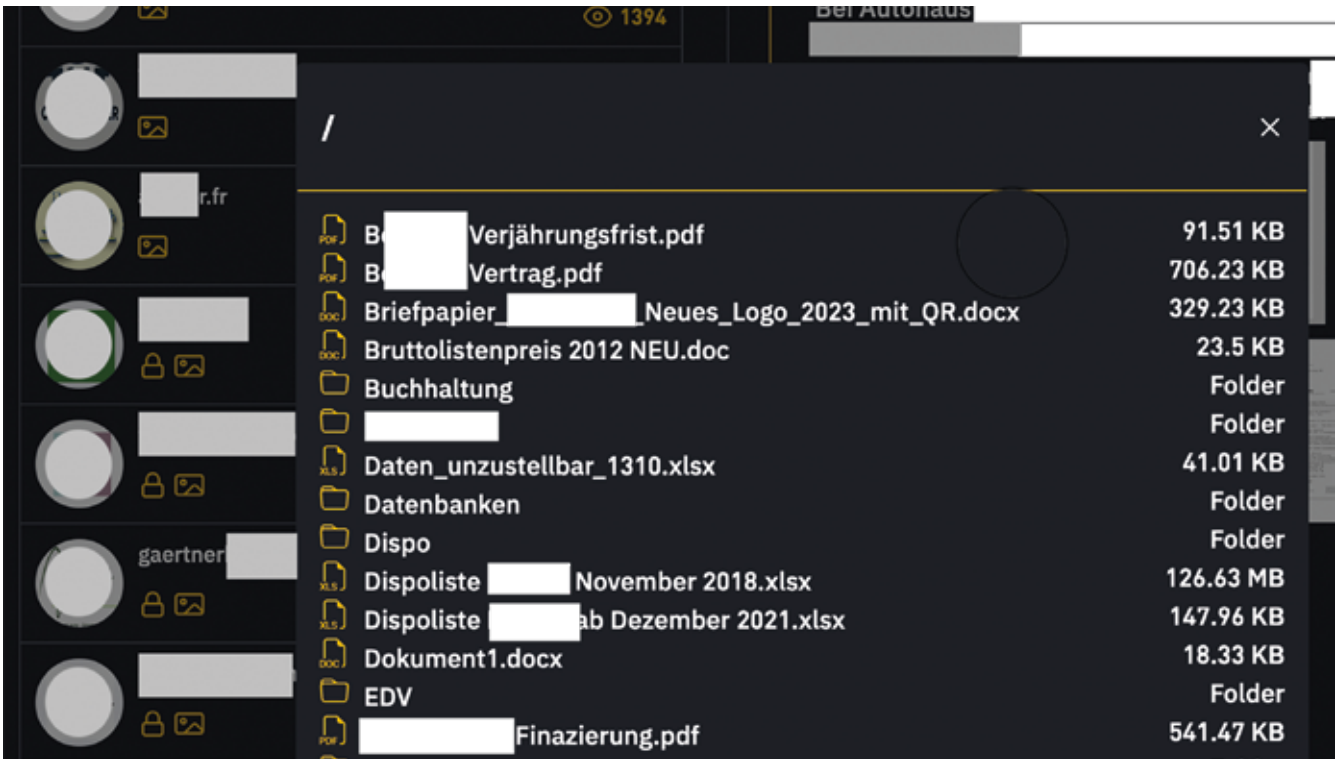
Daten, die es längst nicht mehr geben sollte

Wird bekannt, dass etwa die Daten des zentralen Dateiservers kopiert wurden, steigt der Druck zusätzlich. Denn vielen Verantwortlichen und Beschäftigten ist häufig bekannt, dass die zentrale Datenablage oft auch ein riesiger Datenfriedhof ist und es etwa aufgrund gesetzlicher Vorgaben, wie der Datenschutz-Grundverordnung, viele dieser Dateien nicht mehr geben dürfte. Aber neben fehlender Zeit, um die Verzeichnisse zu bereinigen, haben viele Verantwortliche und Betroffene die Sorge, dass sie die Daten irgendwann noch einmal brauchen könnten.

So lagern dann oftmals Gigabyte an Daten in Hunderten oder Tausenden Verzeichnissen, Dokumenten, eingescannten Dateien und „Excel-Listen" mit sensiblen Mitarbeiter-, Kunden- oder Geschäftsinformationen. Nicht selten finden sich in den veröffentlichten Verzeichnissen auch „Passwort-Listen" oder die Dokumentation der IT-Infrastruktur.

Die Konsequenzen für die betroffenen Unternehmen

Finden die Interessierten in den veröffentlichten Daten Informationen, wie etwa Zugangsdaten, können diese verwendet werden, um das Unternehmen zusätzlich anzugreifen. So wäre es etwa denkbar, dass



Screenshot der Webseite einer Ransomware-Gruppe mit veröffentlichten Daten eines deutschen Opfers >

> die gefundenen Zugangsdaten für Microsoft 365, Einkaufsplattform oder Social-Media-Präsenz genutzt werden, um sich dort einzuloggen. Nach einem Passwortwechsel durch den Angreifer verliert das Unternehmen dann zumindest zeitweise den Zugriff darauf. Und das, während viele noch mit der Aufrechterhaltung des Notbetriebs und der Wiederherstellung beschäftigt sind.

Meldung an Aufsichtsbehörde, Betroffene und Vertragspartner

Sind in den Verzeichnissen sensible personenbezogene Daten vorhanden, was vielfach der Fall ist, muss der Vorfall regelmäßig spätestens innerhalb von 72 Stunden an die Datenschutz-Aufsichtsbehörde gemeldet werden. Je nach Risiko für die betroffenen Personen müssen auch diese über den Vorfall informiert werden.

Ist das Unternehmen als Auftragsverarbeiter aktiv oder hat es entsprechende vertragliche Vereinbarungen, müssen auch die Auftraggeber bzw. Vertragspartner über den Vorfall informiert werden. In einigen Branchen und Organisationen gibt es zudem weitere Meldepflichten, welche berücksichtigt werden müssen.

Schadensersatzforderungen und finanzielle Verluste bis hin zur Insolvenz

Sind sensible personenbezogene Daten von der Ransomware-Attacke und insbesondere der Veröffentlichung betroffen, besteht darüber hinaus das Risiko, dass betroffene Personen Schadensersatz verlangen oder einklagen.

Aber auch wenn keine Person Schadensersatz verlangt und kein „Lösegeld“ bezahlt wird, dürften die meisten Unternehmen hohe Kosten für die Wiederherstellung der IT und die häufig verbundene Betriebsunterbrechung haben. Immer wieder gibt es sogar Medienberichte über Insolvenzen infolge von entsprechenden Cyberangriffen.

Eintritts- und Schadensminimierung dank Ihrer Mithilfe

Damit es möglichst gar nicht erst zu einem Angriff kommt, versucht Ihre IT-Abteilung sicherlich, Ihre Systeme so gut wie möglich abzusichern. Eine 100%ige Sicherheit wird aber selten erreichbar sein. Denn je strenger die technischen Sicherheitsmaßnahmen, desto mehr wird auch oftmals die alltägliche Arbeit beeinflusst.

Zudem lassen sich in der Praxis auch nicht immer alle möglichen Sicherheitsrisiken durch technische Maßnahmen absichern. Deswegen ergreifen Unternehmen sogenannte organisatorische Maßnahmen. Darunter fällt die Festlegung der Zuständigkeiten und Abläufe, aber auch Richtlinien, Arbeitsanweisungen und Ähnliches. Sofern Ihnen diese nicht bekannt sind, sollten Sie sie erfragen.

Technisches Hacking und Social Engineering

Es gibt Ransomware-Attacken, bei denen die Angreifer sich durch Hacking Zugriff von außen verschafft und zuerst Daten kopiert und dann verschlüsselt haben. Wohl sehr viel häufiger aber kam Social Engineering zum Einsatz, also Manipulation. Die Angreifer versuchen, einen Beschäftigten so zu manipulieren, dass dieser eine Schadsoftware in einer verseuchten Datei öffnet oder den Kriminellen einen Fernwartungszugang ermöglicht.

Vorsicht bei E-Mails, Anrufen und Warnmeldungen

Die Variationen der Manipulationsversuche sind vielfältig. Mal senden die Angreifer E-Mails mit Schadsoftware, ein anderes Mal geben sie sich als Techniker oder Support-Mitarbeiter aus und bieten ihre Hilfe an.

Vielfach erfolgt der Angriff weiterhin per E-Mail. Damit E-Mails möglichst nicht durch eine Schutzsoftware herausgefiltert werden, senden die Angreifer statt Dateien auch Links zu Onlinespeichern, in denen die Datei, etwa eine angebliche Rechnung oder Bewerbung, gespeichert ist.

Da viele Unternehmen E-Mails absichern, nutzen Angreifer zunehmend auch alternative Kommunikationswege und versenden z. B. Chat-Nachrichten via Microsoft Teams. Ende letzten Jahres wurde etwa berichtet, dass die Gruppe „Black Basta“ zuerst einzelne Benutzer mit Spam-Mails überhäuft, um dann per Microsoft Teams Chat Hilfe anzubieten.

Bitte seien Sie bei derartigen Kontaktaufforderungen sehr vorsichtig. Es wird erwartet, dass entsprechende Nachrichten und insbesondere E-Mails durch den Einsatz von künstlicher Intelligenz zunehmend schwieriger zu erkennen sein werden. Bestenfalls bringen Sie bereits im Vorfeld in Erfahrung, an wen Sie sich bei Unsicherheiten bezüglich verdächtiger Nachrichten und Kontaktaufnahmen wenden können.

Schadensminimierung durch schnelle Reaktion

Zudem sollten Sie im Vorfeld in Erfahrung bringen, an wen Sie sich in Ihrem Unternehmen wenden können, wenn Sie den Verdacht haben, doch auf einen Kriminellen hereingefallen zu sein, und ob es ggf. interne Handlungsvorgaben gibt. Denn im „Fall der Fälle" kommt es auf jede Minute an!

Wichtig: Nicht immer ist direkt erkennbar, dass etwa eine Schadsoftware-Attacke erfolgreich war! Eventuell passiert nach dem Öffnen einer entsprechenden Datei augenscheinlich nichts Außergewöhnliches. Im Hintergrund werden jedoch Dateien an die Angreifer übertragen und weitere Geräte im Netzwerk infiziert.

Durch eine schnelle Reaktion kann ein Zugriff der Schadsoftware auf andere Geräte oder ein Upload der Daten verhindert oder zumindest begrenzt werden.

In einigen Unternehmen gibt es deshalb etwa die Vorgabe, bei Verdacht auf einen Sicherheitsvorfall die Netzwerkverbindung sofort zu trennen.

Schadensminimierung durch Datenbereinigung

Eine wichtige Maßnahme kann auch eine Datenbereinigung sein. Dies betrifft sowohl Dateien als auch E-Mails und Datenbanken. Oftmals sind die Daten sogar mehrfach vorhanden. Im schlimmsten Fall befindet sich etwa eine Rechnung im Buchhaltungsprogramm, in einem digitalen Archiv, als PDF in einem Verzeichnis, nach Empfang oder Versand noch im E-Mail-Programm und im dazugehörigen E-Mail-Archiv.

Einige Unternehmen haben sich der Thematik angenommen und einen Datenlebenszyklus (Data Lifecycle Management) etabliert. In diesen Unternehmen werden etwa Dateien in spezifischen Verzeichnissen oder mit bestimmten Labels automatisch gelöscht.

Zudem speichern einige Unternehmen Daten mit einer höheren Sensibilität in speziellen Anwendungen oder selbst verschlüsselten Verzeichnissen. Damit soll auch verhindert oder zumindest erschwert werden, dass diese Daten nach einer erfolgreichen Ransomware-Attacke lesbar veröffentlicht werden.

Vorbeugen kann wenigstens den Schaden begrenzen

In Gesprächen mit Verantwortlichen hört man oft, dass es keine Frage sei, ob, sondern wann ein erfolgreicher Hacking-Angriff geschehe. Damit man dann zumindest den Schaden minimiert, sollte jedem im Unternehmen bekannt sein, wer die Ansprechpartner für diesen Fall sind. Zudem sollten möglichst nur Daten verarbeitet werden, die wirklich benötigt werden – und zwar so sicher wie möglich. (ST)

WUSSTEN SIE SCHON? SIND IHRE DATEN WIRKLICH NÜTZLICH?

Auf IT-Systemen von Unternehmen lagern oft riesige Datenmengen – verteilt auf zentrale File-Server, persönliche Verzeichnisse und unterschiedlichste Anwendungen. Hunderte Verzeichnisse, Tausende Dateien, Millionen Datensätze. Immer wieder finden sich redundante, veraltete oder längst irrelevante Daten. Untersuchungen, wie die Adress-Studie der Deutschen Post, zeigen auf, dass – je nach Branche – selbst viele Adressdaten veraltet sind.

Dabei liegt genau hier ein entscheidender Hebel für die Zukunft: Wer weiß, welche Daten wo gespeichert sind und wozu sie genutzt werden, kann sie nicht nur sicherer verarbeiten, sondern auch echten Mehrwert schaffen – etwa für Auswertungen, Automatisierungen oder auch den Einsatz von künstlicher Intelligenz.

Datenqualität ist die Voraussetzung für Digitalisierung. Wer seine Datenbestände aktiv pflegt, profitiert häufig durch weniger Risiko und mehr Nutzen. In einigen Unternehmen wird die Expertise von Datenschutzbeauftragten auch hierfür aktiv genutzt. Denn Ihr Datenschutzbeauftragter weiß, wie mithilfe von Pseudonymisierung personenbezogene Daten geschützt werden können. Zudem kann er aufzeigen, wie mit einer korrekten Anonymisierung am Ende die Datenschutzgesetze gar nicht mehr zur Anwendung kommen. Dabei wird das Gesetz nicht umgangen, sondern bestmöglich erfüllt. (ST)

SICHERN SIE IHR UNTERNEHMEN VOR ANGREIFERN

Kriminelle handeln meist wie Unternehmen: ob allein, im Team oder als Organisation – ihr Ziel ist fast immer Geld. Sie erpressen, verkaufen Daten oder bieten illegale Dienstleistungen im Dark Web an.

Sie schützen Ihr Unternehmen mit Technik und klaren Regeln (Richtlinien, Schulungen). Doch der wichtigste Schutzfaktor sind die Menschen selbst: Werden Sie zur **Human Firewall** – und machen Sie es Angreifern schwer. In unserem Video zeigen wir Ihnen, wie das geht!

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: j-mel – Adobe-Stock.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