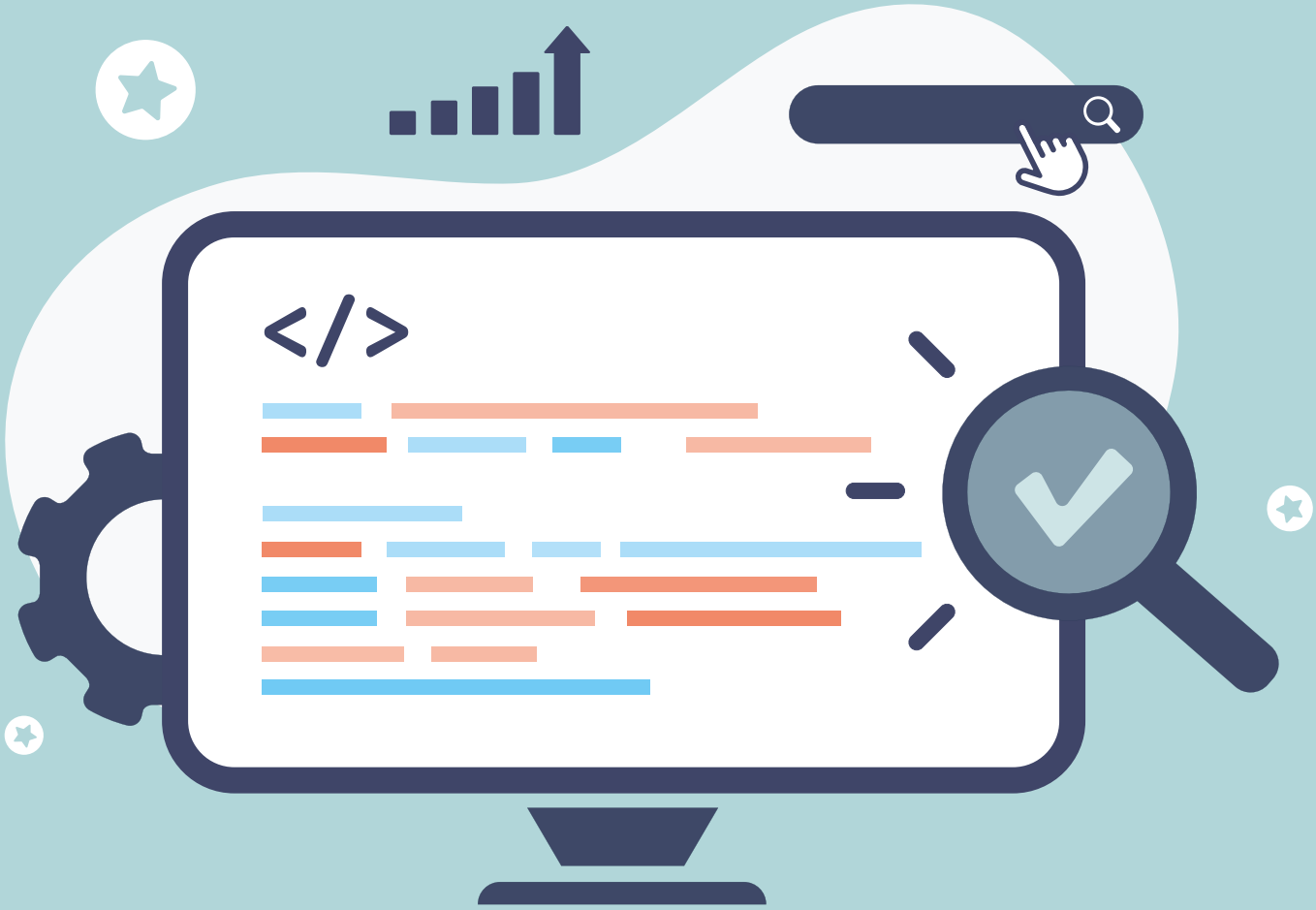
10/25

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER



METADATEN

... und Änderungen: Gerne übersehen, immer wieder peinlich!

VISHING

„Achtung, hier spricht der falsche Chef!“ Vorsicht vor Phishing per Telefon!

powered by
PRIVACYXPERTS

Wenn Daten zu viel verraten – und Stimmen zu überzeugend klingen

Liebe Leserinnen, liebe Leser,

die größten Risiken in der digitalen Welt sind oft nicht spektakulär – sie sind still, beiläufig und werden zu spät bemerkt. Zwei Beispiele dafür zeigen wir Ihnen in dieser Ausgabe.

Zum einen geht es um Metadaten und Änderungsvermerke – unsichtbare, aber äußerst verräterische Informationen in Dateien. Sie sind technisch gesehen nur „Beifang", aber sie können vertrauliche Daten preisgeben, für Angriffe genutzt werden oder schlicht peinlich sein. Noch immer werden diese digitalen Fußspuren zu oft übersehen – mit Folgen für Sicherheit, Datenschutz und Reputation.

Zum anderen werfen wir einen Blick auf eine besonders perfide Form des Social Engineering: Vishing – Telefonbetrug mit psychologischer Finesse. Keine Hackertechnik, keine Schadsoftware – nur eine gut gespielte Rolle, ein bisschen Druck und der richtige Moment. Und schon geben Mitarbeitende mehr preis als ihnen lieb ist.

Beide Themen zeigen: Es braucht keinen digitalen Großangriff, um sensible Informationen abzugreifen. Oft reichen ein unbedachter Klick oder ein scheinbar harmloses Telefonat.

In diesem Sinne wünschen wir Ihnen eine aufmerksame Lektüre. Bleiben Sie wachsam.

Mit freundlichen Grüßen
Ihr Redaktionsteam von „Privacy@Work"

PS: Als kleine Aufmerksamkeit liegt dieser Ausgabe ein Jahreskalender bei, der Ihnen hilft, den Überblick über Termine und Projekte zu behalten. Auch für die Urlaubsplanung ist er praktisch – alle Ferienzeiten der Bundesländer sind darin übersichtlich aufgeführt.

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.

METADATEN UND ÄNDERUNGEN: GERNE ÜBERSEHEN, IMMER WIEDER PEINLICH!

Sicherheits- und Datenschutzvorfälle durch Metadaten oder erkennbare Datenänderungen werden nicht häufig öffentlich gemacht. Das führt aber auch im Jahr 2025 dazu, dass viele von den Gefahren nicht wissen. In diesem Beitrag erfahren Sie, was Metadaten sind, wie diese und Änderungsvermerke in der Praxis zu Problemen führen und wie Sie diese vermeiden können.

Das sind Metadaten

Wenn wir von Daten sprechen, denken wir meistens an den Inhalt einer Datei, etwa PDF-, Word- oder Excel-Datei, oder einer Datenbank, den wir über ein Programm oder einen Browser aufrufen können. Metadaten sind zusätzliche Informationen über diese Daten.

So enthalten etwa PDF-, Word- und Excel-Dateien Angaben zum Autor, Datum der Erstellung und Änderung. Metadaten finden sich aber auch z. B. in E-Mails und bei der Internetnutzung etwa im Header einer E-Mail oder im Protokoll der Internetnutzung die IP-Adressen und Zeitstempel.

Nicht übersehen: Versionen und Kommentare

In diesem Zusammenhang sollten auch Dateiversionen, Änderungen und Kommentare in Dateien nicht übersehen werden. In einigen Anwendungen, wie etwa Word und Excel, können neben dem eigentlichen Inhalt und den Metadaten auch Datenänderungen und Kommentare enthalten sein. Dies sind zwar keine klassischen Metadaten. Aber diese Daten werden – je nach Einstellung der Ansicht – oft nicht direkt in der Datei angezeigt und technisch eher wie Metadaten behandelt. Wichtig ist jedoch, dass diese Daten – ähnlich wie Metadaten – auch übersehen werden und Probleme bereiten können.

Achtung: Beim Einsatz von Microsoft-Büroprogrammen in Verbindung mit SharePoint oder OneDrive (etwa Microsoft 365) gibt es den Versionsverlauf und – bei entsprechender Einstellung – die Dokumentation der Änderungen. Der Versionsverlauf wird in SharePoint dokumentiert und ist nicht in der Datei enthalten. Wird die Datei allerdings per Link geteilt und hat die empfangende Person die entsprechenden Rechte, kann diese unter Umständen auf die Versionen zugreifen. Außerdem: Ist die Dokumentation der Änderungen aktiviert, werden diese „in der Datei“ gespeichert – ebenso Kommentare.

Risiko 1: Änderungsverläufe bei Office-Dokumenten

Manchmal werden etwa Verträge und Angebote auch als Word-Datei hin und her geschickt. In diesen Fällen sehen die jeweiligen Empfänger teilweise nicht nur die entsprechenden Metadaten, wie welche Person diese zu welcher Zeit bearbeitet hat. Immer wieder kommt es vor, dass Absender Änderungen durch die Anwendung dokumentieren lassen und vergessen, die Änderungsvermerke zu löschen. Damit sind etwa vorherige Preise, Gehälter oder Formulierungen aufrufbar. Solche Pannen werden zwar selten öffentlich dokumentiert, sind aber in der Unternehmenspraxis durchaus bekannt.

Im schlimmsten Fall erhält somit ein Interessent einen Vertrag oder ein Angebot im Word-Format. Über das Einblenden der durchgeführten Änderungen könnte er einsehen, welche Daten im Vorfeld in der Datei enthalten waren, also etwa ein anderer Interessent und dessen Preis.

Im Personalbereich könnte ein Bewerber im ungünstigsten Fall die Angaben für andere Kollegen sehen, für welche die Datei vorher überarbeitet wurde.

Risiko 2: EXIF-Daten in Fotos

Wenn Sie etwa Fotos mit Ihrem Smartphone erstellen, werden üblicherweise weitere Angaben in den Metadaten der Fotos hinterlegt. Darunter fallen häufig das genutzte Gerät, Datum und Uhrzeit und der Standort (GPS-Daten). Bei einigen Geräten wird nach der Fotoerstellung auch hinterlegt, was auf dem Foto zu sehen ist. Das kann je nach Situation durchaus kritisch sein. Denn nicht immer soll bekannt sein, wo sich etwa ein Rechenzentrum oder Lager mit wertvollen Gütern befindet.

Bitte denken Sie auch beim privaten Versand oder der Nutzung von Bildern, etwa auf Dating- oder Verkaufsplattformen, daran, dass über die Bilder möglicherweise mehr verraten wird als gewollt!

>

> Risiko 3: Wie Angreifer Metadaten nutzen können

Metadaten können von Kriminellen auch für Angriffe genutzt werden. Einerseits können durch Metadaten etwa die verwendeten Anwendungen bekannt werden, welche für die Erstellung eingesetzt wurden. Die Kriminellen können dann prüfen, ob für die Anwendung eine Sicherheitslücke vorhanden ist, und diese ausnutzen.

Die Metadaten können aber auch für Social-Engineering-Angriffe verwendet werden. Stellen Sie sich bitte vor, dass eine Führungskraft im Ausland einen neuen Standort für das Unternehmen aufbauen möchte. Diese veröffentlicht Bilder vom zukünftigen Standort. Durch die Informationen aus dem Posting bzw. Beitrag und den Standortdaten aus dem Foto könnten Kriminelle ihren Angriff sehr realistisch gestalten und etwa „als Behörde“ Geld für das konkrete Grundstück fordern.

Datenschutz, Reputation und Sicherheit

Versehentlich gesendete bzw. veröffentlichte Metadaten können für Unternehmen gefährlich sein. So können etwa personenbezogene Daten versehentlich an Dritte weitergegeben werden, z. B. wenn eine Word-Arbeitsvertrags-Datei immer nur überarbeitet und ohne weitere Sicherheitsmaßnahmen an Bewerber gesendet wird.

Aber auch wenn keine Person von der versehentlichen Weitergabe betroffen ist, können etwa einsehbare Kommentare oder vorherige Preise der Reputation des Unternehmens schaden.

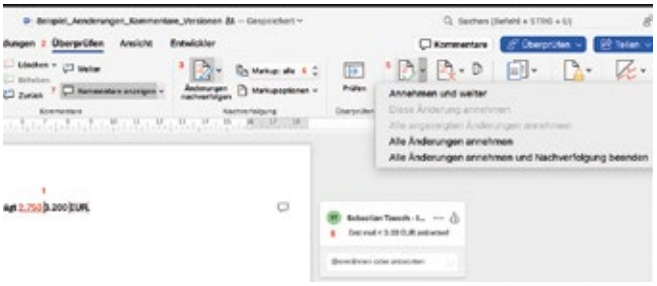
Zudem können Metadaten z. B. die internen Anwendungen und Zuständigkeiten verraten und von Kriminellen für technische oder Social-Engineering-Angriffe ausgenutzt werden.

Metadaten entfernen

Zum Schutz sollten die Metadaten vor dem entsprechenden Versand bzw. der Veröffentlichung entfernt werden. Das geht teilweise direkt über die jeweiligen Anwendungen.

Microsoft Word, Excel und PowerPoint

Bei den Windows-Versionen der jeweiligen Programme können Sie die Metadaten nach einer Prüfung löschen lassen. Rufen Sie dazu das Menü „Datei“ → „Informationen“ → „Auf Probleme prüfen“ → „Dokument prüfen“ auf. Nach der Prüfung können auf einen Klick auf „Alle entfernen“ die Metadaten gelöscht werden.



Änderungen und Kommentare in Word löschen

Die Änderungen in der Datei (Punkt 1) können Sie über das Menü „Überprüfen“ (Punkt 2) aufrufen. Dort können Sie über „Änderungen nachverfolgen“ (Punkt 3) einstellen, ob alle Änderungen protokolliert werden oder nicht.

Um die Änderungen zu sehen, muss „Markup“ entsprechend angepasst werden (Punkt 4). Über „Änderungen“ (Punkt 5) können Sie die Änderungen einzeln oder gesamt übernehmen, sodass im Anschluss auch nur noch der überarbeitete Text vorhanden ist.

Die möglichen Kommentare (Punkt 6) lassen sich per Menü einblenden (Punkt 7) und löschen (Punkt 8).

Bei Einsatz von OneDrive und SharePoint sowie der Versionierung können Sie – je nach Berechtigung – die vorherigen Versionen der Datei löschen. Die Versionen lassen sich etwa nach einem Rechtsklick auf die Datei und Auswahl „Versionsverlauf“ aufrufen. Hier finden Sie bei entsprechender Berechtigung auch die Möglichkeit, die alten Versionen zu löschen.

Eine weitere Möglichkeit ist, Dokumente vor der Weitergabe in eine PDF zu überführen und diese zu übermitteln. Vorsichtshalber sollte die erzeugte PDF-Datei auf mögliche Metadaten überprüft werden. Denn je nach PDF-Erstellung bleiben Metadaten erhalten oder werden bei der PDF-Erstellung hinterlegt.

Metadaten in Windows-Dateieigenschaften entfernen (mit Einschränkung)

In Windows können Sie einige Metadaten direkt einsehen und entfernen: Rechtsklick auf die Datei → „Eigenschaften“ → Register „Details“ →„Eigenschaften und persönliche Informationen entfernen“. Dies ist eine

einfache Möglichkeit, um offensichtliche Metadaten – wie Autor oder Erstellungsdatum – zu löschen.

Wichtig: Diese Funktion entfernt nur bestimmte Standardmetadaten. Eingebettete Informationen – wie Änderungsverläufe in Office-Dokumenten oder Kommentare in PDFs – bleiben bestehen. Nutzen Sie daher zusätzlich die Dokumentprüfung in Office-Programmen und prüfen Sie PDFs oder Bilder mit geeigneten Tools, um wirklich alle sensiblen Daten zu entfernen.

Für das Löschen von EXIF-Daten gibt es eigene Tools, wie etwa ExifTool.

Mein Fazit

Metadaten, protokollierte Änderungen und Kommentare werden leider oft übersehen und verraten dann mehr als gewünscht. Diese teilweise sensiblen Daten lassen sich jedoch mit wenigen Klicks in den jeweiligen Anwendungen zuverlässig entfernen. (ST)

„ACHTUNG, HIER SPRICHT DER FALSCHE CHEF!“

Stellen Sie sich vor, Ihr Telefon klingelt, und am anderen Ende meldet sich jemand freundlich, aber bestimmt: „Hier ist die IT. Wir brauchen sofort Ihr Passwort.“ Oder noch besser: „Guten Tag, ich rufe im Auftrag der Geschäftsführung an. Bitte überweisen Sie direkt 10.000 € – es ist sehr dringend.“ Klingt absurd? Leider nicht. Solche Anrufe gehören inzwischen zu den beliebtesten Maschen von Kriminellen.

Diese Art des Angriffs nennt sich Vishing (Voice Phishing) – also Phishing per Telefon. Dabei setzen die Angreifer auf psychologischen Druck, freundliches Auftreten oder falsche Autorität. Ziel ist es immer, Sie am Telefon so unter Druck zu setzen, dass Sie vertrauliche Informationen herausgeben oder gar Geld anweisen.

Wir zeigen Ihnen, wie Sie mit ein paar einfachen Regeln solche Anrufe schnell entlarven und souverän reagieren können.

4 Tricks der Anrufer – so werden die Opfer aufs Glatteis geführt

Beim Vishing geht es selten um technische Raffinesse. Die Angreifer setzen auf etwas viel Einfacheres: menschliche Reflexe (Social Engineering). Freundlichkeit, Hilfsbereitschaft, Gehorsam gegenüber Vorgesetzten oder die Angst, etwas falsch zu machen. Genau das nutzen sie am Telefon aus.

Nachfolgend haben wir ein paar typische Szenen aufgeführt, die Sie vielleicht kennen – oder die Ihnen zumindest verdächtig vorkommen sollten:

1. Der vermeintliche IT-Helfer

„Guten Tag, hier ist Ihr IT-Support. Wir haben ein Problem mit Ihrem Konto. Nennen Sie uns bitte schnell Ihr Passwort, damit wir das sofort beheben können.“

Mein Tipp:
Kein seriöser IT-Kollege fragt je nach einem Passwort.

2. Der Chef in Eile

„Ich bin gerade im Ausland und habe eine vertrauliche Überweisung, die sofort erledigt werden muss. Bitte handeln Sie ohne Rückfrage – es eilt!“

Mein Tipp:
Genau hier sollen Sie NICHT gehorchen, sondern Rücksprache halten.

3. Der Gewinnversprecher

„Sie haben ein Preisausschreiben gewonnen. Bitte geben Sie uns Ihre persönlichen Daten, um den Gewinn überweisen zu können.“

Mein Tipp:
Seriöse Veranstalter rufen nicht mit solchen Forderungen an.

4. Der vermeintliche Kunde

„Ich brauche dringend eine Auskunft über meinen Vertrag. Sagen Sie mir doch bitte meine Kundennummer.“

Mein Tipp:
Hier sollen interne Daten abgegriffen werden, die vertraulich bleiben müssen.

So funktioniert Vishing im echten Alltag

Man kann es sich wie ein kleines Theaterstück am Telefon vorstellen. Die Täter schreiben ein Drehbuch, >

> wählen eine passende Rolle und spielen dann sehr überzeugend. Sie setzen auf zwei starke Gefühle bei Ihnen als Mitarbeitende. Erstens auf Angst vor Fehlern oder Konsequenzen. Zweitens auf Vertrautheit durch scheinbar interne Details und freundlichen Ton. Diese Mischung aus Druck und Nähe bringt viele dazu, spontan zu handeln.

1. Vorbereitung

Die Täter sammeln offene Informationen über unser Unternehmen und über einzelne Personen. Quellen sind Firmenwebseiten, Pressemitteilungen, Stellenanzeigen, soziale Netzwerke und oft auch frühere Datenlecks. Namen von Vorgesetzten, interne Begriffe, Projekte oder Kundennummern sind Gold wert. Je mehr echte Details, desto glaubwürdiger wirkt der Anruf.

2. Rollenwahl

Aus den Infos bauen die Täter eine Figur, die zu Ihnen passt. IT-Kollege, Kollegin aus der Buchhaltung, Servicedienstleister, Kunde, Paketdienst oder sogar Geschäftsführung. Die Rolle entscheidet darüber, welche Fragen erlaubt wirken und wie viel Autorität mitschwingt.

3. Kulisse aufbauen

Damit alles echt klingt, wird die Anruferkennung oft gefälscht. Auf dem Display steht dann eine interne Durchwahl oder eine bekannte Servicenummer. Dazu kommen akustische Details. Hintergrundgeräusche eines Großraumbüros, Tippgeräusche, kurze Warteschleife. Das erhöht die Glaubwürdigkeit.

4. Warm-up und Vertrautheit

Der Einstieg ist freundlich und beiläufig. Es fallen vertraute Namen und Projekte. Gern kommt ein Kompliment oder ein Dankeschön. Das soll Nähe schaffen. Beispiel: „Wir hatten doch gestern die Störung im Kundenportal. Danke, dass Sie da so schnell reagiert haben. Jetzt brauchen wir nur noch eine kurze Rückbestätigung."

5. Druckphase

Sobald Sie innerlich nicken, dreht der Ton auf Tempo. Es wird eilig. Systeme sind angeblich gesperrt. Fristen laufen ab. Der Kunde wartet. Die Geschäftsführung erwartet sofortige Erledigung. Hier wirken die Hebel Autorität, Dringlichkeit und Knappheit. Genau in dieser Phase sollen Sie nicht mehr nachdenken, sondern machen.

6. Die Forderung

Jetzt kommt die eigentliche Bitte. Zugangsdaten, Einmalcodes, Bestätigung per Link, Freigabe einer Zahlung, Preisgabe von Kundendaten. Die Forderung wird als klein und harmlos verkauft. Nur schnell, es ist bloß eine Formalität, dauert keine Minute. Manche Täter bieten sogar Hilfe an, z. B.: „Ich bleibe kurz dran, dann ist das Thema für Sie erledigt."

7. Absicherung gegen Rückfragen

Falls Sie zögern, wird nachgelegt. Die Täter nennen eine angebliche interne Ticketnummer, leiten an einen scheinbaren Kollegen weiter oder schicken parallel eine Mail mit Firmenlogo. Gern wird ein Rückruf aktiv verhindert. Leider sind gerade alle Leitungen belegt, etwa: „Deshalb schaffen wir das am schnellsten direkt mit Ihnen."

8. Ausstieg

Sobald die Information oder die Freigabe da ist, endet das Gespräch freundlich, beispielsweise: „Vielen Dank, großartig, Sie haben uns gerettet." Danach Funkstille. Die Täter nutzen die erlangten Daten sofort oder verkaufen sie weiter.

Die Psychologie dahinter – das müssen Sie beachten

Die Methode setzt auf bekannte Denkabkürzungen:

- **Autorität.** Menschen folgen Anweisungen von angeblich höheren Stellen.
- **Dringlichkeit.** Zeitdruck senkt die Sorgfalt.
- **Vertrautheit.** Echte Details erzeugen das Gefühl von innen statt von außen.
- **Gegenseitigkeit.** Wer zuerst hilft oder lobt, bekommt eher Hilfe zurück.
- **Konsistenz.** Wer einmal zugestimmt hat, sagt auch beim nächsten kleinen Schritt leichter Ja.

Mein Tipp:

Achten Sie auf die Kombination aus Eile und Nähe. Der Anruf wirkt erstaunlich passend zu Ihrem Alltag, gleichzeitig darf es auf keinen Fall Verzögerung geben. Es wird von Ihnen eine Information verlangt, die Sie normalerweise niemals am Telefon herausgeben würden. Rückfragen oder Rückrufe werden ausgeredet. Es gibt keine saubere schriftliche Spur über die üblichen Wege in Ihrem Unternehmen.

Ihre Checkliste gegen Vishing

- Bleiben Sie misstrauisch bei Dringlichkeit. Wenn jemand am Telefon Druck aufbaut, ist das ein Warnsignal.
- Geben Sie niemals Passwörter oder Zugangsdaten am Telefon weiter. Kein Kollege, keine IT und keine Geschäftsführung dürfen danach fragen.
- Fragen Sie aktiv nach. Lassen Sie sich Name, Abteilung und Rückrufnummer geben – und rufen Sie über die offiziellen Kontakte Ihres Unternehmens zurück.
- Brechen Sie im Zweifel das Gespräch ab. Höflich, aber bestimmt: „Ich kläre das erst intern."
- Melden Sie den Vorfall sofort. Informieren Sie Ihren Vorgesetzten, die IT oder den Datenschutzbeauftragten, damit niemand anderes in die Falle tappt.
- Vertrauen Sie Ihrem Bauchgefühl. Wenn sich etwas seltsam anfühlt, ist es das meist auch.

Mein Fazit

Die wichtigste Botschaft für Sie als Mitarbeitende. Wenn es dringend und vertraut zugleich klingt, ist Vorsicht angesagt. Ein kurzer Stopp und eine Rückfrage auf dem offiziellen Weg entzaubern fast jeden Trick.

(AH)

WUSSTEN SIE SCHON? – MELDUNGEN AUS DER DATENSCHUTZPRAXIS

Manchmal klingen Datenschutzpannen fast wie Drehbücher für einen Krimi – nur leider passieren sie wirklich. Das Unabhängige Landeszentrum für Datenschutz hat in einem Vortrag einige echte Fälle zusammengetragen. Ein kleiner Auszug:

Ein Kryptotrojaner verschlüsselt Kundendaten und legt das Unternehmen lahm. In eine Arztpraxis wird eingebrochen, die Datensysteme verschwinden spurlos. In einem anderen Fall haben alle Mitarbeitenden Zugriff auf die Personalakten – auch diejenigen, die damit gar nichts zu tun haben.

Sozialdaten landen per E-Mail unverschlüsselt bei der falschen Adresse, ein gestohlenes Notebook sorgt für schlaflose Nächte und durch die Eingabe eines simplen URL-Pfads sind Studierendendaten im Internet für jedermann sichtbar.

Auch Arztbriefe landen schon mal ohne Einwilligung beim falschen Empfänger, Mitarbeitende schnüffeln unbefugt in Patientendaten oder sensible Kundendaten gehen bei einem Cloud-Anbieter verloren. Und wenn private Datenträger ins Spiel kommen, sind die Probleme praktisch vorprogrammiert.

Mein Tipp:

Damit solche Pannen gar nicht erst passieren, braucht es kein Hexenwerk. Oft reicht schon ein kurzer Moment der Aufmerksamkeit, bevor eine sicher verschlüsselte E-Mail mit sensiblen Daten rausgeht.

Auch wenn es manchmal bequem erscheint, private USB-Sticks oder Messenger zu nutzen – bitte lassen Sie es. Offizielle Systeme sind nicht zum Spaß da, sondern um genau solche Krimis zu verhindern.

Und denken Sie daran: Türen und Daten gehören gleichermaßen verschlossen, egal ob im Aktenschrank oder im Laptop. Wenn Ihnen einmal etwas seltsam vorkommt, fragen Sie lieber nach. Niemand wird Ihnen das übel nehmen, im Gegenteil – Sie beweisen damit, dass Ihnen Datenschutz und Sicherheit nicht egal sind.

So bleiben unsere Geschichten spannend, aber zum Glück nur auf dem Papier, denn echte Datendramen enden selten gut. Ein unbedachter Klick, eine vergessene Sperre oder ein zu schnell weitergeleitetes Dokument – und schon ist der nächste Vorfall da. Dabei sind es oft kleine Nachlässigkeiten, die große Folgen haben. Ein kurzer Moment der Aufmerksamkeit kann dagegen viel bewirken.

Prüfen Sie also lieber einmal mehr, ob Empfänger, Dateifreigaben oder Cloud-Links wirklich passen. Und wenn Sie unterwegs arbeiten, achten Sie darauf, dass niemand auf Ihren Bildschirm schaut.

Datenschutz ist kein Hindernis, sondern Ihr persönlicher Schutzschild. Je bewusster wir handeln, desto sicherer bleibt das Vertrauen unserer Kunden – und das ist letztlich das wichtigste Kapital, das wir in unserem Unternehmen haben.

(AH)

LIEFERKETTEN-ANGRIFFE VERMEIDEN

Lieferkettenangriffe, auch bekannt als Supply-Chain-Angriffe, sind eine Art von Cyberangriff, bei dem ein Angreifer nicht direkt das eigentliche Zielunternehmen attackiert, sondern stattdessen die Geschäftspartner, um sich so Zugang zu den Systemen und Daten des Zielunternehmens zu verschaffen. Auch mittelständische Unternehmen können von dieser Art von Angriff betroffen sein, da diese häufig auf externe Software, Wartung und IT-Dienste setzen. Damit Sie in Zukunft gewappnet sind, erklären wir Ihnen alles Wichtige im Video!

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: bestforbest – 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