Datenschutz Radar

Eine Ausgabe von DSBOK.de | Oktober 2025

Auskunft über Daten von Beschäftigten?

Müssen Beschäftigte damit rechnen, dass das Unternehmen dabei auch ihren Namen herausgibt? / *Seite 6*

INHALT:

Liebe Leserin, lieber Leser,

viele Datenpannen werden durch Unwissenheit und Fehlverhalten verursacht oder begünstigt. So kann sich der Schaden durch einen **Cybervorfall** deutlich erhöhen, wenn Betroffene nicht die richtigen Sofortmaßnahmen einleiten, nachdem der Angriff entdeckt wurde. Der erste Beitrag dieser Ausgabe enthält deshalb **Tipps für IT-Notfälle**. Und wie steht es um betriebliche Vorgänge, wie die **Kontrolle der Fahrerlaubnis** von Beschäftigten durch den Arbeitgeber? Was es hier zu beachten gilt, erklärt der zweite Beitrag dieser Ausgabe. Auch wenn von Dritten Auskunft verlangt wird über **Daten von Mitarbeitenden**, gilt es zu wissen, wie man sich richtig verhält. Der dritte Beitrag klärt hierzu auf.

Den Abschluss dieser Ausgabe macht ein Beitrag über das **Vertrauen in Lieferanten**. Können auch von E-Mails eines vertrauenswürdigen Lieferanten Risiken ausgehen? Lesen Sie hierzu den vierten Beitrag. ■

Oliver Krause
Externer Datenschutzbeauftragter
Datenschutzauditor
ok@dsbok.de

Sind Sie vorbereitet?

Wie schwerwiegend eine Datenpanne oder ein IT-Vorfall ist, hängt entscheidend davon ab, wie die Sofortmaß-nahmen danach aussehen.

■ IT-Vorfall: Was tun im Ernstfall?

Die Mehrheit der IT-Nutzerinnen und -Nutzer ist sich unsicher, wie man bei einem IT-Notfall richtig reagiert, wie der Cybersicherheitsmonitor 2025 des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Polizei zeigt. Unsicherheit bei einem IT-Vorfall erhöht aber die Datenrisiken.

Vorbereitet sein auf Cybervorfälle

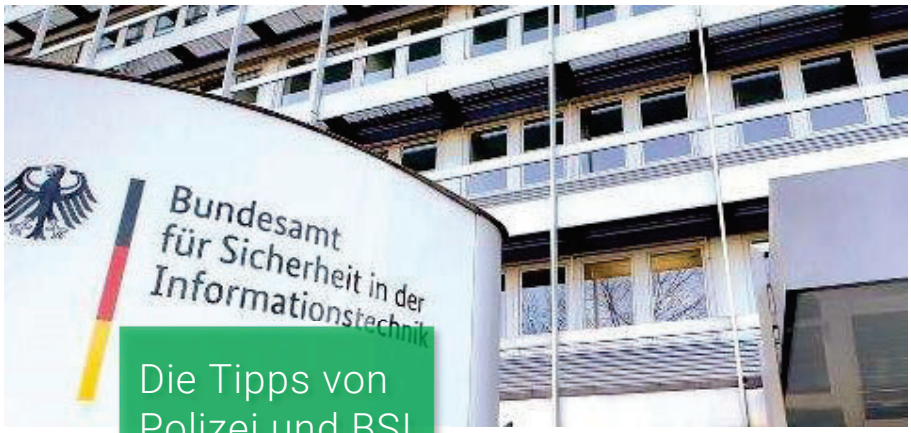
„Cyberkriminalität taucht im Alltag von vielen Menschen auf. Ob als betrügerische E-Mail oder als Betrug beim Online-Shopping“, warnt Dr. Stefanie Hinz, Vorsitzende der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK). „Wenn Sie betroffen sind, erstatten Sie Anzeige. Prävention, Aufklärung und konsequente Strafverfolgung tragen entscheidend dazu bei, die digitale Welt sicherer zu machen.“

Sieben Prozent der Bundesbürgerinnen und Bundesbürger wissen, dass sie im letzten Jahr von Internetkriminalität betroffen gewesen sind, die Polizei geht aber von einer hohen Dunkelziffer aus. Doch selbst wenn Opfer von Cyberkriminalität wissen, dass sie angegriffen wurden und nun vertrauliche Daten in Gefahr sind, ist die Cyber-bedrohung nicht abgewendet oder der Folgeschaden begrenzt.

Vielmehr müssen Betroffene wissen, wie sie reagieren sollen. Genau hier bestehen aber oftmals Defizite, wie der Cybersicherheitsmonitor 2025 ergeben hat.

Wissen, wie sich Schäden minimieren lassen

Wie schwerwiegend eine Datenpanne oder ein IT-Vorfall ist, hängt entscheidend davon ab, wie die Sofortmaßnahmen danach aussehen. Fehler nach einem Cyber-Vorfall können die Lage sogar noch verschlimmern. Dabei ist jede betroffene Person gefragt, nicht nur die IT-Sicherheitsbeauftragten, Datenschutzbeauftragten oder die IT-Administration.



Das BSI und die ProPK haben daher gemeinsam zwei neue sowie drei überarbeitete „Checklisten für den Ernstfall" mit Handlungsempfehlungen im Fall einer Infektion mit einem Schadprogramm oder Betrug beim Onlinebanking veröffentlicht. Darin finden sich insbesondere auch Hinweise, die alle IT-Nutzerinnen und IT-Nutzer betreffen können, beruflich wie privat. Diese beiden Vorfälle sind besonders häufig: Phishing/Passwortdiebstahl und Online-Erpressung/Ransomware.

Die Tipps von Polizei und BSI lauten in diesem Fall:

Ändern Sie schnellstmöglich das Passwort! Kontaktieren Sie den Anbieter, wenn Sie nicht länger auf Ihr Benutzerkonto zugreifen können! Beenden Sie alle aktiven Sitzungen! Kontrollieren Sie die Account-Einstellungen! Geben Sie Ihren Kontakten Bescheid!

Ändern Sie auch die Passwörter weiterer, potenziell mitbetroffener Accounts! Behalten Sie Ihre Kontoaktivitäten im Blick!

Wenn das Nutzerkonto gehackt wurde…

Die meisten Angriffe haben das Ziel, die Nutzerzugänge zu Anwendungen und Daten zu übernehmen. Dazu werden insbesondere Passwörter gestohlen. Hat man den Verdacht, dass ein Passwort in falsche Hände gekommen ist, weil man zum Beispiel auf eine Phishing-Mail hereingefallen ist, muss man schnell reagieren.

Wenn Ihr Bildschirm eine Nachricht von Online-Erpressern zeigt

Bei einem Ransomware-Angriff werden Daten kriminell und gegen den Willen der Betroffenen verschlüsselt. Eine Entschlüsselung wird erst gegen Zahlung eines Lösegeldes in Aussicht gestellt. Dabei erscheint in der Regel eine Zahlungsaufforderung auf dem Display des angegriffenen Geräts. Die Polizei rät dringend davon ab, das Lösegeld für die Daten zu bezahlen.

Stattdessen geben Polizei und BSI diese Hinweise zu Softwaremaßnahmen: Trennen Sie das Gerät vom Netzwerk: Schalten Sie das WLAN aus! Starten Sie einen Virenscan! Ändern Sie Ihre Passwörter! Lassen Sie Ihr System neu aufsetzen!

Es zeigt sich: Den größten Teil der Notfall-Reaktion übernimmt die IT-Sicherheitsabteilung. Im Ernstfall muss von den Betroffenen meist nicht viel getan werden, aber das Richtige. Wer ruhig bleibt und sich nicht zu Fehlverhalten im IT-Notfall verleiten lässt, hilft sehr dabei, größere Schäden bei Datenpannen und Cyberattacken zu vermeiden. ■

§ 21 Straßen-Verkehrs Gesetz

„Ihren Führerschein bitte!". Lesen Sie, warum das so ist und welche Spielregeln für den Umgang mit Ihren Daten gelten.

■ Führerscheinkontrolle durch den Arbeitgeber

Sie sollen ein Firmenfahrzeug benutzen, um einen Arbeitsauftrag zu erledigen. Als Sie den Autoschlüssel in Empfang nehmen wollen, heißt es plötzlich „Ihren Führerschein bitte!". Lesen Sie, warum das so ist und welche Spielregeln für den Umgang mit Ihren Daten gelten.

Als Fahrzeughalter hat Ihr Arbeitgeber erhebliche Pflichten

Rechtlich gesehen ist Ihr Arbeitgeber Fahrzeughalter. Das gilt zum einen für klassische „Dienstfahrzeuge", die Beschäftigte nur für Arbeitsfahrten benutzen dürfen. Bei „Firmenwagen", die Beschäftigte im vereinbarten Umfang auch für private Zwecke nutzen dürfen, trifft das ebenfalls zu. Fahrzeughalter wiederum haben generell erhebliche Pflichten. Dazu gehört auch die Pflicht, als Halter eines Fahrzeugs dieses Fahrzeug nur solchen Personen zu überlassen, die über die erforderliche Fahrerlaubnis verfügen.

Eine Pflichtverletzung hätte ernste Konsequenzen

Sollte Ihr Arbeitgeber gegen diese Pflicht verstoßen, hätte er mit ernsten Konsequenzen zu rechnen. Das Straßenverkehrsgesetz sieht einen solchen Verstoß als Straftat an. Die Sanktion besteht entweder in einer Geldstrafe oder gar in einer Freiheitsstrafe bis zu einem Jahr. Das ergibt sich aus § 21 Straßenverkehrsgesetz.

Der Führerschein dokumentiert die Fahrerlaubnis

Wenn im Alltag vom „Führerschein“ die Rede ist, ist rechtlich gesehen oft die „Fahrerlaubnis“ gemeint. Typisches Beispiel: Wenn ein Gericht jemandem wegen einer Trunkenheitsfahrt verurteilt, heißt es oft, das Gericht habe ihm „den Führerschein“ weggenommen. Rechtlich korrekt formuliert hat dieser Mensch jedoch die Fahrerlaubnis verloren. Den Führerschein muss er aber tatsächlich auch abliefern. Denn dieses amtliche Dokument würde sonst den falschen Eindruck erwecken, dass sein Inhaber immer noch über die darin näher beschriebene Fahrerlaubnis verfüge.

Der Arbeitgeber muss sich den Führerschein vorlegen lassen

Bevor ein Arbeitgeber Beschäftigten ein Fahrzeug überlässt, muss er sich den Führerschein vorlegen lassen. Nur so kann er nachprüfen, ob die für dieses Fahrzeug erforderliche Fahrerlaubnis vorhanden ist. Und nur so kann der Arbeitgeber für sich selbst strafrechtliche Risiken ausschließen. Selbstverständlich bedeutet das nicht, dass etwa der Vorstand eines größeren Unternehmens die Kontrolle persönlich durchführen muss. Im Normalfall ist die entsprechende Pflicht durch Organisationsverfügungen intern delegiert, zum Beispiel auf die Leitung des Fuhrparks eines Unternehmens.

Eine Dokumentation ist zwingend

Um belegen zu können, dass der Arbeitgeber seine Kontrollpflicht beachtet hat, muss er die erforderlichen Daten festhalten. Unentbehrlich ist es dabei, den vollständigen Namen, die Führerscheinklasse und das Ausstellungsdatum des Führerscheins zu dokumentieren. Denn nur so lässt sich im Ernstfall belegen, dass Beschäftigte die erforderliche Fahrerlaubnis nachgewiesen haben.

Völlig korrekt ist es, wenn sich ein Arbeitgeber die Richtigkeit dieser Angaben durch eine Unterschrift bestätigen lässt. Er muss das nicht zwingend tun, es ist aber allgemein üblich und führt über das „Vier-Augen-Prinzip“ dazu, dass Schreibfehler und dergleichen nahezu ausgeschlossen sind.

Der Arbeitgeber erfüllt eine Rechtspflicht

Sowohl die Einsichtnahme in den Führerschein als auch das Festhalten der wichtigsten Daten daraus sind datenschutzrechtlich relevant. Es erfolgt dabei jeweils eine Verarbeitung von personenbezogenen Daten. Dass dieses Vorgehen rechtmäßig ist, ergibt sich aus Art. 6 DSGVO. Danach ist eine Verarbeitung personenbezogener Daten rechtens, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Damit feststeht, dass Beschäftigte ihre Fahrerlaubnis nicht verloren haben, muss ein Arbeitgeber ungefähr alle sechs Monate Wiederholungskontrollen durchführen und auch sie dokumentieren.

Eine Führerscheinkopie wäre nicht zulässig

Die Idee, schlicht einen Scan oder eine Kopie des Führerscheins anzufertigen und den Scan oder die Kopie für die Dokumentation aufzubewahren, scheint auf den ersten Blick sehr naheliegend. Das würde aber mit dem Grundsatz der Datenminimierung

(Art. 5 Abs. 1 Buchst. c DSGVO) kollidieren. Denn dabei würde etwa auch das Bild des Führerscheininhabers gespeichert, und das ist schlicht nicht erforderlich. Prinzipiell denkbar wäre, dass Beschäftigte dazu ihre Einwilligung erteilen. Dem stehen aber die Aufsichtsbehörden für den Datenschutz oft skeptisch gegenüber, weil sie an der Freiwilligkeit einer solchen Einwilligung zweifeln. Haben Sie deshalb Verständnis dafür, wenn Ihr Arbeitgeber sich darauf nicht einlassen will. ■

Manchmal befürchten Beschäftigte

sie müssten persönlich mit Auskunfts-ansprüchen von Kundinnen und Kunden rechnen. Diese Sorge ist unbegründet.

■ Auskunft über Daten von Beschäftigten?

Die DSGVO gibt betroffenen Personen einen sehr weitreichenden Auskunftsanspruch. Unternehmen sind verpflichtet, Forderungen nach Auskunft nachkommen. Müssen Beschäftigte damit rechnen, dass das Unternehmen dabei auch ihren Namen herausgibt?

Einen Auskunftsanspruch haben nur Menschen

Wenn Beschäftigte Kundenanfragen beantworten, Bestellungen auf den Weg bringen oder Rechnungen erstellen, verarbeiten sie Daten der jeweiligen Kundinnen und Kunden. Soweit es sich bei den Kundinnen und Kunden um juristische Personen handelt, etwa eine AG oder eine GmbH, kommt die DSGVO nicht zur Anwendung. Juristische Personen haben deshalb keinen Auskunftsanspruch nach Art. 15 DSGVO. Anders sieht es aus, wenn es sich bei den Kundinnen oder Kunden um Menschen handelt. Dann ist die DSGVO anwendbar und es besteht ein Auskunftsanspruch gemäß DSGVO.

Der Auskunftsanspruch richtet sich gegen das Unternehmen

Manchmal befürchten Beschäftigte, sie müssten persönlich mit Auskunfts-ansprüchen von Kundinnen und Kunden rechnen. Diese Sorge ist unbegründet. Der Auskunftsanspruch richtet sich gegen den „Verantwortlichen“. Verantwortlicher ist

Beschäftigte sind keine „Daten-empfänger“ im Sinn der DSGVO

Damit Beschäftigte ihre Arbeit erledigen können, stellt ihnen das Unternehmen die erforderlichen Daten zur Verfügung. Dazu gehören auch die Daten von Kundinnen und Kunden. Dies hat zu der Frage geführt, ob Beschäftigte als „Empfänger“ dieser Daten anzusehen sind. Wäre dies zu bejahen, würde sich der Auskunftsanspruch gegen das Unternehmen auch darauf erstrecken, wer diese Empfänger sind. Der Europäische Gerichtshof (EuGH) hat diese Sichtweise jedoch abgelehnt. Nach seiner Auffassung werden Beschäftigte nicht dadurch zu Daten-empfängern im Sinn der DSGVO, dass ihr Arbeitgeber ihnen die notwendigen Daten zur Verfügung stellen.

dabei das jeweilige Unternehmen, nicht dagegen einzelne Beschäftigte. Einzige, allerdings wichtige Ausnahme: Sollten Beschäftigte Daten des Unternehmens zweckentfremden und rein für sich persönlich nutzen, werden sie selbst zum Verantwortlichen.
Wer also etwa die Telefonnummer einer Kundin verwendet, um sie aus rein persönlichen Motiven anzurufen, die mit der Arbeit im Unternehmen nichts zu tun haben, wird Verantwortlicher im Sinn des Datenschutzrechts. Etwaigen Auskunftsforderungen der Kundin sieht er sich dann persönlich ausgesetzt.

Der Auskunftsanspruch hat eine wichtige Schranke

Der Auskunftsanspruch endet dort, wo er die Rechte und Freiheiten anderer Personen beeinträchtigt. Solche anderen Personen können auch Beschäftigte in einem Unternehmen sein. In jedem Unternehmen gibt es viele Dokumente, in denen Namen und dienstliche Kommunikationsdaten von Beschäftigten enthalten sind. Manchmal lassen sich aus ihnen auch weitere Angaben über Beschäftigte entnehmen, etwa zu ihrer Funktion im Unternehmen. Dann stellt sich die Frage, ob sich der Auskunftsanspruch gemäß DSGVO auch auf solche Angaben erstreckt.

Beim Austausch von Mails wird es konkret

Wenn Beschäftigte mit Kunden korrespondieren, nennen sie dabei selbstverständlich ihren Namen. In aller Regel beschränken sich Beschäftigte dabei auf den Nachnamen, weil das genügt. Je nach Branche kommt es aber auch vor, dass der Vorname zusätzlich üblich ist. In manchen Branchen nennen Beschäftigte üblicherweise sogar nur ihren Vornamen. Wenn nun eine Kundin oder ein Kunde Auskunft gemäß DSGVO verlangt, stellt sich die Frage, ob der Name des Beschäftigten genannt werden muss, der die Angelegenheit bearbeitet hat. In der Regel kann ein Unternehmen eine solche Forderung ablehnen.

Der Auskunftsanspruch erstreckt sich auf die eigenen Daten dessen, der Auskunft verlangt. Daten anderer Personen erfasst er in aller Regel nicht. Solange Beschäftigte im Rahmen ihres Arbeitsvertrags und auf Weisung ihres Arbeitgebers handeln, besteht kein Anspruch darauf, ihre Identität zu erfahren.

Die praktische Umsetzung kann schwierig sein

Für den Normalfall kann man also beruhigen. Allerdings kann ein Unternehmen nicht einfach deshalb jede Auskunft ablehnen, weil etwa in einer Mail-Korrespondenz die

Namen einzelner oder mehrerer Beschäftigter auftauchen. Wenn es diese Namen verdecken will, bleibt nur die Schwärzung. Sie verursacht naturgemäß erhebliche Arbeit. Deshalb sollte man bedenken: In vielen Fällen, etwa bei völlig alltäglicher Korrespondenz mit Kunden, gibt es dafür keinen sachlichen Grund. Hier müssen es Beschäftigte dann hinnehmen, dass ihr Name eben doch herausgegeben wird. ■

Die Gefahr, dass Kunden oder Geschäfts-partner

einen hohen Schaden verursachen, ohne dies zu wissen und zu wollen.

■ Risiko Geschäftspartner: kein blindes Vertrauen

Gute Geschäfte brauchen eine Vertrauensbasis. Dabei darf aber nicht vergessen werden, dass auch von Geschäftspartnern ein Datenrisiko ausgehen kann. Die Zahl der Datenpannen in Partnernetzwerken und Lieferketten steigt.

Wenn Partner zum Risiko werden

Jedes zehnte Unternehmen berichtet davon, Opfer von Cyberangriffen geworden zu sein, die von einem Geschäftspartner oder von einem Kunden ausgegangen sind, so die TÜV Cybersecurity Studie 2025. Bedenkt man, dass bei vielen Cyberattacken gar nicht klar ist, wie sie genau abgelaufen sind, könnte die Zahl der betroffenen Unternehmen sogar noch höher liegen.

Was bedeutet aber dieses Ergebnis einer Umfrage zur Cybersicherheit? Kann man seinen Geschäftspartnern oder Kunden nicht mehr vertrauen? Wie sollen dann noch erfolgreiche Projekte möglich sein?

Tatsächlich ist es nicht vorstellbar, keinem Kunden und keinem Lieferanten mehr zu vertrauen. Auf menschlicher Ebene ist dies auch nicht erforderlich und so gemeint. Vielmehr müssen sich Vertrauensverhältnisse im digitalen Bereich ändern. Hier

besteht die Gefahr, dass man leicht getäuscht wird, aber auch, dass Kunden oder Geschäftspartner einen hohen Schaden verursachen, ohne dies zu wissen und zu wollen.

Viele Attacken und Datenpannen

von Partnernetzwerken und Lieferketten resultieren aus Schwachstellen, die sich irgendwo in diesem Netzwerk befinden, sich dann aber auch auf alle anderen Teilnehmenden der Lieferkette oder des Partnernetzwerks auswirken können.

Lieferanten und Kunden könnten selbst Opfer sein

Wenn zum Beispiel Phishing-Mails von einem Kunden oder Lieferanten kommen, muss das nicht bedeuten, dass diese Person nun plötzlich kriminell geworden ist. Vielmehr kann ein echter Internetkrimineller das Passwort des Lieferanten oder des Kunden gestohlen haben. Die E-Mail stammt dann gar nicht von dem Absender, der angezeigt wird, sondern von einem kriminellen Dritten.

Gelingt es zum Beispiel einem Hacker, Schadsoftware auf dem Rechner des Lieferanten zu platzieren, dann könnte dieser Virus in der nächsten Mail des Lieferanten stecken, ohne dass der Absender dies ahnen würde. Dann wäre der Lieferant zwar eigentlich vertrauenswürdig, aber nicht mehr die IT, die er nutzt.

KI kann das Vertrauen missbrauchen

Durch die zunehmende Verbreitung von KI (Künstliche Intelligenz) ist es für Cyberkriminelle noch leichter, Vertrauen auszunutzen. KI kann gefälschte E-Mails sehr echt aussehen lassen, selbst Videobilder und Stimmen in Video-Sitzungen könnten manipuliert sein. Man kann deshalb digitalen Nachrichten, aber auch klassischen Briefen oder Fax-Nachrichten nicht mehr blindlings vertrauen.

Es geht also nicht darum, dass Kunden und Lieferanten nicht mehr vertrauenswürdig wären, sondern die von ihnen genutzten IT-Systeme können Sicherheitslücken haben, die bei Angriffen ausgenutzt werden. In Zeiten der fortschreitenden Digitalisierung muss streng unterschieden werden zwischen dem Vertrauen, das man einer Person schenkt, und dem notwendigen Misstrauen, das herrschen muss bei E-Mails und anderen Kommunikationsformen, die scheinbar von Lieferanten oder Kunden kommen. Vertrauen muss also neu betrachtet und differenziert werden. ■