Datenschutz Radar

Eine Ausgabe von DSBOK.de | Februar 2026

Ja, Sie sind Pwned!

Ihre eigene E Mail-Adresse und das damit verbundene Passwort sind in einem bekannten Sicherheitsvorfall aufgetaucht. **Was jetzt?** *Seite 4*

INHALT:

Liebe Leserin, lieber Leser,

keine Frage: Wenn es **eine Datenpanne** gibt, müssen Sie **schnell und richtig reagieren**. Doch bevor Maßnahmen ergriffen werden können, braucht es Gewissheit darüber, ob und wie man selbst betroffen ist. Spezielle Datenbanken können hier helfen, indem sie betroffene Datensätze auflisten und eine gezielte Abfrage ermöglichen. Im ersten Artikel dieser Ausgabe erfahren Sie, worauf Sie dabei achten sollten – und was Sie lieber vermeiden sollten.

Der zweite Beitrag widmet sich einem besonderen Weg des Datentransfers: dem **Versand digitaler Informationen auf Speichermedien** wie USB Sticks per Post. Wir zeigen, welche Sicherheitsaspekte dabei wichtig sind und wie Sie sensible Daten zuverlässig schützen können. Auch im öffentlichen Raum begegnen uns digitale Themen immer häufiger. Wer mit dem Auto unterwegs ist, trifft zunehmend auf Parkplätze, die **Kennzeichenerfassung** einsetzen. Doch wie steht es hierbei um den Datenschutz? Das beleuchten wir im dritten Artikel. Im letzten Beitrag greifen wir schließlich die verbreitete Warnung auf, **Zwei Faktor Authentifizierungen seien nicht mehr sicher**. Was ist dran an diesen Meldungen? Bedeutet das, dass man auf dieses Sicherheitsverfahren verzichten sollte? Die klaren Antworten finden Sie auf der letzten Seite.

Ich wünsche Ihnen eine interessante Lektüre! ■

Oliver Krause
Externer Datenschutzbeauftragter
Datenschutzauditor
ok@dsbok.de

Aber Vorsicht vor angeblichen Warnmeldungen!
Enthält sie einen Link zur Prüfung, könnte es sich um einen Phishing-Versuch handeln…

■ Sind Sie Teil eines Datenlecks?

„Schon wieder eine Datenpanne in den Schlagzeilen" – das könnten Sie fast jede Woche sagen. Und plötzlich stellen Sie fest, dass es sich um einen Online-Dienst handelt, den Sie privat oder beruflich nutzen. Doch wie können Sie herausfinden, ob Sie selbst betroffen sind und beispielsweise ein Passwort ändern sollten?

Datenbanken über Datenlecks

Auch ohne direkte Information vom Betreiber des betroffenen Dienstes könnten Ihre Daten Teil des bekannt gewordenen Datenlecks sein. Was also tun? Im Internet gibt es verschiedene Dienste, mit denen geprüft werden kann, ob persönliche Daten von Datenausspähung oder Datenmissbrauch betroffen sind.

Sebastian Schmidt

Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Nicht nur ein Passwort?

„Solche Daten werden in sogenannten Credential-Stuffing-Listen gesammelt. Diese ermöglichen es Angreifenden, automatisiert und in Millisekunden Log-in-Versuche bei verschiedenen Diensten wie Online-Shops oder sozialen Netzwerken durchzuführen“, erklärt der Landesdatenschutzbeauftragte. „Gerade deshalb ist es gefährlich, wenn Nutzende gleiche oder sehr ähnliche Passwörter für unterschiedliche Dienste verwenden.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Nach neuen Berichten über Datenpannen mit mehr als 1,3 Milliarden erbeuteten Passwörtern hat der Landesdatenschutzbeauftragte von Mecklenburg-Vorpommern etwa auf die Datenbank „**Have I Been Pwned**“ (HIBP) hingewiesen. Dort lässt sich abfragen, ob die eigene E Mail-Adresse und das damit verbundene Passwort in einem bekannten Sicherheitsvorfall auftauchen. Finden sich bei HIBP Treffer, sollten die Passwörter der betroffenen E Mail-Adressen umgehend geändert werden. Zudem lohnt es sich, über die Aktivierung einer Zwei-Faktor-Authentifizierung nachzudenken.

Vorsicht vor angeblichen Warnmeldungen

Nicht jeder vermeintlich hilfreiche Dienst zur Prüfung gefährdeter E Mail-Adressen ist tatsächlich seriös – manche sind sogar gefährlich. Nach einer Meldung über ein Datenleck sollte man daher nicht wahllos im Internet nach Datenbanken suchen, sondern ausschließlich vertrauenswürdige Quellen nutzen, die etwa die Datenschutzaufsicht oder das BSI (Bundesamt für Sicherheit in der Informationstechnik) empfehlen.

Besondere Vorsicht ist geboten, wenn eine E Mail eintrifft, die über eine angebliche Datenpanne informiert. Enthält sie einen Link zur Prüfung, könnte es sich um einen Phishing-Versuch handeln, der E Mail-Adresse und Passwort abgreifen soll. Man wird dann nicht nur selbst Teil eines Datenlecks, sondern erhält durch die Kriminellen oft sogar eine Rückmeldung, dass alles in Ordnung sei und kein Passwortwechsel nötig wäre. In Wahrheit ist man bereits Opfer des Angriffs geworden.

Warndienste oder Phishing-Mail?

Es gibt jedoch seriöse Warndienste, die tatsächlich darüber informieren, dass man von einer Datenpanne betroffen ist. Diese durchsuchen hinterlegte E Mail-Adressen und melden sich, wenn sie beispielsweise im Darknet auftauchen – allerdings nur, wenn man sich zuvor für diesen Dienst registriert hat.

Wenn Sie einen solchen Warndienst nutzen oder nutzen möchten, seien Sie aufmerksam, um nicht auf Phishing hereinzufallen. Ein seriöser Dienst fragt niemals nach einem Passwort oder fordert über einen Link zum Passwortwechsel auf. Seien Sie besonders misstrauisch gegenüber Warnungen, die nach Ihrem Passwort verlangen – so verhindern Sie, selbst Teil der nächsten Datenpanne zu werden. ■

Sicher bis zum Briefkasten

Übrigens die Regelmäßige Leerung des Briefkastens ist wichtig, Post aus dem Briefkasten zu „angeln“, ist meist einfach...

Digitale Daten analog verschicken: So geht’s sicher

Einen USB-Stick oder ein anderes elektronisches Speichermedium mit der Post zu versenden – nichts scheint leichter als das. Gerade deshalb geht dabei häufig etwas schief. Einige einfache Tipps helfen, Pannen effektiv zu vermeiden.

Oft ist ein Versand mit der Post einfach nötig

Der Versand elektronischer Speichermedien mit der klassischen „gelben Post“ wirkt für viele wie ein Relikt aus vergangenen Zeiten. Doch häufiger, als man denkt, ist er auch heute noch notwendig. Mal geht es um einen USB-Stick oder eine Speicherkarte, oft aber auch um Geräte wie Smartphones oder Digitalkameras, in denen Speichermedien fest verbaut sind.

Eine persönliche Übergabe wäre grundsätzlich zu bevorzugen. Doch meist ist das aufgrund großer Entfernungen oder fehlender Zeit nicht möglich. Geht es ausschließlich um den Datentransfer, kann dieser auch über ein geeignetes Kommunikationsportal erfolgen. Das hilft jedoch nicht weiter, wenn ausdrücklich auch das physische Speichermedium weitergegeben werden soll.

Verschlüsselung kann sinnvoll sein

Wenn ein Speichermedium große Datenmengen enthält, kann eine Verschlüsselung sinnvoll sein. Ein USB-Stick mit 128 Gigabyte Kapazität kann beispielsweise rund 12 Millionen bedruckte Seiten aufnehmen. Eine Verschlüsselung ist daher zwar empfehlenswert, aber nicht zwingend notwendig oder vorgeschrieben. Denn für Postsendungen gilt das Postgeheimnis: Wer eine Sendung unbefugt öffnet, begeht eine Straftat und muss mit einer Freiheits- oder Geldstrafe rechnen (§ 202 StGB). Dieser Schutz gilt auch für Datenträger.

Eine gute Verpackung ist wichtig

Ein USB-Stick in einem dünnen Briefumschlag kann in automatischen Sortieranlagen leicht den Umschlag zerreißen und herausfallen. Die Zuordnung ist dann meist nicht mehr möglich. Wattierte Versandtaschen verhindern solche Probleme weitgehend.

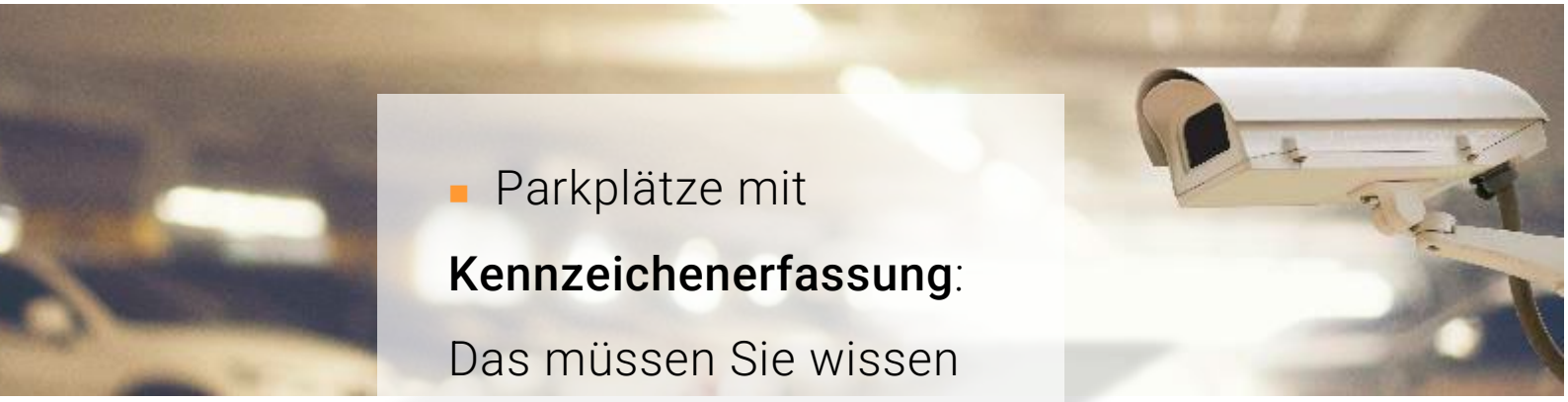
Ein Päckchen, das z. B. ein Handy enthält, sollte zudem ausreichend stabil sein. Wer unsicher ist, findet bei der Deutschen Post AG entsprechende Empfehlungen.
Auch der Verschluss spielt eine große Rolle: Stabiles Klebeband sorgt zuverlässig dafür, dass die Sendung geschlossen bleibt. Viele private Postdienstleister bieten zudem Sicherheitsverschlüsse oder Sicherheitsaufkleber an. Metallklammern allein reichen nicht aus, da sie sich verbiegen und in Sortiermaschinen hängen bleiben können – der Umschlag reißt dann schnell auf.

Eine Sendungsverfolgung ist viel wert

Kommt eine Sendung nicht an, beginnt die Suche – und eine Sendungsverfolgung macht diese deutlich einfacher. Normale Briefe bieten diese Möglichkeit nicht. Anders ist es beim Einwurfeinschreiben: Solche Sendungen werden mehrfach gescannt, sodass nachvollziehbar ist, bis wohin sie gelangt sind.
Auch Pakete lassen sich verfolgen, Päckchen hingegen meist nicht. Die Postanbieter informieren über die jeweils geltenden Regeln; online sind sie ebenfalls abrufbar. Trotz Sendungsverfolgung sollten die Erwartungen jedoch realistisch bleiben.

Regelmäßige Leerung des Briefkastens ist wichtig

Unternehmen wie Privatpersonen erhalten heute nur noch selten klassische Briefpost. Der früher selbstverständliche tägliche Blick in den Briefkasten fällt dadurch oft weg. Das kann sich als Schwachstelle erweisen: Post aus dem Briefkasten zu „angeln“, ist meist einfach, und ein über Tage voller Kasten kann sowohl Profikriminelle als auch Gelegenheitstäter aufmerksam machen. Wer Post mit Speichermedien erwartet, sollte den Briefkasten daher täglich kontrollieren. ■



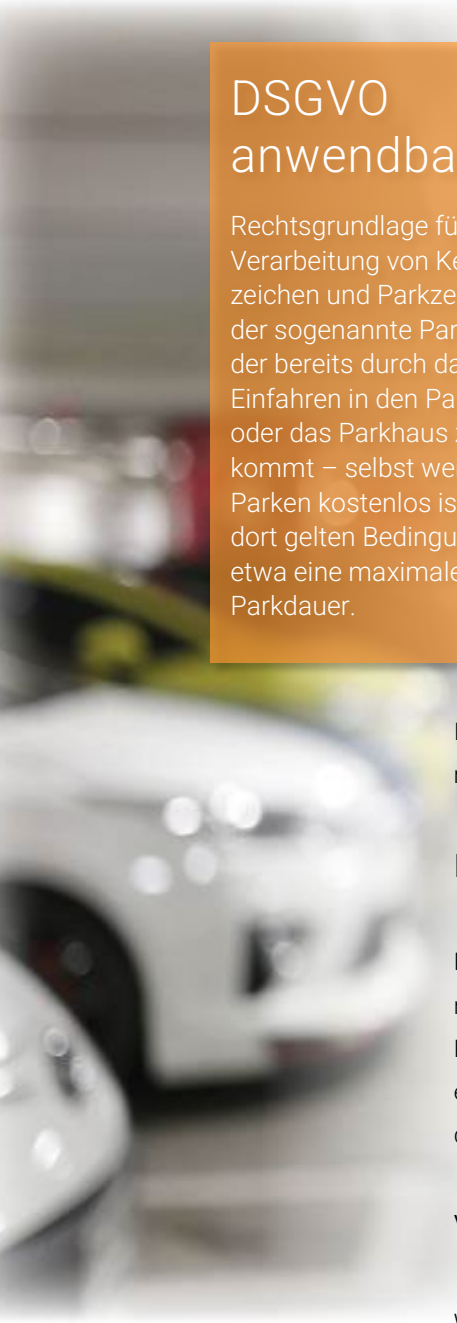
■ Parkplätze mit **Kennzeichenerfassung**: Das müssen Sie wissen

Das Erfassen von Kennzeichen beim Parken ist inzwischen weit verbreitet. Für den Datenschutz ist das unproblematisch, sofern bestimmte Vorgaben eingehalten werden.

Das Kennzeichen ersetzt Ticket und Parkscheibe

Früher musste man auf Supermarktparkplätzen an die Parkscheibe denken oder im Parkhaus ein Ticket ziehen, das am Kassenautomat für die Abrechnung der Parkzeit genutzt wurde. Vergessene Parkscheiben oder verlorene Tickets konnten teuer werden.

Heute erfasst an der Einfahrt eine Kennzeichen-Kamera das Nummernschild sowie Datum und Uhrzeit der Einfahrt. Bei der Ausfahrt wird das Kennzeichen erneut erfasst. Bei gebührenfreien Parkplätzen prüft das System, ob die zulässige Parkzeit eingehalten wurde. Ist das der Fall, werden die Daten kurzfristig gelöscht. Bei gebührenpflichtigen Parkplätzen wird zusätzlich geprüft, ob die Parkgebühr korrekt bezahlt wurde.



DSGVO anwendbar?

Rechtsgrundlage für die Verarbeitung von Kennzeichen und Parkzeiten ist der sogenannte Parkvertrag, der bereits durch das Einfahren in den Parkplatz oder das Parkhaus zustande kommt – selbst wenn das Parken kostenlos ist. Auch dort gelten Bedingungen, etwa eine maximale Parkdauer.

Die DSGVO ist anwendbar

Kfz-Kennzeichen gelten als personenbezogene Daten, wenn der Halter eine natürliche Person ist. Auch wenn das Kennzeichen selbst keine direkte Identifikation ermöglicht, ist es eindeutig einer Person zugeordnet.

Die Informationspflichten der DSGVO gelten

Nach Art. 13 DSGVO müssen Parkplatzbetreiber umfassend über die Datenerhebung informieren: Wer erhebt die Daten? Zu welchem Zweck? Wie läuft die Verarbeitung ab? Was geschieht danach mit den Daten? Daher finden sich an Einfahrten oft ausführliche Informationstafeln. Beschwerden über fehlende Informationen sind selten – die meisten Betreiber erfüllen die Vorgaben zuverlässig.

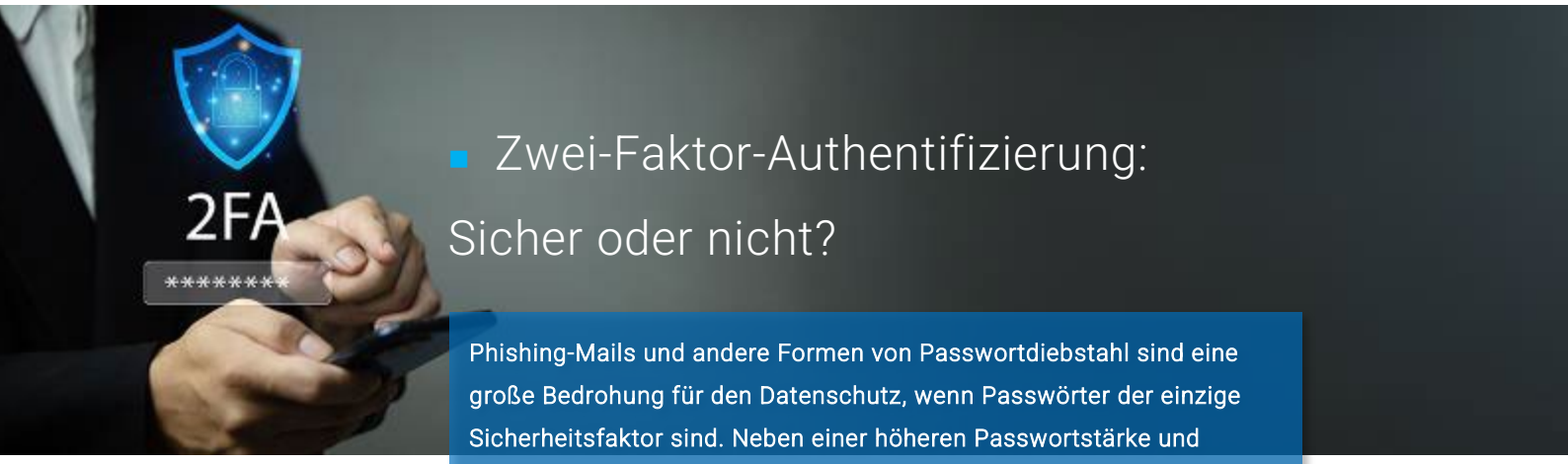
Bei juristischen Personen ist theoretisch alles anders

Fahrzeuge, die auf eine juristische Person wie eine GmbH zugelassen sind, fallen nicht unter die DSGVO. Das ist in Erwägungsgrund 14 ausdrücklich festgehalten. Praktisch spielt das aber keine Rolle: Parkplatzbetreiber können nicht erkennen, ob ein Fahrzeug einer natürlichen oder einer juristischen Person gehört – und wenden daher die DSGVO für alle Fahrzeuge gleichermaßen an.

Vertragsverstöße führen zu Konsequenzen

Wer auf einem kostenlosen Parkplatz länger steht als erlaubt oder bei gebührenpflichtigen Parkplätzen ohne Bezahlung abfährt, muss mit einer Vertragsstrafe rechnen – häufig zwischen 40 € und 60 €.

Um Ansprüche durchzusetzen, kann der Parkplatzbetreiber über eine Halterauskunft beim Kraftfahrt-Bundesamt Namen und Anschrift des Fahrzeughalters ermitteln. Grundlage dafür ist das Straßenverkehrsgesetz. Da das Parken rechtlich zum „ruhenden Verkehr“ gehört, fällt auch die Durchsetzung von Parkgebühren darunter. Die Kosten der Halterauskunft werden zusätzlich zur Vertragsstrafe in Rechnung gestellt. ■



■ Zwei-Faktor-Authentifizierung: Sicher oder nicht?

Phishing-Mails und andere Formen von Passwortdiebstahl sind eine große Bedrohung für den Datenschutz, wenn Passwörter der einzige Sicherheitsfaktor sind. Neben einer höheren Passwortstärke und Alternativen wie Passkeys wird daher regelmäßig die Zwei-Faktor-Authentifizierung (2FA) empfohlen, um den Zugangsschutz deutlich zu erhöhen.

Inzwischen häufen sich jedoch Warnungen, dass auch eine 2FA nicht vollkommen sicher ist – so etwa in einem aktuellen Sicherheitshinweis des Landeskriminalamts (LKA) Niedersachsen.

Wie kann das sein, dass eine Zwei-Faktor-Authentifizierung überwunden wird? Und lohnt sich 2FA dann überhaupt noch? Hier helfen keine voreiligen Schlussfolgerungen, sondern fundierte Informationen.

Es geht um den Diebstahl von Session-Cookies

Bei einer Zwei-Faktor-Authentifizierung wird zusätzlich zum Passwort ein zweiter Sicherheitsfaktor verwendet, beispielsweise ein Hardware-Token, ein Fingerabdruck oder ein Einmalpasswort (OTP). Internetkriminelle versuchen jedoch nicht, sowohl Passwort als auch zweiten Faktor zu stehlen – das wäre in der Praxis viel zu aufwendig.

Stattdessen greifen sie Session-Cookies an. Ein Session-Cookie ist eine kleine Textdatei, die im Browser oder in einer App gespeichert wird und bestätigt, dass sich

die Nutzerin oder der Nutzer erfolgreich mit beiden Sicherheitsfaktoren angemeldet hat. So muss die 2FA während einer Sitzung nicht ständig wiederholt werden.

Diese Cookies funktionieren wie digitale Ausweise für eine laufende Sitzung. Werden sie gestohlen, kann ein Angreifer die Sitzung übernehmen, ohne sich selbst mit 2FA anmelden zu müssen. Denn die erfolgreiche doppelte Anmeldung hat das Opfer bereits durchgeführt – und der Cookie dient als Nachweis.

Wissen Sie, wie sicher Ihre Zwei-Faktor-Authentifizierung tatsächlich ist?

Ist eine Zwei-Faktor-Authentifizierung absolut sicher? Nein, Cyberkriminelle können unter Umständen auch eine 2FA überwinden. Werden bei einem 2FA-Verfahren Session-Cookies verwendet, können diese gestohlen und zur Sitzungsübernahme missbraucht werden. Dadurch kann der starke Zugangsschutz ausgehebelt werden.

Ist 2FA unsicher, weil Hardware-Tokens verloren gehen können? Nein, denn auch wenn Tokens verloren gehen oder gestohlen werden, reicht das allein nicht aus – zusätzlich ist das Passwort nötig. Zwar können Tokens verloren gehen oder gestohlen werden, doch der Angreifende bräuchte zusätzlich das zugehörige Passwort. Bei Session-Cookies hingegen reicht das Cookie selbst aus, da darin gespeichert ist, dass beide Faktoren erfolgreich eingegeben wurden. Die Übernahme des Cookies ermöglicht dann den Zugriff auf die Sitzung – und damit auf die Daten.

Wichtig: Nicht auf 2FA verzichten

Dass Kriminelle Session-Cookies stehlen können, bedeutet nicht, dass man auf 2FA verzichten sollte – darin ist sich auch das LKA Niedersachsen einig.
Zum einen arbeiten nicht alle 2FA-Verfahren mit Session-Cookies, zum anderen bietet 2FA immer einen zusätzlichen Schutz, auch wenn dieser nicht unüberwindbar ist.
Diese klare Empfehlung lautet weiterhin: Überall dort, wo es möglich ist, 2FA aktivieren. ■