Newsletter Datenschutz

Ausgabe 06 | 2023

Wenn die KI zum Datenleck wird...

Ihr Datenschutz-Info Blatt

Liebe Leserin, lieber Leser,

ob Dashcam im Fahrzeug, E-Mail-Verteiler, Cyberattacke oder ChatGPT: Immer ist der Datenschutz gefragt! So erfahren Sie in dieser Ausgabe, was bei Dashcams im Auto zu beachten ist und wann womöglich ein Bußgeld fällig werden kann.
Verteiler bei E-Mails können ebenfalls mehr sichtbar machen, als sie sollten. Deshalb erhalten Sie wichtige Hinweise zum Einsatz von offenen und verdeckten Adressenlisten als E-Mail-Verteiler.
Ein weiteres Thema in dieser Ausgabe sind die Schwachstellen in der IT, die Cyberangriffe ermöglichen und so zu immer mehr Datenschutzverletzungen beitragen. Sie erfahren dabei, dass es nicht nur neue IT-Sicherheitslücken sind, die zu einer großen Gefahr werden können.
Nicht zuletzt beleuchtet diese Ausgabe die Datenschutzprobleme, die bei der Nutzung von KI-Diensten wie ChatGPT auftreten könnten. Machen Sie am besten gleich den Wissenstest dazu auf der letzten Seite.

Ihr Frank Berns, Datenschutzbeauftragter

Bußgelder wegen Aufnahmen mit einer Dashcam

Sie lassen beim Autofahren ständig eine Kamera auf dem Armaturenbrett mitlaufen? Vorsicht, das kann schnell richtig teuer werden! Diese Punkte müssen Sie beachten, damit es keinen Ärger gibt.

Die Versuchung ist groß

Gute Dashcams gibt es schon für um die 50 Euro. So jedenfalls das Ergebnis entsprechender Tests von Computer-BILD, CHIP und anderen Zeitschriften. Und im Ernstfall liefern die Aufnahmen den Beweis dafür, dass man an einem Unfall nicht schuld war. Also nichts wie ran und eine solche Kamera installieren? Die Antwort: ja, aber ...

Die Aufzeichnungen sind umfangreich

Dashcams sind dazu da, den Verkehr vor dem eigenen Fahrzeug aufzuzeichnen. Dabei erfasst die Kamera alle möglichen Verkehrsteilnehmer, vom Pkw der Vorderfrau über das Fahrrad schräg rechts vom Fahrzeug bis hin zu Fußgängern, die vor dem Fahrzeug die Fahrbahn queren. Im Normalfall sind sämtliche Aufnahmen überflüssig. Denn Unfälle sind trotz aller Gefahren des Straßenverkehrs relativ selten. Und nur wenn es zu einem Unfall gekommen ist, braucht man die Aufnahmen.

KONTAKT zu uns MAIL@Konzept17.de

Löschung ist wichtig

Deshalb verlangt der Datenschutz, dass alle Aufnahmen sehr schnell gelöscht werden. Jedenfalls solange es keinen Unfall gibt. Kommt es zu einem Unfall, darf die Aufzeichnung dagegen gespeichert bleiben. Rechtlich formuliert: Nur wenn es zu einem Unfall kommt, hat der Fahrer ein berechtigtes Interesse daran, den Unfallhergang durch Filmaufnahmen zu beweisen. Ansonsten überwiegt das Interesse der anderen Verkehrsteilnehmer, nicht ohne Anlass gefilmt zu werden.

Automatische Löschung ist auch möglich

Gute Kameramodelle bewältigen diese Vorgaben problemlos. Sie arbeiten mit einem sogenannten „Ringspeicher". Das funktioniert so: Solange nichts Besonderes passiert, speichert die Kamera das Verkehrsgeschehen nur für kurze Zeit. Dann werden die Aufnahmen mit neuen Aufnahmen überschrieben. Wenn das Auto sehr stark abgebremst wird, registrieren das Bewegungssensoren in der Kamera. Sie sorgen dafür, dass alle gerade vorhandenen Aufnahmen dauerhaft gespeichert bleiben. Diese Aufnahmen stehen dann als Beweismittel zur Verfügung.

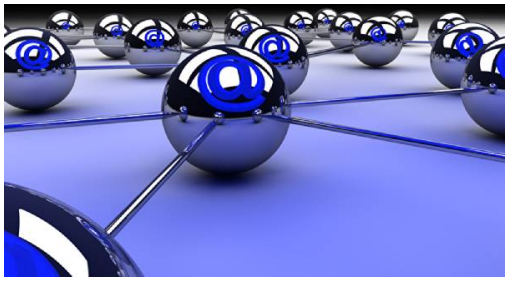
Verstöße gegen die Vorgaben kosten Geld

Manche lassen die Kamera alle Aufnahmen dauerhaft speichern. Die Routine für das automatische Löschen aktivieren sie nicht. Das verstößt gegen den Datenschutz. Denn solche durchgängigen Aufzeichnungen sind nicht erforderlich. Damit ist die Datenschutz-Grundverordnung (DSGVO) verletzt. Fällt das der Polizei auf, kommt es zu einem Bußgeldverfahren. Verhängt wird das Bußgeld durch die Datenschutzaufsicht. Üblich sind dabei Beträge von mehreren 100 Euro.

Mehrere Verstöße kosten mehrfach Geld

Dabei gibt es eine rechtliche Tücke, die viele übersehen. Jede abgeschlossene Fahrt, von der Aufnahmen vorhanden sind, stellt einen eigenständigen Verstoß gegen die DSGVO dar. Verfügt ein Fahrzeughalter beispielsweise über Aufzeichnungen von zehn Fahrten, hat er damit zehn eigenständige Ordnungswidrigkeiten begangen. Entsprechend summieren sich mehrere Bußgelder.

Vorsicht bei Sammelmails mit offenem Verteiler



Sie schicken eine E-Mail an mehrere Adressaten. In manchen Fällen darf jeder Adressat alle anderen Adressaten sehen, in anderen dagegen nicht. Das kommt Ihnen bekannt vor? Gerade dann lesen Sie bitte unbedingt weiter!

Und täglich grüßt das Murmeltier

„Und täglich grüßt das Murmeltier" – so lautet der Titel einer Filmkomödie. Der Hauptdarsteller steckt in einer Zeitschleife. Deshalb passiert um ihn herum jeden Tag immer wieder genau dasselbe. Dazu gehört, dass erstmals nach dem Winter die Murmeltiere aus dem Bau kommen. Und das eben jeden Tag aufs Neue. Ähnlich sieht es beim fehlerhaften Umgang mit Mailverteilern aus. Wir können davor warnen, so oft wir wollen. Die Pannen wiederholen sich trotzdem jeden Tag aufs Neue.

Nach wie vor gibt es bei Mails drei Adress-Varianten

Wer eine Mail an mehrere Adressaten schicken will, hat drei Adress-Varianten zur Verfügung:

- Variante 1: Die Mailadressen aller Adressaten kommen in das „An"-Feld.
- Variante 2: In das „An"-Feld kommt nur die Mailadresse eines Adressaten. Die Mailadressen aller anderen Adressaten kommen in das „Cc"-Feld.
- Variante 3: Auch hier kommt in das „An"-Feld nur die Mailadresse eines Adressaten. Die Mailadressen anderer Adressaten kommen in das „Bcc"-Feld.

Nach wie vor besteht ein wichtiger Unterschied zwischen den drei Adress-Varianten

Der Unterschied besteht darin, welche Adressaten die Adressen der anderen Adressaten sehen können – oder eben auch nicht. Hier gilt in guter Murmeltier-Tradition:

- Bei Variante 1 kann jeder Adressat die Mailadressen aller anderen Adressaten sehen. Denn alle Adressen stehen im selben offenen Adressfeld.
- Bei Variante 2 ist das genauso. Zwar erhält hier nur der Adressat, der im „An"-Feld steht, die Mail direkt. An alle Adressaten, die im „Cc"-Feld stehen, geht „nur" eine Kopie dieser Mail. Dabei handelt es sich allerdings um eine offene Kopie. Deshalb sehen hier alle Adressaten die Mailadressen aller anderen Adressaten.
- Bei Variante 3 ist es dagegen ganz anders. Die Abkürzung „Bcc" steht für „Blind-Kopie". Adressaten, die in diesem Adressfeld stehen, können nicht erkennen, wer die Mail sonst noch erhalten hat.

Variante 3 (die mit dem „Bcc") ist die problemlose Gestaltung

Variante 3 (die mit „Bcc") passt dann punktgenau, wenn die Adressaten der Mail nichts miteinander zu tun haben und deshalb nichts voneinander wissen sollen. Typisches Beispiel: Eine Marketing-Mail geht an alle Kunden eines Unternehmens.

Daraus ergibt sich diese Faustregel

Diese Variante ist in allen Zweifelsfällen die richtige. Die Faustregel lautet daher: Es ist kein Problem, Variante 3 (die mit dem „Bcc") zu benutzen, wenn eine Mail an mehrere Adressaten gehen soll. Die Nutzung der anderen beiden Varianten erfordert dagegen immer eine besondere Begründung. So passt Variante 2 (die mit dem „Cc") etwa dann, wenn zwei Mailpartner sich austauschen und andere Personen davon wissen sollen.

Das kann man nicht oft genug wiederholen

Sie meinen, dass wir bis hier aus Texten abgeschrieben haben, die wir Ihnen schon einmal geschickt haben? Ja, das ist richtig. Es ist aber leider auch notwendig. Denn nahezu alle neuen Tätigkeitsberichte von Aufsichtsbehörden für den Datenschutz schildern entsprechende Fälle. Und allmählich verlieren die Aufsichtsbehörden die Geduld. Bisher waren die rechtlichen Folgen in solchen Fällen meist überschaubar. Das ändert sich aber gerade.

Am Anfang steht die Meldung der Datenschutzverletzung

Wer beispielsweise eine Marketing-Mail an alle Kunden mithilfe von Variante 1 (die mit dem „An") oder Variante 2 (die mit dem „Cc") verschickt, hat einen klaren Verstoß gegen die DSGVO begangen. Dieser

Datenschutzverstoß ist der Datenschutzaufsicht mithilfe der üblichen Meldeformulare im Internet zu melden. Wer das versäumt, riskiert schon deswegen eine Geldbuße.

Als Nächstes kommt eine Geldbuße

Je nachdem, wie sensibel die Mailadressen sind, kommt es zu einer Geldbuße in unterschiedlicher Höhe. Mailadressen können durchaus sensibel sein. Beispiel: Eine Klinik verschickt aktuelle Informationen an schwangere Frauen, die in der Klinik entbinden wollen. Dass die Frauen schwanger sind, ergibt sich aus dem, was die Klinik ihnen in der Mail schreibt. Das wird dann im Zweifel teuer. Geht es dagegen um eine Werbemail für Bücher, wird die Geldbuße deutlich niedriger ausfallen.

Sperren Sie das Murmeltier endlich ein!

Wenn Sie diesen Text sorgfältig gelesen haben, sollte Ihnen keine Panne mehr mit Mailverteilern passieren. Bildlich gesprochen: Sie haben das Murmeltier erfolgreich in seinem Bau eingesperrt und lassen es dort friedlich schlafen. Das vermeidet Stress im Unternehmen.

Keine Updates in der IT, kein Datenschutz

Denken Sie auch, dass die vielen Aktualisierungen in der IT lästig sind? Doch ein Verzicht auf regelmäßige Updates würde den Datenschutz und die Datensicherheit aushöhlen: Viele Datenpannen geschehen, weil es offene Sicherheitslücken in der IT gibt.

Nervige Updates?

Kaum ein Tag vergeht, an dem nicht eine Aktualisierung für IT-Geräte heruntergeladen und eingespielt werden muss. Ob im Beruf oder im Privatleben: Die Apps auf Smartphones und Tablets, die Betriebssysteme und Anwendungen auf den PCs und Notebooks, ja sogar die Fernbedienung und das Smart-TV benötigen immer wieder eine Aktualisierung der Software.

Dabei sind neue Funktionen und Erweiterungen eher die Ausnahme. Schaut man sich an, warum eine Aktualisierung ansteht, wird das Update meist mit notwendigen Fehlerbehebungen begründet. Die meisten Fehler aber sind Probleme für den Betrieb des Geräts und für die Sicherheit der Daten.

IT-Fehler sind oftmals Schwachstellen

Die Fehler in der Software passieren meist ungewollt während der Entwicklung. Die Programmiererinnen und Programmierer entdecken ihre Fehler erst spät oder sogar zu spät. Internetkriminelle suchen aktiv nach Fehlern in der IT, um sie auszunutzen und zum Beispiel Berechtigungen und Zugriffsmöglichkeiten zu erlangen, die sie nicht haben sollten.

Die Fehler in der IT sind deshalb auch Schwachstellen oder Sicherheitslücken. Sie machen die gefürchteten und immer stärker zunehmenden Cyberangriffe erst möglich. Eine IT ohne Schwachstellen ließe sich nicht missbrauchen, doch leider gibt es keine fehlerfreie IT.

Wenn Updates zu spät kommen

Kommt es zu einem Angriff, bevor die Schwachstelle durch Updates, auch Patches genannt, behoben ist, haben die Internetkriminellen und Datendiebe meist leichtes Spiel. Viele Datenschutzverletzungen

entstehen durch solche Cyberattacken, die IT-Schwachstellen ausnutzen. Tatsächlich sind IT-Sicherheitslücken und entsprechende Angriffe inzwischen eine der Hauptursachen für Datenpannen, wie die Datenschutzaufsichtsbehörden regelmäßig melden.

Nun könnte man denken, die Schwachstellen werden nicht rechtzeitig behoben, weil es keinen Patch dafür gibt. Das kommt zwar vor. Doch sehr häufig würde es durchaus schon ein Sicherheitsupdate geben, aber das jeweilige Unternehmen oder der betroffene Nutzende haben das verfügbare Update nicht installiert. Teils liegt dies an der Unkenntnis, dass es bereits ein Update gibt. Teils wird aber auch der Aufwand für die vielen Aktualisierungen gescheut.

So sagte zum Beispiel Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein: „Mit Sorge blicke ich auf das Thema Informationssicherheit". So hätten immer noch viele Organisationen ihre Hausaufgaben nicht gemacht, um bekannte Schwachstellen in IT-Systemen zu beseitigen. „Die Datenpannen-Meldungen zeigen uns, wie solche Sicherheitslücken immer wieder ausgenutzt werden und oft auch Daten abfließen können", so Marit Hansen weiter.

Viele Schwachstellen bleiben offen, obwohl ein Update verfügbar wäre

Ein Beispiel zeigt, wie gefährlich es sein kann, ein verfügbares Update nicht zu installieren. So berichtete das Bundesamt für Sicherheit in der Informationstechnik (BSI) davon, dass bei einem weltweit breit gestreuten Angriff Tausende Server mit Ransomware infiziert und kriminell verschlüsselt wurden, um Lösegeld zu erpressen. Dabei nutzten die Angreifer eine Schwachstelle in einer bestimmten IT-Lösung aus, die bereits lange bekannt war und für die es schon länger eine Fehlerbehebung gab.

Es ist zwar auch richtig und wichtig, eine bereits ausgenutzte Schwachstelle zu schließen, also „die Tür zu schließen", durch die die Angreifenden gekommen waren. Doch weitaus besser wäre es, nicht erst nach dem erfolgreichen Angriff die Empfehlungen zur Behebung der Schwachstellen zu lesen und umzusetzen. Mit dem erfolgreichen Angriff ist es sehr oft bereits zu einer Datenpanne gekommen.

Tipp: Priorisieren, Automatisieren und die Bedeutung der Updates bedenken

Statt die Vielzahl der Updates zu beklagen oder sogar verfügbare Updates nicht zu installieren, sollten Unternehmen wie auch Privatpersonen überlegen, wie sie den zweifellos bestehenden Aufwand verringern, aber auch rechtfertigen können.

Zum einen sind nicht alle Updates gleichermaßen kritisch. Denn die möglichen Folgen einer offenen Schwachstelle unterscheiden sich. In Schwachstellen-Datenbanken gibt es deshalb zu Schwachstellen und Updates in aller Regel eine Bewertung, wie hoch das Risiko durch die jeweilige Schwachstelle ist.

Sind der mögliche Schaden und die Wahrscheinlichkeit eines Angriffs hoch, muss die betreffende Schwachstelle eine hohe Priorität zur Behebung erhalten. Dabei sollten möglichst Lösungen genutzt werden, die Updates automatisch herunterladen und installieren oder aber zumindest auf die verfügbaren Updates hinweisen.

Nicht zuletzt sollte man bedenken: Ohne Updates ist heute kein Datenschutz mehr möglich. Es würden Löcher bleiben, durch die Daten abfließen können, Datenpannen wären oft die Folge. Updates gehören deshalb zum Datenschutz dazu.

Wenn die KI zum Datenleck wird

Datenschützer warnen schon länger davor, dass die unbedachte Nutzung von Künstlicher Intelligenz (KI) zum Risiko für die Privatsphäre werden kann. Dienste wie ChatGPT sorgen nun für eine einfache Verbreitung von KI in Unternehmen und Haushalten. Höchste Zeit, den Umgang mit KI zu hinterfragen.

KI: Mehr als ein nützlicher Assistent

Der Chatbot antwortet druckreif auf jede Frage, oder die App malt ein Bild nach Anweisung und im gewünschten Stil – eine breite Öffentlichkeit hat in den vergangenen Wochen und Monaten ausprobiert, was Künstliche Intelligenz inzwischen leisten kann, berichtete der Digitalverband Bitkom. Rund drei Viertel der Bundesbürgerinnen und Bundesbürger (73 Prozent) sind nun der Meinung, dass KI eine Chance ist.

Auch Unternehmen sind offen für KI-Dienste wie ChatGPT & Co: Bereits jedes sechste Unternehmen plant laut Bitkom den KI-Einsatz zur Textgenerierung. „Die aktuellen Entwicklungen in der Künstlichen Intelligenz ermöglichen es uns, erstmals direkt mit der KI zu interagieren, und schaffen völlig neue Einsatzbereiche quer durch alle Branchen“, sagte Bitkom-Präsident Achim Berg. „KI wird künftig zum Büroalltag genauso dazugehören wie heute der PC. KI hat das Potenzial, die massiven Auswirkungen der demografischen Entwicklung und des sich verschärfenden Fachkräftemangels abzufedern.“

Datenschützer sind alarmiert

Datenschutzaufsichtsbehörden weisen auch auf mögliche Risiken hin. KI-Systeme wie ChatGPT, die plötzlich zur Internet-Suche oder zum Schreiben von Texten zu allen möglichen Zwecken Verwendung finden: eine gute Sprachqualität, doch „ausgedachte“ Behauptungen werden wie echte Fakten präsentiert, Betroffenenrechte laufen leer, überzeugende Antworten auf die Fragen des Datenschutzes fehlen, so zum Beispiel das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein.

Als erste Aufsichtsbehörde in Europa hatte die italienische Datenschutzbehörde der Firma OpenAI untersagt, personenbezogene Daten von italienischen Bürgerinnen und Bürgern im Rahmen der Anwendung ChatGPT zu verarbeiten. Zu klären ist insbesondere, wie mit personenbezogenen Daten der Nutzer oder Dritter umgegangen wird. Wer speichert sie, zu welchem Zweck und wie lange?

Neue und verschärfte Sicherheitsrisiken

IT-Sicherheitsforschende warnen davor, dass solche KI-Dienste dafür genutzt werden könnten, bei Cyberangriffen die Opfer leichter zu täuschen, indem zum Beispiel „erfolgreiche“ Phishing-Mails leichter zielgenau erstellt werden können.

Doch auch legitime Nutzerinnen und Nutzer könnten mit solchen KI-Diensten die Datensicherheit aushöhlen, indem sie dem KI-Service vertrauliche Daten übermitteln, die in den Datenbestand des Dienstes aufgenommen, ausgewertet und an Dritte ausgegeben werden könnten. Zum Beispiel könnte womöglich der Versuch, ein Bewerbungsschreiben per KI optimieren zu lassen, zu einer ungewollten

Datenweitergabe an Dritte führen.

Verschiedene Unternehmen haben bereits intern Verbote erlassen, vertrauliche Daten in Dienste wie ChatGPT einzutragen. Dieser Gefahr sollten sich aber alle Nutzenden bewusst sein.

Wissen Sie, wie KI-Dienste zum Datenleck werden könnten? Machen Sie den Test!

Frage: Wenn man in einen KI-Dienst seine eigenen Daten eingibt, damit diese zum Beispiel in einen professionellen Lebenslauf verwandelt werden, bleibt dies vertraulich. Stimmt das?

1. Nein, es ist nicht ohne Weiteres auszuschließen, dass die eingegebenen Daten in den gesamten Datenbestand aufgenommen werden.
2. Ja, jede Nutzung eines KI-Dienstes ist so vertraulich wie ein Gespräch unter vier Augen, nur zwischen KI und Nutzer oder Nutzerin.

Lösung: Die Antwort 1. ist richtig. KI-Dienste sind darauf angelegt, zu „lernen", also auf die Eingaben der Nutzenden zu reagieren, um die Antworten immer weiter zu optimieren. Dabei ist es die Idee von KI, aus möglichst vielen Quellen Daten zu beziehen. Ob die Daten dann später für andere Zwecke genutzt werden als die ursprünglichen, ist eine Frage an den Datenschutz, den die KI gewährleistet. Automatisch kann man nicht von der Einhaltung der Zweckbindung ausgehen.

Frage: Antworten, die eine KI gibt, sind sorgfältig geprüft und vertrauenswürdig. Ist das so?

1. Ja, jede KI basiert auf einer Qualitätssicherung, sodass man den Ergebnissen vertrauen kann.
2. Nein, die Antworten können fehlerhaft sein. Eine weitere Prüfung ist notwendig.

Lösung: Die Antwort 2. ist richtig. KI-Expertinnen und Experten warnen davor, einer KI einfach zu vertrauen. KI-Lösungen sind nicht fehlerfrei. Es kann sogar sein, dass Dritte eine KI so trainiert haben, dass sie gezielt falsche Antworten gibt, um zum Beispiel Nutzende zu manipulieren. Dazu werden die Trainingsdaten „vergiftet". Man spricht von Data Poisoning. Es ist denkbar, dass über Antworten von KI Nutzende zu Aktivitäten verleitet werden sollen, die Sicherheitslücken und Datenpannen nach sich ziehen, wie zum Beispiel die Preisgabe von Zugangsdaten und Geschäftsgeheimnissen.

Impressum

Redaktion:
Frank Berns, Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de