Newsletter Datenschutz
Ausgabe 10 | 2019

Konzept 17

Geldbußen bei Datenmissbrauch nur für die verantwortliche Stelle?

Ihr Datenschutz-Info-Blatt

Liebe Leserin, lieber Leser,

auch wenn im Datenschutz das Unternehmen die verantwortliche Stelle ist: Datenschutz betrifft jeden einzelnen Beschäftigten. Wie diese Ausgabe zeigt, drohen auch Mitarbeiterinnen und Mitarbeitern Geldbußen, wenn sie Daten missbrauchen, zusätzlich zu arbeitsrechtlichen Konsequenzen. Ebenso muss jeder Internetnutzer daran mitwirken, dass der Besuch von Webseiten nicht zu einem Datenrisiko wird.

Falsche Vorstellungen von Einwilligungen, die Kunden erteilen, will diese Ausgabe ebenso ausräumen wie unvollständige Bilder von den Gefahren für den Datenschutz, die von einem Drucker ausgehen können. Der Datenschutz kann nur gelingen, wenn jeder seinen Anteil tut und datenschutzgerecht handelt. Die aktuellen Beiträge helfen Ihnen dabei - mit konkreten Tipps und einem Wissensquiz auf der letzten Seite.

Ich wünsche Ihnen viel Spaß beim Lesen! *Ihr Frank Berns, Datenschutzbeauftragter*

Datenschutzverstöße: Geldbußen gegen Mitarbeiter?

Geldbußen gegen Mitarbeiter von Unternehmen sieht die DSGVO nicht vor. So liest man in der letzten Zeit häufig. Doch stimmt das überhaupt? Die ehrliche Antwort auf diese Frage lautet: Meist schon, aber keineswegs immer!

Datenschutzverstoß eines Mitarbeiters

Ein Mitarbeiter übermittelt Daten, obwohl die Datenschutz-Grundverordnung (DSGVO) das nicht zulässt. Der Grund: Er kennt sich mit den Vorschriften nicht richtig aus und hat sie falsch interpretiert. Eigentlich hätte ihm dies nicht passieren dürfen, denn er hat eine betriebsinterne Datenschutz-Schulung besucht. Aber wie es so geht: Gerade als diese Frage behandelt wurde, war er gedanklich woanders.

Das ist ein typischer Fall von Fahrlässigkeit. Dass er bloß fahrlässig gehandelt hat, würde dem Mitarbeiter für sich allein allerdings nichts helfen. Denn die Regelung zur Verhängung von Geldbußen in Art. 83 DSGVO kennt auch Geldbußen für fahrlässiges Handeln.

Unternehmen als Verantwortlicher

Dennoch kann die zuständige Aufsichtsbehörde für den Datenschutz gegen den Mitarbeiter persönlich keine Geldbuße verhängen. Das ist nur gegenüber "Verantwortlichen" (und "Auftragsverarbeitern") vorgesehen. Und Verantwortlicher im Sinn der DSGVO ist das Unternehmen, nicht der Mitarbeiter. Anders formuliert: Begeht ein Mitarbeiter im Rahmen seiner Tätigkeit einen Datenschutzverstoß, kann das durchaus eine Geldbuße nach sich ziehen. Diese Geldbuße wird allerdings gegen das Unternehmen verhängt, für das der Mitarbeiter gehandelt hat.

Arbeitsrechtliche Maßnahmen möglich

Arbeitsrechtliche Maßnahmen, insbesondere eine Abmahnung, kann das Unternehmen wegen des fahrlässigen Verhaltens ergreifen. Sie sind unabhängig von einer Geldbuße.

Verfolgung rein privater Interessen

Völlig anders ist das Ergebnis allerdings, wenn ein Mitarbeiter rein private Interessen verfolgt. Beispiel: Der Mitarbeiter hat die Möglichkeit, für dienstliche Zwecke Bonitätsabfragen zu machen. Er will eine Wohnung vermieten, die ihm privat gehört. Deshalb möchte er die finanzielle Situation eines Mietinteressenten ausloten. Dafür missbraucht er die Abfragemöglichkeit, die er am Arbeitsplatz hat. In diesem Fall wird der Mitarbeiter selbst zum Verantwortlichen im Sinn der DSGVO. Denn in diesem Fall bestimmt allein er den Zweck seiner Abfrage. Die Mittel, die ihm dienstlich zur Verfügung stehen, missbraucht er hierfür. Damit ist für diese Abfrage er selbst und nicht sein Arbeitgeber der Verantwortliche im Sinn der DSGVO. Die Folge: Die Aufsichtsbehörde für den Datenschutz kann gegen ihn persönlich eine Geldbuße verhängen.

Praxisfall aus Baden-Württemberg

Solche Fälle sind in der Praxis durchaus schon vorgekommen. Besonders stark beachtet wurde der Fall eines Polizisten in Baden-Württemberg. Er interessierte sich für eine Frau, die er in einem Auto gesehen hatte. Um ihren Namen zu erfahren, ermittelte er die Halterin des Autos. Dazu benutzte er Abrufmöglichkeiten, die er nur für dienstliche Zwecke verwenden durfte. Das brachte ihm eine Geldbuße der Datenschutzaufsicht ein und außerdem ein Disziplinarverfahren durch seinen Dienstherrn.

Relevant auch für Unternehmen

Für Mitarbeiter in Unternehmen würde bei einem vergleichbaren Fall dasselbe gelten wie für den Polizisten. Missbrauchen sie Abfragemöglichkeiten für rein private Zwecke, müssen sie die Folgen tragen. Dazu gehört auch, dass die Aufsichtsbehörde für den Datenschutz eine Geldbuße gegen sie verhängen kann.

KONTAKT zu uns MAIL@Konzept17.de

Websites: Mehr als die Datenschutzerklärung

Sind Sie mit dem Webbrowser im Internet unterwegs, können Ihre personenbezogenen Daten schnell in Gefahr geraten. Viele Webseiten haben Datenschutzmängel. Dabei ist eine unvollständige Datenschutzerklärung nur ein Beispiel.

Datenschutz bei Webseiten oftmals mangelhaft

Wer glaubt, weniger prominente Webauftritte sind in Datenschutzfragen ein Risiko, bekannte Webseiten dagegen nicht, der irrt sich. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat vor einigen Monaten Websites mit sehr großer Reichweite untersucht. Obwohl sich einige der prominentesten Internetdienste unter den Geprüften befanden, fiel das Ergebnis aus Datenschutzsicht ernüchternd aus: Im Umgang mit Passwörtern und Tracking-Werkzeugen erkannte das Landesamt zahlreiche Mängel.

Ähnliche Resultate erhielt auch der Europäische Datenschutzbeauftragte (EDPS). Seine Prüfungen bei den Websites der wichtigsten EU-Organe und -Einrichtungen ergab, dass bei sieben von zehn geprüften Websites Datenschutz- und Datensicherheitsprobleme aufgetreten sind. Eines der Probleme war das Tracking durch Dritte ohne vorherige Zustimmung. Weitere Schwachstellen betrafen die Verwendung von Trackern für Webanalysen ohne vorherige Zustimmung der Besucher und die Übermittlung personenbezogener Daten, die die Webseitenbetreiber über Webformulare mithilfe unverschlüsselter Verbindungen erfassten.

Die Lücken im Datenschutz sind vielfältig

Auch wenn sich hinter dem Link "Datenschutz" auf Webseiten meist die Datenschutzerklärung (Privacy Policy) verbirgt - der Datenschutz muss nicht nur richtig erklärt werden, er muss auch anderen Anforderungen der Datenschutz-Grundverordnung (DSGVO) genügen. Es geht zum Beispiel um die Verwendung von Cookies, um Web Beacons, um Seitenelemente, die von Dritten geladen werden, und um die Sicherheit verschlüsselter Verbindungen (HTTPS).

Es geht aber auch um den Einsatz neuer Technologien in Websites, zum Beispiel um Chatbots, die die Anbieter vermehrt in Internetauftritte einbinden, um unzureichende Verschlüsselung, die nicht dem Stand der Technik entspricht, um den Ausfall von Webseiten, da sie nicht belastbar genug sind,

Wichtig: die eigenen Geräte schützen!

und um Datenschutz-Optionen, die fehlen oder nicht datenschutzfreundlich voreingestellt sind.

Einwilligung & Datenminimierung

Natürlich geht es auch um Fragen der Einwilligung ins Online-Tracking (Nachverfolgen der Nutzeraktivitäten), um die Rechtmäßigkeit der Verarbeitung der Nutzerdaten insgesamt oder auch um die Datenminimierung, die Webseiten zum Beispiel dann verletzen, wenn Online-Formulare Daten abfragen, die für den Vorgang gar nicht nötig sind. So ist für den Download eines Reiseprospekts die Telefonnummer oder das Geburtsdatum des Nutzers sicherlich nicht erforderlich. Doch der Betreiber der Webseite möchte das gern für andere Zwecke wie Werbung wissen.

Auch Sicherheitslücken betreffen den Datenschutz

Nicht zu vergessen sind auch die technischen Schwachstellen der Content-Management-Systeme (CMS), Web-Frameworks und Plugins, die für die Websites zum Einsatz kommen. Diese Sicherheitslücken ermöglichen es Angreifern, heimlich Nutzerdaten abzugreifen oder die Systeme des Nutzers mit Schadsoftware zu attackieren. Selbst verschlüsselte Verbindungen zu Webseiten können gefährlich sein, wenn das Sicherheitszertifikat für die Verschlüsselung Probleme aufweist, aber noch nicht zurückgezogen wurde.

Der Prüfdienst SIWECOS untersuchte zum Beispiel 754 Webseiten kleiner und mittelständischer Unternehmen aus NRW hinsichtlich Sicherheitslücken. Ergebnis: 71,8 Prozent der KMU-Webseiten in NRW waren nicht optimal konfiguriert, 6,6 Prozent der Seiten hatten eklatante Sicherheitsmängel.

Kein harmloser Webseiten-Besuch

Was aber können Sie tun, wenn Sie das nächste Mal einen Webbrowser nutzen und Internetauftritte besuchen, ob beruflich oder privat? Sorgen Sie zum einen auf Ihrer Seite für die richtige Datensicherheit. Dazu gehören aktuelle Browserversionen, aktuelle Browser-Plugins und aktuelle Betriebssysteme ebenso wie ein Anti-Malware-Programm auf allen Endgeräten - also auch auf dem Smartphone, dem Tablet oder der Smartwatch.

Viele Sicherheits- und Datenschutzmaßnahmen sind allerdings Sache des Webseiten-Betreibers. Er muss den Webserver absichern, Schwachstellen im CMS beseitigen und eine aktuelle Datenschutzerklärung zur Verfügung stellen. Hier können Sie als Nutzer nur darauf achten, dass Sie die Webseiten mit geeigneten Werkzeugen vor dem Besuch überprüfen, zum Beispiel mit einem sogenannten Link-Scanner. Er prüft Webseiten, ohne dass Sie diese Seiten im Browser öffnen müssen.

Stellen Sie fest, dass es Probleme mit einer Webseite gibt, verzichten Sie auf den Online-Besuch. Machen Sie sich in jedem Fall klar, dass eine Webseite nicht einfach ein Dokument ist und ein Webbrowser nicht einfach ein Anzeigeprogramm. Es geht bei Websites und Webbrowsern um komplexe Anwendungen, die viele Anforderungen an den Datenschutz erfüllen müssen. Ein Besuch im Internet kann also schnell und spannend sein, unproblematisch für den Datenschutz ist er in vielen Fällen allerdings nicht.

Impressum

Redaktion:
Frank Berns
Datenschutzbeauftragter

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

Einwilligung von Kunden in mangelhafte Datensicherheit möglich?

Datenschutz macht Arbeit. Das gilt besonders für Maßnahmen der Datensicherheit, wie etwa die Verschlüsselung von E-Mails. Kann man sich solche Mühen sparen, wenn ein Kunde damit ausdrücklich einverstanden ist?

Datensicherheit verlangt Differenzierung

Gleich zu Beginn eine Klarstellung: Nein, es steht nirgends in der Datenschutz-Grundverordnung (DSGVO), dass E-Mails immer verschlüsselt werden müssten. Aber die DSGVO verlangt, dass man sich Gedanken darüber macht, wann dies nötig ist. Die sehr umfangreiche Regelung über die Sicherheit der Verarbeitung in Art. 32 DSGVO zwingt Unternehmen dazu, sich zu entscheiden. Ist das Risiko für den Datenschutz so hoch, dass eine Verschlüsselung notwendig ist? Oder ist das nicht der Fall?

Der Zwang zur Entscheidung gilt auch für viele andere Fragen rund um die Sicherheit der Verarbeitung. So ist etwa eine Entscheidung nötig, wie intensiv eine Zugangskontrolle sein muss. In einem großen Rechenzentrum wird sie sicher anders aussehen als in einer Werbeagentur mit einigen wenigen Kundenlisten.

Eigene Entscheidung des Kunden denkbar?

Aber vielleicht kann man sich alle komplizierten Überlegungen sparen, wenn man den Kunden um eine Einwilligung bittet? Und zwar um eine Einwilligung darin, dass er mit einer mangelhaften Datensicherheit einverstanden ist. Denn der Kunde müsste doch die Freiheit haben, selbst zu entscheiden.

Fall aus der Praxis: eine Tagesklinik

Das mag sich zunächst absurd anhören. Doch genau dies wurde in der Praxis bereits versucht. Versuchsgelände war dabei ausgerechnet eine Tagesklinik. Es ging dabei um medizinische Daten, also nicht um etwas Banales. Unter anderem ließ sich die Klinik unterschreiben, dass sie auch telefonisch über Diagnosen Auskunft geben darf. Das Risiko, dass ein Unbefugter anruft und die Diagnose erfährt, hätte der Patient tragen müssen.

Kaum Widerstand der Betroffenen

Auch wenn es unwahrscheinlich klingt - ganz offensichtlich unterschrieben Hunderte von Patienten eine entsprechende Erklärung. Sie scheinen kein Problem damit gehabt zu haben, der Klinik einen solchen Freibrief auszustellen. Oder fühlten sie sich vielleicht unter Druck gesetzt, das zu tun? Gleich wie: Aufgegriffen wurde das Ganze nicht wegen entsprechender Beschwerden bei der (in diesem Fall österreichischen) Datenschutzaufsicht. Vielmehr stellte die zuständige Aufsichtsbehörde bei einer amtlichen Überprüfung fest, was hier ablief.

Untersagungsverfügung der Aufsichtsbehörde

Bildlich gesprochen grätschte sie hier sofort ein. Sie untersagte der Tagesklinik, weiterhin so zu verfahren. Die Begründung hierfür hat nichts mit der besonderen Situation im medizinischen Bereich zu tun. Das macht sie für alle Unternehmen interessant.

Ablehnende Haltung der Aufsichtsbehörde zu Einwilligungen

Im Kern geht es um die generelle Frage, ob ein Betroffener auf Maßnahmen der Datensicherheit verzichten kann, obwohl sie nach den Maßstäben der DSGVO erforderlich sind.

Die im Beispielfall zuständige Aufsichtsbehörde hält diesen Ansatz für völlig untauglich. Formal begründet sie dies damit, dass die Vorschriften zur Datensicherheit der Verarbeitung das Thema "Einwilligung des Betroffenen" nicht einmal erwähnen. Daraus zieht sie den Schluss, dass eine Einwilligung hier von vornherein keine Rolle spielen kann.

Eine Einwilligung kann zwar dazu führen, dass bestimmte Daten verarbeitet werden dürfen. Sie kann aber nicht von der Pflicht befreien, diese Verarbeitung so sicher durchzuführen, wie es die DSGVO vorschreibt.

Kritische Stimmen

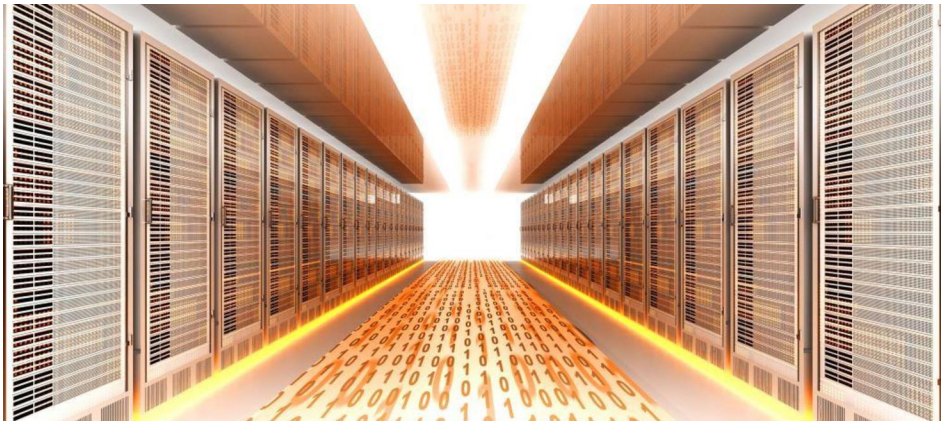
Kritiker bemängeln an dieser Argumentation, hier werde dem Betroffenen letztlich ein Schutz aufgedrängt, den er gar nicht wolle. Schließlich gehe es um den Schutz seiner eigenen personenbezogenen Daten. Dann müsse er aber auch entscheiden können, ob er diesen Schutz einfordern möchte.

Objektive Komponente der Datensicherheit

Man kann dies jedoch auch anders sehen. Der Zweck der DSGVO besteht nämlich nicht nur darin, die Rechte einzelner Betroffener zu schützen. Vielmehr hat sie außerdem noch den Zweck, den freien Verkehr personenbezogener Daten innerhalb der EU zu ermöglichen. Selbstverständliche Voraussetzung hierfür ist die praktische Umsetzung der Vorgaben aus der DSGVO. Sie muss objektiv gesehen gewährleistet sein. Für eine Entscheidungsfreiheit einzelner Betroffener ist dann konsequenterweise kein Raum.

Gefahr von Geldbußen

Zumindest die wenigen Aufsichtsbehörden, die sich dazu schon geäußert haben, vertreten diese Auffassung. Das Risiko, es anders zu versuchen, ist für Unternehmen zu groß. Denn gar zu schnell kann eine mangelhafte Datensicherheit eine empfindliche Geldbuße nach sich ziehen.



Das Maß an Datensicherheit, das die DSGVO fordert, ist nicht verhandelbar, so zumindest die Meinung einiger Datenschutz-Aufsichtsbehörden

Drucker-Sicherheit: Wenn der Drucker zum Datenleck wird

Nicht nur wenn Sie einen vertraulichen Ausdruck am Drucker liegen lassen, ist der Datenschutz bedroht. Auch über das Internet erfolgen Attacken auf Drucker in Unternehmen und Privathaushalten. Drucker brauchen daher Aufmerksamkeit.

Drucker als Einfallstor

Drucker stehen schon so lange in Unternehmen und Home Offices, dass kaum jemand auf die Idee käme, sie als Teil des Internet of Things (IoT) zu sehen. Tatsächlich aber sind vernetzte Drucker nichts anderes als IoT-Geräte. Allein dieser Hinweis sollte aufschrecken lassen: Aktuell wird häufig über Schwachstellen in IoT-Systemen berichtet. Das Internet der Dinge zählt zu den besonders beliebten Angriffszielen. Also sollte man auch damit rechnen, dass Drucker mit Netzwerkanschluss angegriffen werden.

Tatsächlich geschieht genau das: Forscher von Microsoft haben kürzlich festgestellt, dass die russische Hackergruppe "Fancy Bear" gezielt IoT-Systeme angreift, darunter zahlreiche Netzwerkdrucker. Doch das ist nur ein Beispiel von vielen.

Ausdrucke blockieren, Daten stehlen

Attacken auf Drucker haben vor allem zwei Ziele: Die Drucker werden zum einen überlastet, genau wie dies mit Webservern geschieht (DDoS-Attacke, Distributed-Denial-of-Service-Attacke). Zum anderen dienen die Drucker als Datenquelle, entweder indem die Angreifer den Druckerspeicher auslesen oder indem sie Druckerverbindungen ins Netzwerk und zu anderen Endgeräten ausnutzen.

Dabei missbrauchen sie auch Zusatzfunktionen solcher Drucker, die als Multifunktionsdrucker bezeichnet werden und zum Beispiel eine Fax-Funktion aufweisen. So senden Angreifer zum Beispiel eine manipulierte Grafikdatei an die Fax-Nummer. Der Multifunktionsdrucker versucht dann, diese Grafikdatei und damit das angebliche Fax auszudrucken. Dabei wird die manipulierte Datei ausgeführt, und der Schadcode kann sein Unheil anrichten, wenn der Drucker Schwachstellen aufweist.

Mehr Datensicherheit bei Druckern

Drucker müssen deshalb stärker als mögliches Datenrisiko verstanden und in der Datensicherheit berücksichtigt werden. Wenn es um IoT-Risiken geht, sollten Sie also auch an Drucker denken. Für Drucker muss es eine Sicherheitsrichtlinie geben, und alle Druckerverbindungen müssen auf verdächtige Aktivitäten hin untersucht werden. Kontaktiert ein Drucker zum Beispiel eine Anwendung, mit der sich normalerweise keine Druckaufträge erteilen lassen, ist das bereits verdächtig.

Entscheidend ist, dass Drucker wie alle anderen Endgeräte regelmäßig Sicherheitsupdates bekommen. Außerdem müssen die Zugriffe auf die Druckfunktionen begrenzt sein nach dem Motto "Need to print".

Managen Dienstleister die Drucker, nicht die interne IT-Abteilung, müssen Sicherheitsvorgaben Teil des Vertrags sein.

Nicht die physische Sicherheit vergessen

Es reicht allerdings nicht aus, mögliche Angreifer von außen abzuwehren. Viele Drucker bieten auch lokale Schnittstellen, damit sich zum Beispiel Dateien von einem USB-Speicherstift aus direkt ausdrucken lassen. Auch über diesen Weg lassen sich Schadprogramme einbringen und Druckerspeicher ausspionieren.

Ebenso sollten Unternehmen an Besucher denken, die Ausdrucke mitnehmen, die Beschäftigte am Drucker vergessen haben. Oder an Nutzer, die bereits durchgeführte Druckaufträge nochmals laufen lassen. Hier helfen Berechtigungssysteme und klare Nutzerrichtlinien, die zum Beispiel vorgeben, dass man Ausdrucke zeitnah abholt und insbesondere bei vertraulichen Inhalten sofort zur Stelle ist, um den Ausdruck mitzunehmen.

Kennen Sie die Datenrisiken bei Druckern? Machen Sie den Test!

Frage: Netzwerkdrucker lassen sich nur über das Netzwerk erreichen. Stimmt das?

a) Nein, viele Geräte bieten auch einen Fernzugriff über das Internet an.
b) Ja, deshalb können auch nur Beschäftigte unseres Unternehmens auf den Drucker zugreifen.

Lösung: Die Antwort a) ist richtig. Zum einen bestehen vielfach Verbindungen ins Internet, um den Drucker für Fernwartungen und Firmware-Updates zugänglich zu machen. Zum anderen sind viele Drucker inzwischen für mobile Mitarbeiter erreichbar, die über eine Smartphone-App von unterwegs auf dem Firmendrucker in der Zentrale ausdrucken. Schützen Unternehmen solche Verbindungen ins Internet nicht, können Hacker sie missbrauchen.

Frage: Drucker ohne Netzwerkanschluss sind kein Risiko für den Datenschutz. Stimmt das?

a) Ja, denn Hacker können so nicht auf die Drucker zugreifen.
b) Nein, denn Daten lassen sich auch in Papierform (Ausdrucke) oder über lokale Schnittstellen wie USB stehlen.

Lösung: Die Antwort b) ist richtig. Lassen Beschäftigte Ausdrucke einfach liegen, überwacht das Unternehmen die lokalen Schnittstellen nicht und begrenzt es die Nutzungsrechte am Drucker nicht, können angebliche Besucher über den Drucker und die Ausdrucke an vertrauliche Daten gelangen. Jede Interaktion mit dem Drucker, ob über das Bedienfeld, über den Ausgabeschacht, die lokalen Schnittstellen, das Netzwerk oder das Internet, muss überwacht und abgesichert sein. Drucker sind Teil der Unternehmens-IT und des IoT und brauchen entsprechenden Schutz.