Gemeinsam Außergewöhnliches erreichen

ronau-it
Dipl.-Ing. (FH) Roger Naumer

Datenschutz *Now!*

Die Mitarbeiterzeitung zum Datenschutz

Ausgabe 03/2019

Liebe Leserin, lieber Leser,

um personenbezogene Daten richtig zu schützen, reicht der gute Wille nicht. Man muss genau informiert sein, was man tun darf und was nicht. Wissen Sie zum Beispiel, wie Sie einen Datenträger entsorgen, ohne die darauf befindlichen Daten zu gefährden? Kennen Sie die notwendigen Sicherheitsmaßnahmen, wenn Sie unterwegs einen öffentlichen WLAN-Hotspot nutzen möchten? In dieser Ausgabe Ihrer Datenschutz-Zeitung erfahren Sie, worauf Sie dabei achten müssen.

Risiken für den Datenschutz stehen auch bei den anderen Beiträgen im Mittelpunkt. So erfahren Sie, was es mit der Datenschutz-Folgenabschätzung auf sich hat und welche Folgen Künstliche Intelligenz für den Datenschutz haben kann – nicht erst in Zukunft, sondern bereits heute im beruflichen und privaten Alltag.

Ich wünsche Ihnen interessante Informationen!

Roger Naumer - der Datenschutzbeauftragte Ihres Vertrauens

WLAN-Hotspots: Was Sie für mehr Sicherheit tun können

Wer unterwegs das Internet nutzen möchte, greift gern zu WLAN-Hotspots in Bahnhöfen, Hotels und Geschäften. Doch um die Datensicherheit ist es dabei oftmals nicht gut bestellt. Sorgen Sie deshalb für zusätzliche Schutzmaßnahmen!

Schnell noch das Angebot verschicken

Stellen Sie sich vor, Sie kommen von einem Kundentermin zurück und machen eine kurze Pause in einem Bistro. Eine gute Gelegenheit, das versprochene Angebot auf dem Notebook zu erstellen. Da das mobile Internet in Deutschland Nachholbedarf hat, fragen Sie die Bedienung nach einem WLAN-Zugang. Sie erfahren, dass Sie nicht einmal ein Passwort brauchen, das WLAN ist offen und kostenlos.

Leider ist ein offener WLAN-Hotspot nicht nur ein Grund zur Freude, denn die Sicherheit der Daten kann in Gefahr geraten. Da es aber in vielen Gegenden in Deutschland keine wirkliche Alternative

durch schnelles mobiles Internet gibt, greifen dann doch viele Nutzer zu den WLAN-Angeboten.

Aber bitte nicht ohne zusätzlichen Schutz

Die IT-Sicherheitsbehörde BSI und die Polizei empfehlen, sich vor dem Einloggen in ein öffentliches WLAN-Netzwerk möglichst über das Sicherheitsniveau des Hotspots zu erkundigen.

Trotz möglicher Sicherheitsmaßnahmen wie Verschlüsselung oder Passwortschutz bleibt für den Nutzer stets offen, wer zum Beispiel Zugang zum Router hat und dort Einstellungen vornehmen oder ändern kann.

Bei offenem WLAN sollte man darauf verzichten, sensible persönliche Daten einzugeben, beispielsweise zum Einloggen in E-Mail-Konten, soziale Netzwerke oder beim Online-Banking, so das BSI. Es besteht bei einem freien WLAN immer das Risiko, dass Cyber-Kriminelle solche Daten mitlesen und missbrauchen.

Vorsicht vor dem bösen Zwilling

Eine mögliche Attacke könnte so aussehen, dass ein Datendieb einen Hotspot aufstellt, der vorgibt, der Hotspot des Bistros zu sein. Wenn Sie sich mit diesem „bösen Zwilling“ verbinden, kann der kriminelle Betreiber Ihre Daten abfangen und mitlesen, sofern es keine entsprechende Verschlüsselung gibt (Evil-Twin-Attacke).

Selbst mit Verschlüsselung kann ein bösartiger Hotspot-Betreiber, der natürlich das WLAN-Passwort seines Hotspots kennt, die Daten mitlesen.

Nur eine Ende-zu-Ende-Verschlüsselung zwischen Absender und Empfänger kann hier Schutz bieten.

Mehr Sicherheit bei offenen WLANs

Lässt es sich nicht vermeiden, ein offenes WLAN zu verwenden, achten Sie besonders auf diese Punkte:

- Schalten Sie die WLAN-Funktion nur an, wenn Sie sie brauchen. Nach der Nutzung schalten Sie das WLAN wieder ab.
- Achten Sie auf eine SSL-Verschlüsselung im Webbrowser. Versenden oder holen Sie ohne Verschlüsselung keine vertraulichen Daten ab. Das gilt auch für entsprechende mobile Apps bei Smartphones und Tablets.
- Verwenden Sie einen zuverlässigen VPN-Dienst (Virtual Private Network).
- Deaktivieren Sie Datei- und Verzeichnisfreigaben für andere Nutzer des Netzwerks. Sonst teilen Sie womöglich ungewollt Daten über das WLAN.

Entsorgung von Datenträgern

Fehler bei der Entsorgung von Datenträgern gehören unverändert zu den häufigsten Datenpannen. Eine überraschend große Zahl einschlägiger Verletzungsmeldungen an die Aufsichtsbehörden für den Datenschutz zeigt: Die Aufmerksamkeit bei der Entsorgung von Datenträgern darf nicht nachlassen!

Papier als klassischer Datenträger

Klassischer „Datenträger“ ist Papier. Büros ganz ohne personenbezogene Daten auf Papier sind nach wie vor selten. Fast jeder druckt gelegentlich eine E-Mail aus. Und Notizzettel aller Art finden sich auch fast überall.

All dies landet im Papierkorb. Hoffentlich im richtigen. Denn sollte zum Beispiel für Kunststoffabfälle auch noch ein „gelber Sack“ bereitstehen, findet immer wieder so mancher Zettel seinen Weg unzulässigerweise dorthin.

Altbestände

Oft gibt es noch „Altbestände“ in Form von Ordnern voller Papier oder auch in Form von Schachteln voller loser Blätter. Der Grund: Relativ viele Unterlagen müssen aus rechtlichen Gründen eine bestimmte Zeit aufbewahrt werden. Sie sind daher noch vorhanden, obwohl im Übrigen vielleicht inzwischen rein elektronisch gearbeitet wird. Oft genug erfolgt dabei die Aufbewahrung länger, als es rechtlich erforderlich wäre.

Die Punkt-Methode

Ob Ordner wirklich noch gebraucht werden, lässt sich leicht feststellen. Man legt neben das Ordnerregal Klebepunkte. Wer tatsächlich auf einen Ordner zugreift, bringt auf ihm einen Klebepunkt an. Schon nach einigen Wochen zeigt sich erfahrungsgemäß: Auf fast keinem Ordner klebt ein Punkt.

CDs und USB-Sticks

CDs und USB-Sticks sind weiterhin in vielen Büros anzutreffen. Das gilt sogar dann, wenn ihre Verwendung längst untersagt wurde und sie die Mitarbeiter mangels entsprechender Anschlussmöglichkeit am PC überhaupt nicht mehr benutzen können.

Pannen aus schlechtem Gewissen

Solche Datenträger, die eigentlich nicht mehr da sein dürften, werden besonders häufig vorschriftswidrig entsorgt. Irgendwann tauchen sie in Schubladen oder Schränken auf. Man erinnert sich, dass es einmal eine Anordnung gab, all diese Dinge bis zu einem bestimmten Termin zu entsorgen. Leider geschah das nicht. Und jetzt scheut man sich, das zuzugeben.

Statt die zuständigen Stellen im Unternehmen einzuschalten, geschieht die Entsorgung irgendwie. Schlimmstenfalls im heimischen Hausmüll oder gar im Abfalleimer des nächsten öffentlichen Parks. All

dies kommt in der Realität leider vor.

Entsorgung = Vernichtung

Wesentlich ist bei jeder Entsorgung von Datenträgern, die einschlägigen Vorgaben einzuhalten. Entsorgung bedeutet im Normalfall, dass der Datenträger vernichtet werden muss.

Das geschieht meist durch Zerkleinerung des Datenträgers. Die entsprechenden Vorgaben sind etwas für Fachleute. Der einzelne Mitarbeiter muss sie nicht beherrschen. Es liegt jedoch in seiner Verantwortung, Datenträger an die Stellen im Unternehmen weiterzuleiten, die sich um die Entsorgung kümmern.

Folgen etwaiger Pannen

Kommt es bei der Entsorgung von Datenträgern zu ernsthaften Pannen, findet das oft große Beachtung in der Öffentlichkeit.

Das gilt vor allem dann, wenn Unbefugte beispielsweise Papier aus offenen Behältern mitnehmen konnten. Der Weg des Vorfalls in die Medien ist dann kurz. Zwingende Folge ist zudem eine Meldung an die zuständige Datenschutz-Aufsichtsbehörde, dass der Datenschutz verletzt wurde.

All dies lässt sich durch entsprechende Sorgfalt vermeiden.

Einige unbequeme Fragen

Jede Mitarbeiterin und jeder Mitarbeiter sollte sich mit folgenden Fragen auseinandersetzen:

- Mit welchen Datenträgern, auf denen sich personenbezogene Daten befinden, arbeite ich?
- Welche Datenträger dieser Art bewahre ich auf, obwohl ich sie gar nicht mehr benutze?
- Verfüge ich noch über Daten, deren Vernichtung früher schon einmal angeordnet wurde?
- Kenne ich die Vorgaben dafür, wie lange solche Datenträger aufbewahrt werden müssen?
- Weiß ich, wohin ich Datenträger zur Vernichtung bringen kann?
- Gibt es in unserem Unternehmen irgendwelche Anweisungen oder Vorgaben zu dem Thema (beispielsweise im Intranet)?

Durchaus darüber reden

Sinnvoll ist es, das Thema auch mit Kolleginnen und Kollegen einmal zu diskutieren. Dabei stellt sich meist schnell heraus, wo die Schwachstellen liegen, ob am eigenen Arbeitsplatz oder am Arbeitsplatz der Kolleginnen und Kollegen.

In jedem Fall aber handeln

Wichtig ist es aber, nicht nur zu reden, sondern auch praktische Konsequenzen zu ziehen. Sie können das Thema nicht sofort angehen, weil zu viel anderes zu tun ist? Dann machen Sie sich eine Notiz im Terminkalender, wann Sie auf das Thema zurückkommen wollen. Dann muss es aber wirklich sein!

Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung ist etwas, das es vor der Datenschutz-Grundverordnung (DSGVO) so nicht gab. Sie funktioniert nur, wenn alle Abteilungen im Unternehmen ihren Beitrag dazu leisten. Deshalb sollte jede Mitarbeiterin und jeder Mitarbeiter wissen, was es damit auf sich hat.

Normales und hohes Risiko

Jede Verarbeitung von Daten kann Risiken für den Datenschutz mit sich bringen. Bei manchen Technologien können diese Risiken höher sein als üblich. Ein Beispiel: Bei Verfahren der Gesichtserkennung fallen Bilddaten in großen Mengen an. Nicht immer ist überschaubar, wozu sie möglicherweise missbraucht werden könnten.

Risikominimierung als Zweck

Die Datenschutz-Folgenabschätzung soll Risiken erfassen und sie möglichst abwenden. Am Beispiel der Gesichtserkennung lässt sich gut zeigen, was damit gemeint ist. Es geht nicht darum, solche Verfahren generell zu verbieten. Möglicherweise sind die anfallenden Daten jedoch nur kurze Zeit erforderlich und können dann gelöscht werden. Schon damit lässt sich oft ein etwaiges Missbrauchsrisiko ausreichend eindämmen.

Ablösung von Meldepflichten

Auch wenn mancher dies auf den ersten Blick anders empfindet – das Verfahren der Datenschutz-Folgenabschätzung soll gegenüber der Situation vor der DSGVO eine Vereinfachung bringen. Vor der DSGVO gab es für bestimmte Verfahren, die als riskant empfunden wurden, Meldepflichten an die Aufsichtsbehörde für den Datenschutz. Solche Meldepflichten gibt es jetzt nicht mehr. An ihre Stelle ist die Folgenabschätzung durch die Unternehmen selbst getreten.

Vorprüfung für alle Verfahren

Gesetzlich angeordnet ist eine Datenschutz-Folgenabschätzung nur dann, wenn eine Datenverarbeitung voraussichtlich ein hohes Risiko für den Datenschutz mit sich bringt. So regelt es Art. 35 Abs. 1 DSGVO. Ein hohes Risiko liegt nach dieser Regelung beispielsweise nahe, wenn ein Unternehmen neue Technologien verwendet oder wenn die Verarbeitung große Mengen von Daten betrifft.

Eigentlich soll es also nicht notwendig sein, jedes neue Verfahren einer Datenschutz-Folgenabschätzung zu unterwerfen. Ein Unternehmen muss jedoch erst einmal feststellen, ob diese Voraussetzungen im konkreten Fall vorliegen. Deshalb ist für jedes neue Verfahren zumindest eine kurze Überprüfung notwendig, ob möglicherweise eines der Kriterien erfüllt ist, die zu einer Folgenabschätzung zwingen. Sollte dies der Fall sein, schließt sich daran die eigentliche Datenschutz-Folgenabschätzung an.

Fragen korrekt beantworten!

Dies ist der Hintergrund dafür, dass Mitarbeiterinnen und Mitarbeiter künftig bei jeder Einführung eines neuen Verfahrens damit rechnen müssen, dass Fragen in diese Richtung gestellt werden. Es ist wichtig, sie korrekt zu beantworten. Nur so lässt sich unnötiger Aufwand vermeiden. Häufig wird sich herausstellen, dass gerade keine besonderen Risiken vorliegen. Damit ist die Angelegenheit erledigt, und eine Datenschutz-Folgenabschätzung findet gerade nicht statt.

Sollte eine Datenschutz-Folgenabschätzung nötig sein, dann erfolgt sie sinnvollerweise parallel zur Entwicklung oder – wenn ein fertiges Verfahren eingekauft werden soll – jedenfalls vor dem Echteinsatz der Verarbeitungstätigkeit.

Verarbeitung sensibler Daten

Wenn es um sensible Daten geht, wird besonders häufig eine Datenschutz-Folgen-abschätzung nötig sein. Sensible Daten sind etwa medizinische Daten oder auch Daten über strafrechtliche Verurteilungen. Dass sensible Daten verarbeitet werden, ist jedoch nur ein erstes Indiz. Wenige sensible Daten, die nicht den Kern der Verarbeitung bilden, zwingen nicht zu einer Folgenabschätzung. Anders sieht es dagegen aus, wenn solche Daten im Zentrum der Verarbeitung stehen.

Biometrische Daten und Persönlichkeitsprofile

Sehr häufig wird eine Folgenabschätzung notwendig sein, wenn es um biometrische Daten geht. Dazu gehören etwa Gesichtsbilder oder Fingerabdrücke. Außerdem liegt sie dann besonders nahe, wenn umfassende Persönlichkeitsprofile Verwendung finden.

Aufwand und Ertrag

Natürlich löst eine Datenschutz-Folgenabschätzung Arbeit aus. Dem steht aber gegenüber, dass sie im Ergebnis häufig Ärger vermeidet. Oft lassen sich Risiken für den Datenschutz durch relativ einfache Maßnahmen begrenzen. Neben der schon erwähnten rechtzeitigen Löschung von Daten kommt dabei beispielsweise eine intensive Information der betroffenen Personen in Betracht. Manchmal sind auch zusätzliche Maßnahmen gegen unbefugten Zugriff erforderlich. Im Normalfall geht es also gerade nicht darum, auf die Verarbeitung bestimmter Daten völlig zu verzichten.

Künstliche Intelligenz ist keine Zukunftsmusik

Wenn sich Datenschützer vermehrt mit Künstlicher Intelligenz (KI) befassen, hat das einen guten Grund: KI hält Einzug in Beruf und Privatleben. Doch die KI ist oftmals nicht einfach zu erkennen, ebenso wenig die damit verbundenen Datenrisiken.

KI nicht nur in der IT-Abteilung

Eine aktuelle Studie des Dienstleisters Robert Half zeigt: Künstliche Intelligenz wird immer mehr zur Top-Priorität. Fast die Hälfte der deutschen IT-Entscheider (45 %) möchte in den nächsten beiden Jahren in Projekte zu KI investieren und damit die IT-Strategie im Unternehmen unterstützen.

Offensichtlich hat KI eine große Zukunft in der Unternehmens-IT. Doch es wäre weit gefehlt, zu

glauben, KI sei nur ein Zukunftsthema. Bestimmte Formen von KI sind bereits jetzt im Einsatz, sowohl in Firmen als auch in Privathaushalten.

Verbraucher sehen KI eher positiv

Eine Studie von Adesso zeigt: Sprachassistenten in Smartphones, Navigationssysteme in Autos oder die Gesichtserkennung von Foto- und Video-Apps – immer mehr Menschen nutzen bereits KI, ohne sich groß darüber den Kopf zu zerbrechen. Für 83 % steht fest, dass KI in Zukunft viele lästige Aufgaben übernehmen und das Leben erleichtern kann. 61 % glauben, dass KI ihnen künftig Vorteile bringen wird. Nur eine Minderheit von 29 % hat bei dem Thema Bedenken.

Für einen intelligenten Supermarkt können sich in der Umfrage 57 % begeistern. Jeden Artikel, den der Verbraucher in seinen Einkaufskorb legt, erkennt ein im Supermarkt installiertes Kamerasystem dank KI-gestützter Bilderkennungssoftware. Der Kunde kann den Laden mit seinen Waren ohne Kassenvorgang verlassen. Die Bezahlung erfolgt automatisch durch Belastung des Kundenkontos mit dem Rechnungsbetrag, den Kassenzettel gibt es digital per App.

Datenschützer nehmen KI in den Fokus

Künstliche Intelligenz wird Teil des Alltags und bringt dabei neue Risiken für den Datenschutz mit sich. Datenschützer haben deshalb die sogenannte Hambacher Erklärung zur Künstlichen Intelligenz veröffentlicht. In der Erklärung nennen die Aufsichtsbehörden für den Datenschutz beispielhaft den Einsatz von KI-Systemen in der Medizin, insbesondere in der Diagnose, in der Sprachassistenz und bei der Bewertung von Bewerbungsunterlagen in der Bewerberauswahl.

Für ihre Entwicklung, also für das maschinelle Lernen, benötigen KI-Systeme große Datenmengen. Dabei verarbeiten sie häufig auch personenbezogene Daten. Dadurch ist das Recht des Einzelnen auf Datenschutz und Privatsphäre berührt, so die Datenschützer. Oftmals wissen die betroffenen Nutzer aber gar nicht, dass eine KI ihre Daten verarbeitet.

Beispiel: KI in einem Online-Shop

Wer zum Beispiel einen Webshop nutzt, kann bereits mit einer KI in Kontakt kommen. Eine intelligente Suche muss in der Lage sein, die Absicht des Nutzers zu erkennen und so passende Produktvorschläge zu ermitteln, auch wenn der Nutzer sie in der Suche nicht klar benennen kann. Die KI kann dabei die Suche des Nutzers untersuchen. Mittels der erweiterten Suchanfrage und anhand ähnlicher Anfragen, die die KI schon untersucht hat, kann der Online-Shop dem Nutzer eine individuelle Liste an Artikeln und zudem weiterführende Informationen anzeigen.

Dazu verarbeitet die KI allerdings Daten des Nutzers, ohne dass der betroffene Nutzer darüber informiert wäre oder zugestimmt hätte. Ein Beispiel von vielen, in denen KI personenbezogene Daten auswertet, schon jetzt und in Zukunft noch wesentlich stärker.

Es sollen weiterhin Menschen über Menschen entscheiden

Die Datenschutzaufsichtsbehörden wollen den Fortgang von KI begleiten und fordern Wissenschaft, Politik und Anwender auf, die Entwicklung von KI im Sinne des Datenschutzes zu steuern. Im Kern geht es darum, dass am Ende Menschen und nicht Maschinen über Menschen entscheiden.

Erkennen Sie den Einsatz einer KI? Machen Sie den Test!

Frage: Wenn ein Online-Shop eine KI verwendet, um Nutzerdaten auszuwerten, informiert der Betreiber entsprechend. Stimmt das?

a. Nein, leider fehlen oft die Hinweise auf die KI-Nutzung und die Datenschutz-Folgen.
b. Ja, man findet Hinweise auf eine KI grundsätzlich in der Datenschutzerklärung des Webshops.

Lösung: Die Antwort a. ist richtig. Denn bisher findet man in einer Datenschutzerklärung kaum einen Hinweis darauf, dass eine KI verwendet wird, um Nutzerdaten zu bestimmten Zwecken zu analysieren. Die Nutzer haben auch kaum eine Möglichkeit, die Datenverarbeitung durch die KI abzulehnen.

Frage: Verarbeitet KI personenbezogene Daten, erfolgt dies sicher, transparent und datensparsam. Stimmt das?

a. Ja, denn KI-Systeme werden genauso entwickelt.
b. Nein, die Datenschützer fordern dies, aber bisher kann man leider nicht einfach davon ausgehen.

Lösung: Die Antwort b. ist richtig. In der Hambacher Erklärung haben die Aufsichtsbehörden für den Datenschutz unter anderem klargestellt, dass sich aus dem geltenden Datenschutzrecht Anforderungen ableiten lassen, die KI bereits heute einhalten muss. So muss der Einsatz von KI-Systemen nachvollziehbar und erklärbar sein, den Grundsatz der Datenminimierung enthalten, Diskriminierungen vermeiden sowie technische und organisatorische Standards beachten.

Impressum

Redaktion:

Roger Naumer
Datenschutzbeauftragter

Anschrift:

ronau-it, Dipl.-Ing.(FH) Roger Naumer
Am Wiesgraben 3
67245 Lambsheim

Telefon: +49 (0)6233/459-2833
E-Mail: kontakt@ronau-it.de