Newsletter Datenschutz
Ausgabe 05 | 2017

Datenschutz *Now!*

Die Mandantenzeitung von AdOrga Solutions

Liebe Leserin, lieber Leser,

viele Datenschutzverletzungen passieren ungewollt. Ohne es zu ahnen, kann man zum Gehilfen der Datendiebe werden, indem man die Daten unzureichend schützt. Erfahren Sie in dieser Ausgabe, was Sie tun können, um nicht selbst zum Innentäter zu werden.
Fehler im Datenschutz können schnell geschehen, zum Beispiel im Umgang mit E-Mails an ausgeschiedene Mitarbeiter. Wir klären diesmal auch, was es mit sogenannten Sperrvermerken auf sich hat. Kommen neue Technologien zum Einsatz, ist ebenfalls Vorsicht angebracht. So zum Beispiel bei VR-Brillen. Virtuelle Realitäten (VR) finden sich inzwischen auch am Arbeitsplatz. Sowohl privat als auch beruflich drohen dabei aber Risiken für Ihre Daten. Die schöne Scheinwelt hat es in sich!

Ich wünsche Ihnen viel Spaß beim Lesen!
Ihre Regina Mühlich, Datenschutzbeauftragte

VR-Brillen: Ein Thema für den Datenschutz?

Virtual Reality (VR) ist einer der Top-Trends der Unterhaltungselektronik. Auch am Arbeitsplatz kommen bereits VR-Brillen zum Einsatz. Dabei sind nicht nur virtuelle Welten im Blick, sondern auch Sie als Nutzer.

VR ist keine Vision, sondern Realität

Jeder elfte Deutsche hat bereits eine der Virtual-Reality-Brillen ausprobiert. Fast jeder Dritte kann sich vorstellen, dies künftig zu tun, so eine Umfrage des Digitalverbands Bitkom.

Wenn Sie noch keine VR-Brille aufgesetzt haben: VR-Brillen präsentieren einen Bildschirm direkt vor Ihren Augen und decken das gesamte Sichtfeld ab. Dadurch schauen Sie direkt in die Bilder und Videos und sind scheinbar Teil der virtuellen Umgebung. Selbst wenn Sie nach oben, nach unten oder zur Seite blicken: Die virtuelle Realität umgibt Sie.

Nicht nur Online-Spiele erhalten so einen neuen Erlebniswert. Es profitieren auch berufliche Anwendungen. Bitkom nennt als Beispiele Piloten, die in virtueller Umgebung die Flugzeugbedienung üben, und Ärzte, die riskante Eingriffe digital simulieren. Architekten und Städteplaner können begehbare Entwürfe erstellen. Reiseanbieter können eine Vorschau auf touristische Sehenswürdigkeiten bieten, bevor die Urlauber vor Ort sind.

Der Nutzer steht im Fokus

Bei Virtual Reality hat man als Nutzer das Gefühl, mitten im Geschehen zu sein. Auch wenn das nur virtuell ist: Tatsächlich stehen Sie als Träger einer VR-Brille im Mittelpunkt. Sie wählen das VR-Video aus, das gezeigt wird, Sie installieren die VR-Anwendungen. Mit den führenden VR-Brillen sind spezielle App-Stores verknüpft, bei denen Sie ein Nutzerprofil anlegen.

Je nach Anbieter können Sie sogar Ihr Online-Profil von Facebook oder einem anderen sozialen Netzwerk mit Ihren VR-Anwendungen verknüpfen, Ihre VR-Erlebnisse bei Facebook & Co. teilen und mit Facebook-Freunden innerhalb einer VR-Anwendung kommunizieren.

Eine interessante Erfahrung, aber auch ein mögliches Datenrisiko: VR-Brillen

Sehen und gesehen werden

Selbst wenn Sie keine Verknüpfung zu Facebook herstellen - um ein Nutzerkonto werden Sie kaum herumkommen. Dort lässt sich protokollieren, was Sie sich angesehen haben. Tatsächlich ist es nicht nur geplant, in VR-Anwendungen passende Werbung zu machen, es geschieht schon. Dazu werden Ihre VR-Nutzungsgewohnheiten analysiert.

Mehr noch: Je nach Modell verfügt die VR-Brille über Mikrofon und Kamera, oder Sie stecken Ihr Smartphone in die VR-Brille, das über diese Funktionen verfügt. Mit Kamera und Mikrofon können Sie Kommandos geben, per Sprache oder per Blickkontakt mit der VR-Anwendung. Selbst Fotos und Videos von Ihren Erlebnissen können Sie damit machen.

Vergessen Sie aber nicht: Die Anbieter der VR-Erlebnisse könnten Sie als Nutzer analysieren, Datendiebe Sie sogar über die integrierte Kamera von Smartphone oder VR-Brille heimlich bei der Nutzung der Brille beobachten. Befassen Sie sich deshalb mit dem Datenschutz, bevor Sie in virtuelle Welten eintauchen. Denn die Datenrisiken sind real.

Ausgeschiedene Mitarbeiter als Adressaten von E-Mails - was tun mit den Mails?

Ein Mitarbeiter scheidet aus dem Unternehmen aus. Kann der Arbeitgeber den Mail-Account des Mitarbeiters einfach schließen? Wie ist mit E-Mails umzugehen, die ausdrücklich an ihn gerichtet sind? Das Bayerische Landesamt für Datenschutzaufsicht bietet in seinem Tätigkeitsbericht für 2015/2016 einige Orientierungshilfen für diese Fragen.

Existieren schon Regelungen?

Vorab sei auf Folgendes hingewiesen: Falls zu diesem Thema eine Betriebsvereinbarung existiert, ist alles klar. Es gelten ihre Regelungen. Manchmal treffen das Unternehmen und der ausscheidende Mitarbeiter auch eine ausdrückliche Vereinbarung, etwa in einem Aufhebungsvertrag. Schön für alle Beteiligten! Denn das schafft Klarheit.

Und wenn nicht?

Aber was ist, wenn es an Beidem fehlt? Vielleicht lässt sich noch über eine einvernehmliche Regelung reden. Aber manchmal erscheint das kaum vorstellbar, etwa nach einer fristlosen Kündigung. In solchen Fällen hilft die Meinung der Datenschutzaufsicht weiter.

Schließung des Mail-Accounts

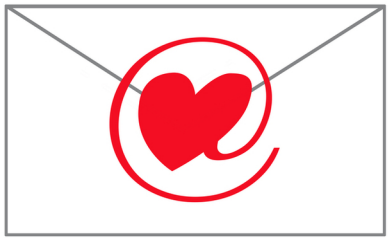
Zunächst zu der Frage, wie lange ein Mail-Account noch bestehen darf. Etwa drei Monate nach dem Ausscheiden sollte er nach Auffassung des Landesamts geschlossen werden. Der Grund: Danach ist nicht mehr damit zu rechnen, dass noch Mails an den ausgeschiedenen Mitarbeiter eingehen. Eine ausdrückliche gesetzliche Regelung dazu gibt es aber nicht.

Private Nutzung erlaubt oder nicht?

Schwieriger ist eine Antwort auf die Frage, ob Mails, die noch eingehen, an einen anderen Mitarbeiter weitergeleitet werden dürfen. Hier unterscheidet das Landesamt danach, ob der Arbeitgeber die private E-Mail-Nutzung erlaubt hat oder nicht.

Falls private Nutzung verboten ist ...

Relativ freie Hand hat der Arbeitgeber, wenn er die private E-Mail-Nutzung verboten hat. In diesem Fall kann er einfach festlegen, dass eine Weiterleitung erfolgt. Denn private Mails können dann ja eigentlich keine eingehen.



Aha, spannend, welche Mails der Ex-Kollege so bekommen hat ...

Im Einzelfall kann dies aber trotzdem vorkommen. Denn immer wieder gibt es Absender, die nicht wissen, dass die private Nutzung verboten ist, oder denen das egal ist.

Umgang mit einzelnen privaten Mails

Sofern eine private Mail im Unternehmen weitergeleitet wird, darf der Empfänger ihren Inhalt nicht lesen. Das gilt naturgemäß nur dann, wenn er schon am Absender und/oder am Betreff erkennen kann, dass die Mail privaten Charakter hat. Eine solche Mail ist entweder zu löschen oder an den ausgeschiedenen Mitarbeiter weiterzusenden.

Falls private Nutzung erlaubt ist ...

Falls der Arbeitgeber private Mails erlaubt hat, handelt es sich um eine freiwillige Leistung des Arbeitgebers. Das führt jedoch nicht dazu, dass er einfach die Weiterleitung aller eingehenden Mails anordnen kann. Vielmehr muss er dann das Fernmeldegeheimnis beachten.

Einwilligung nötig

Ohne eine Einwilligung des ausgeschiedenen Mitarbeiters wäre eine Weiterleitung privater Mails daher nicht zulässig. Andererseits dürfte dann auch niemand in den Account schauen, um dienstliche und private Mails zu trennen.

Das Ergebnis: Der Account wäre letztlich insgesamt blockiert. Für viele Unternehmen ist das nicht akzeptabel.

Übliche Bedingungen für private Nutzung

In der Praxis ist deshalb üblich, dass der Arbeitgeber private Mails nur unter Bedingungen erlaubt:

Bedingung 1: Der Arbeitnehmer erklärt sich damit einverstanden, dass Mails, die nach seinem Ausscheiden eingehen, an einen anderen Mitarbeiter weitergeleitet werden.

Bedingung 2: Er ist außerdem damit einverstanden, dass dieser andere Mitarbeiter den Betreff und den Absender aller eingehenden Mails prüft. Hat eine Mail danach erkennbar privaten Charakter, öffnet er sie nicht. Je nach Vereinbarung löscht er sie oder leitet sie an den ausgeschiedenen Mitarbeiter weiter.

Eigenes Smartphone als Lösung?

Falls private Mails erlaubt sind, geht es also nicht ohne relativ komplizierte Vereinbarungen. Das ist ein wichtiger Grund dafür, warum viele Unternehmen auf dienstlichen Geräten nur dienstliche Mails erlauben.

Viele Mitarbeiter haben ohnehin ständig ihr privates Smartphone dabei. Private Mails schreiben sie von dort aus. Mit den Inhalten solcher Mails hat der Arbeitgeber nichts zu tun. Datenschutzprobleme gibt es keine.

Folgeprobleme anderer Art

Allerdings: Mailen ist hier eine private Tätigkeit während der Arbeitszeit. Ob und in welchem Umfang sie erlaubt ist, sollte man klären, bevor es Ärger gibt. Selbstverständlich ist eine solche Erlaubnis auf keinen Fall.

Außerdem: Probleme kann auch der umgekehrte Fall bereiten. Ein Arbeitnehmer benutzt sein privates Smartphone, um dienstliche Mails zu verschicken. Auch das ist nicht einfach so erlaubt.

Impressum

Redaktion:
Regina Mühlich (V.i.S.d.P.)
Datenschutzbeauftragte

Anschrift:
AdOrga Solutions
Drachenseestr. 15
D-81373 München
Telefon: +49 (0)89 411 726 - 34
E-Mail: info@adorgasolutions.de

Interne Sperrvermerke für gefährdete Kunden?

Bürger, die persönlich gefährdet sind, können von Behörden in manchen Registern "Sperrvermerke" eintragen lassen. Ihre Daten dürfen dann entweder gar nicht weitergegeben werden oder nur unter besonderen Vorsichtsmaßnahmen. Hat das Auswirkungen darauf, wie ein Unternehmen mit Daten solcher Personen umgehen darf?

Schutz gefährdeter Personen durch Behörden

Jeder, der eine Wohnung bezieht, muss sich beim Einwohnermeldeamt anmelden. Seine Daten kommen ins Melderegister. Normalerweise ist das eine völlig unspektakuläre Angelegenheit.

Es gibt allerdings auch Spezialfälle. So kann es vorkommen, dass ein Polizist persönlich gefährdet ist, weil sich Kriminelle an ihm rächen wollen. Er kann dann beantragen, dass für ihn im Melderegister eine Auskunftssperre eingetragen wird. Die Sperre soll verhindern, dass seine Adresse den falschen Leuten in die Hände fällt.

Auskünfte über die aktuelle Anschrift sind ohne eine solche Sperre relativ leicht zu erhalten. Zwar muss man dabei zumindest den Namen und den Vornamen der gesuchten Person nennen können. Gerade bei seltenen Namen stellt das aber keine große Hürde dar.

Auswirkungen auch auf Unternehmen?

So weit, so gut. Bis dahin ist das eine behördeninterne Angelegenheit, die Unternehmen normalerweise nicht weiter interessiert. Das ändert sich freilich sofort, wenn ein solcher Bürger mit Auskunftssperre von einem Unternehmen verlangt, ihn ebenfalls besonders zu schützen. Solche Forderungen häufen sich inzwischen.

Teils extreme Forderungen von Kunden

Manche Kunden gehen sogar so weit, dass sie verlangen, auch im Unternehmen so etwas wie eine interne Auskunftssperre zu bekommen. Sie soll bewirken, dass normale Unternehmensmitarbeiter keinen Zugriff mehr auf die Daten dieses Kunden haben. Ein Zugriff soll nur noch ausgewählten, besonders vertrauenswürdigen Mitarbeitern möglich sein.

Was auf den ersten Blick durchaus nachvollziehbar wirken mag, behindert bei näherem Hinsehen die Arbeitsabläufe erheblich. Gäbe es einen solchen Anspruch, müsste die Datenverarbeitung entsprechend angepasst werden. Außerdem wären besondere Mitarbeiter auszuwählen. Also alles keine Kleinigkeiten!

Position der bayerischen Datenschutzaufsicht

Das Bayerische Landesamt für Datenschutzaufsicht hat in seinem Tätigkeitsbericht 2015/2016 klar Position bezogen, wie mit solchen Forderungen umzugehen ist. Es hebt Folgendes hervor:

- Unternehmen dürfen Daten ohnehin nur verarbeiten, wenn dies für die Tätigkeit des Unternehmens erforderlich ist.

- Ist diese Voraussetzung gegeben, dürfen alle Mitarbeiter Zugriff auf die Daten erhalten, die sie für ihre Arbeit brauchen. So muss etwa die Buchhaltung auf die Daten aller Kunden zugreifen können, bei denen noch eine Rechnung offen ist.

- Zugriffsbeschränkungen, die darüber hinausgehen, kann kein Kunde verlangen. In den Datenschutzgesetzen, die für Unternehmen gelten, gibt es keine Regelungen über so etwas wie Sperrvermerke oder Auskunftssperren.

- Ist im Register einer Behörde ein Sperrvermerk, eine Auskunftssperre oder etwas dergleichen eingetragen, dann hat dies nur für die Arbeit dieser Behörde Bedeutung. Auswirkungen auf Unternehmen ergeben sich dagegen nicht.

Vorsicht vor Überinterpretationen!

Dies ist eine wichtige Klarstellung. Sie darf allerdings auch nicht überinterpretiert werden. So kann Folgendes vorkommen:

- In einem Einwohnermelderegister ist für einen Bürger eine Auskunftssperre wegen Gefährdung eingetragen.

- Ein Unternehmen möchte vom Einwohnermeldeamt die aktuelle Anschrift dieses Bürgers erfahren. Der Grund: Es ist noch eine Rechnung offen, und der Bürger ist umgezogen, ohne dem Unternehmen seine neue Anschrift zu melden.

- Nach einigen Wochen teilt die Behörde die aktuelle Anschrift schließlich mit. Dabei macht sie allerdings eine besondere Auflage. Sie legt fest, dass die Anschrift nur für den Zweck verwendet werden darf, um den es bei der Anfrage ging. Das ist gewissermaßen der Preis dafür, dass das Unternehmen die Anschrift erhält, obwohl eine Auskunftssperre eingetragen ist.

Erst denken, dann Daten weitergeben!

Folge für die Praxis: Die Adresse darf nur zu dem Zweck verwendet werden, den Kunden wegen der konkreten Rechnung anzusprechen. Unzulässig wäre es dagegen, ihm beispielsweise Werbung an diese Adresse zu schicken. Und dass jegliche Weitergabe der Anschrift an Stellen außerhalb des Unternehmens verboten ist, versteht sich von selbst.

Das gilt auch, wenn "befreundete Unternehmen" anfragen, die ebenfalls nach der aktuellen Anschrift suchen.

Im Normalfall haben behördliche Sperrvermerke keine Auswirkungen auf die Behandlung der betroffenen Daten im Unternehmen. Es gibt aber Ausnahmen.

Eine bange Frage: Bin ich ein Innentäter?

Innentäter gelten als eines der größten Risiken für die Datensicherheit in Unternehmen. Nicht die Hacker von außen verursachen die meisten Vorfälle, sondern die sogenannten Insider. Gehören Sie auch dazu?

Insider gibt es nicht nur an der Börse

Sicherlich haben Sie in den Nachrichten schon einmal von Insider-Handel gehört. Bei diesem Vergehen geht es darum, dass jemand sein internes Wissen dazu missbraucht, um Vorteile beim Kauf oder Verkauf von Wertpapieren zu erzielen. Auch im Datenschutz gibt es Insider-Wissen, im Prinzip hat dies jede Mitarbeiterin und jeder Mitarbeiter, der mit personenbezogenen Daten umgeht, also zum Beispiel mit Kundendaten.

Zusätzlich haben Insider Berechtigungen, Daten zu lesen, zu ändern oder zu löschen. Werden diese Berechtigungen missbraucht, spricht man von einer Insider-Attacke.

Keine Sorge, niemand will Ihnen nachsagen, dass Sie eine Insider-Attacke planen oder so etwas jemals getan hätten. Doch vielleicht sind Sie trotzdem ein Innentäter, ohne es zu wissen oder zu ahnen.

Innentäter sind es meist ohne Vorsatz

Die meisten Insider-Vorfälle resultieren aus Nachlässigkeit oder Unwissenheit: So enthalten beispielsweise rund 16 Prozent der Dokumente, die in einer Cloud, also einem Online-Datenspeicher abgelegt werden, sensible Informationen, so eine Studie von Skyhigh Networks.

Diese Dateien dürften deshalb nie in einen ungeschützten Online-Speicher kopiert werden, aber es passiert trotzdem. Durch falsch definierte Zugriffsberechtigungen stehen einige dieser Dokumente dann sogar noch der breiten Öffentlichkeit zur Verfügung. Das geschieht zwar nicht mit Absicht. Es kann aber schwerwiegende Konsequenzen haben.

Fahrlässige Nutzer: ein großes Risiko

Unternehmen sehen laut einer Splunk-Umfrage derzeit die größten Risiken in

- Computer-Viren (67 Prozent),

- hochentwickelten, andauernden Bedrohungen (Advanced Persistent Threats) (42 Prozent),

- Phishing-Attacken (28 Prozent) und

- fahrlässig handelnden Nutzern (27 Prozent).

Das können Nutzer sein, denen persönliche Zugangsdaten entwendet wurden. Diese Nutzer haben sich dann nicht gut genug geschützt und interne IT-Sicherheitsrichtlinien nicht eingehalten. Solche Nutzer werden ungewollt zu Gehilfen der Hacker und Datendiebe.

Denken Sie an Selbstdatenschutz und die internen Vorgaben

Tatsächlich ist so manche Mitarbeiterin und so mancher Mitarbeiter Innentäter, ohne wirklich Täter zu sein. Ungewollt machen sie es den echten Tätern, den Datendieben, aber leicht, an die zu schützenden Daten zu kommen.

So werden Daten nicht verschlüsselt, bevor sie auf einem USB-Stick gespeichert werden, oder das Firmen-Smartphone ist so eingestellt, dass das Gerätepasswort nicht mehr eingegeben werden muss, da dies lästig erschien.

Oder Mitarbeiter holen vertrauliche Ausdrucke nicht vom Drucker ab. Gedruckte Kundenlisten landen im Papierkorb und nicht im Papier-Schredder. Die Liste möglicher Fehler ließe sich beliebig fortsetzen.

Wichtig ist es, dass Sie sich immer klarmachen, dass Sie zum Innentäter werden könnten, ohne es zu wollen, dadurch es aber den Datendieben ermöglichen, schnell und einfach an die Daten der Kunden, Lieferanten oder Beschäftigten zu kommen. Denken Sie deshalb an den Selbstdatenschutz, werden Sie aktiv, indem Sie Ihre Daten und die der anderen schützen. Was genau zu tun ist, erfahren Sie in der Datenschutzschulung und in den Datenschutzrichtlinien.

Wenn Sie sich daran halten, können Sie mit Fug und Recht sagen: Ich bin kein Innentäter, ich schütze mein Insiderwissen und trete aktiv für den Datenschutz ein! Gut so!

Kennen Sie die Gefahren einer Virtuellen Realität (VR)? Machen Sie den Test!

Frage: Mit VR-Brillen schaut man sich Scheinwelten an, echte Gefahren lauern dort nicht. Stimmt das?

a) Ja, denn VR steht für Virtuelle Realitäten, die echte Welt hat damit nichts zu tun.
b) Nein, denn die VR-Brille selbst ist eine echte Realität. Stimmt hier der Datenschutz nicht, bestehen Datenrisiken.

Lösung: Die Antwort b) ist richtig. Überall im Internet und in Apps können Datenrisiken stecken. Das gilt auch für VR-Apps. Der Bildschirm der VR-Brille präsentiert virtuelle Welten, doch die Brille, die Apps und die Nutzerdaten sind real und deshalb gefährdet.

Frage: Was ich in der VR-Brille anschaue, sehe nur ich. Stimmt das?

a) Nein, denn Dritte können die VR-Nutzung auswerten.
b) Nein, Dritte könnten versuchen, auf die Kamerafunktion zuzugreifen.
c) Ja, denn die VR-Brille schließt dicht ab, keiner kann auf meinen Bildschirm darin schauen.

Lösung: Die Antworten a) und b) sind richtig. Die VR-Brille erscheint abgeschlossen, doch es besteht Verbindung zu den Apps, zum Internet und zum Nutzerkonto. Die VR-Nutzung lässt sich auswerten, die Verbindung zu den VR-Apps kann ausspioniert werden, wenn Datenschutz und Datensicherheit nicht stimmen. VR-Anwendungen brauchen den gleichen hohen Schutz wie mobile Apps und VR-Brillen die gleiche Sicherheit wie mobile Endgeräte. Sonst sieht man als Nutzer nicht nur virtuelle Welten, sondern man wird womöglich auch selbst von Dritten über das Internet gesehen und analysiert.