

Datenschutz Now!

Zeitung für Mitarbeiter und Mandanten



Liebe Leserin, lieber Leser,

vielen im Leben ist nicht so einfach, wie es auf den ersten Blick erscheint. So lassen sich Daten in der Regel nicht schlicht auf Knopfdruck löschen. Lesen Sie deshalb, wie sich Daten wirklich entfernen lassen. Auch die Weitergabe eines Passworts geht nicht so einfach und ist keine kleine Gefälligkeit für einen Kollegen, der kurzfristig auf bestimmte Informationen im Netzwerk zugreifen will. In dieser Ausgabe erfahren Sie, welche Konsequenzen eine solche Weitergabe haben könnte.

Wer Spam-Mails für lästige, aber harmlose Werbe-Mails hält, der irrt leider. Spam im E-Mail-Postfach kann zu einer echten Bedrohung werden. Und selbst beim Shopping sollten Sie nicht leichtfertig Ihre Daten preisgeben. Welche Folgen das für Sie konkret haben kann, erfahren Sie auf Seite 4.

Für Ihre Rückfragen zu diesen wichtigen Themen stehe ich Ihnen gerne zur Verfügung!
Herzlichst Ihr *Jan Wandrey, Datenschutzbeauftragter*

Mit einem Klick ist alles weg?

Elektronische Dokumente zu vernichten, ist scheinbar viel einfacher als die Aktenvernichtung mit dem Papier-Schredder. Ein Klick auf die Entfernen-Taste reicht. Aber ist die entsprechende Datei dann wirklich gelöscht? Leider nein!

Plötzlich war das Foto weg ...

Stellen Sie sich vor, bei der Bearbeitung eines Urlaubsfotos passiert Ihnen ein Malheur. Statt das optimierte Bild zu speichern, löschen Sie es. Zu allem Überfluss leeren Sie auch noch am Abend den elektronischen Abfalleimer im Computer. Am nächsten Tag stellen Sie entsetzt fest, dass eines der Urlaubsfotos fehlt, ein ganz besonderer Schnappschuss. Sie haben ihn versehentlich gelöscht. Das Bild ist unwiederbringlich weg. Wirklich?

Datenretter helfen in der Not

Selbst wenn Sie Ihr Urlaubsfoto gelöscht und den digitalen Papierkorb auf Ihrem Rechner geleert haben, ist das Bild immer noch auf Ihrem Computer. Das Foto wurde nicht wirklich gelöscht, sondern nur aus den sichtbaren Dateiordnern genommen. Mit einem Datenrettungsprogramm können Sie es in kurzer Zeit wiederherstellen. Solche Programme finden Sie kostenlos im Internet.

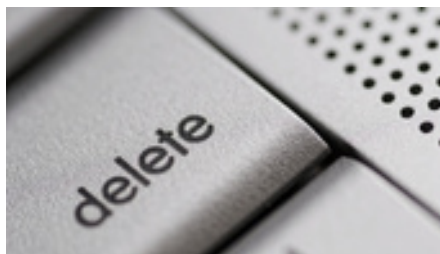
Datenretter machen auch Probleme

Moment, werden Sie jetzt vielleicht sagen. Soll das heißen, dass alle Daten, die ich in der

Firma lösche, auch nicht richtig gelöscht sind? Die Antwort lautet: In aller Regel ja!

Löschen über Windows & Co. reicht nicht

Der einfache Löschbefehl Ihres Computers löscht nicht wirklich. Im ersten Schritt werden die scheinbar gelöschten Dateien in den digitalen Abfalleimer verschoben und können von dort mit einem "Element wiederherstellen" aus dem Papierkorb gezogen werden.



Löschen ist nicht gleich Löschen

Auch ein leerer Papierkorb ist zu wenig

Selbst wenn Sie regelmäßig Ihren Papierkorb auf der Bildschirm-Oberfläche Ihres PC leeren, sind die angeblich gelöschten Dateien nicht wirklich weg. Die Daten liegen weiterhin versteckt auf der Festplatte Ihres Rechners.

Gut für die Urlaubsfotos, schlecht für den Datenschutz

Wenn Sie aber daran denken, dass vertrauliche Daten, die angeblich gelöscht wurden, von jedem, der Zugang zu Ihrem PC hat, wieder zum Vorschein gebracht werden können, ist das mehr als beängstigend!

Auch für Dateien gibt es Schredder

Um elektronische Dokumente sicher und zuverlässig zu vernichten, benötigen Sie wie bei der Aktenvernichtung einen Schredder: einen Datenschredder. Das sind Spezialprogramme, die zum Beispiel die zu löschenden Dateien gezielt mehrfach überschreiben, um eine Wiederherstellung auszuschließen. Fragen Sie Ihren Datenschutzbeauftragten und die Systemadministratoren, welche Datenschredder oder Datenlöschprogramme intern zur Verfügung stehen.

Auch an Kopien und Ausdrucke denken

Doch selbst ein Datenschredder kann nicht alle Daten vernichten, wenn Sie nicht auch an mögliche Kopien der Dateien in anderen Verzeichnissen und an die Ausdrucke denken. Deshalb lautet die Devise: Alle vertraulichen Dokumente, die vernichtet werden sollen, kommen in den Papierschredder, und alle vertraulichen Dateien, die gelöscht werden sollen, in den Datenschredder!

"Psst - du sagst es aber wirklich sonst keinem, ja?"

Knapp 40 % aller Deutschen tun es. Sie geben Passwörter weiter - und zwar im beruflichen Bereich genauso wie privat. Das ergab eine repräsentative Umfrage des IT-Verbandes BITKOM, deren Ergebnis im Juni 2010 veröffentlicht wurde. Der häufigste Grund: So wie man zur Sicherheit einen Hausschlüssel bei einem Freund hinterlegt, gibt man das Passwort für den Fall weiter, dass man es einmal vergessen sollte. Das ist verständlich, aber rechtlich gesehen hoch riskant.

Einmal Hand aufs Herz: Ein wirklich gutes Gewissen hat kaum jemand, wenn er ein Passwort weitergibt. Und irgendwann taucht die Frage auf: Was wäre, wenn ...?

Was wäre, wenn ...?

Wenn nämlich die liebe Kollegin, der gute Freund das Passwort missbrauchen? Wenn der Freund es nutzt, um Infos an die Konkurrenz zu geben, kurz bevor er bei einem Personalabbau entlassen wird? Wenn die Kollegin sauer ist, weil sie meint, ihr sei die Sache mit dem tollen Mann kaputt gemacht worden, und sie jetzt versehentlich oder sogar unbemerkt ein paar wichtige Daten löscht?

Spätestens dann fragen auch Sie sich, wie das denn rein rechtlich aussieht. Und spätestens dann merken Sie, dass es da ganz schön unangenehm werden kann.

Vorsicht im privaten Bereich

Werfen wir zunächst einen Blick in den privaten Bereich. Sie geben die Zugangsdaten für Ihren E-Bay-Account an den Lebenspartner/die Lebenspartnerin weiter. Alles geht gut, solange die Beziehung hält. Er oder sie tut mit dem Account immer nur das, was vereinbart ist.

Aber dann geht die Beziehung auseinander. Und plötzlich haben Sie Verfügungen und Klagen am Hals, weil in Ihrem Namen falsche Angaben gemacht und mangelhafte Waren verschickt werden.

"Ich war das nicht" - und Sie stehen dumm da!

Der/die Ex weist empört alle Schuld von sich. Das sei ja wieder mal typisch, dass Sie alle Verantwortung auf den anderen ... - Sie wissen, wie dann argumentiert wird.

Das Blöde dabei: Beweisen können Sie ihm oder ihr meist gar nichts. Fest steht aber, dass Sie die Zugangsdaten weitergegeben haben. Und da liegt der Verdacht nahe, dass Sie das nicht nur einmal gemacht haben.



Das Weitergeben von Passwörtern kann sowohl im privaten als auch im geschäftlichen Umfeld äußerst unangenehme Folgen haben. Vertrauen Sie weder Partnern noch Kollegen Ihre Zugangsdaten an!

Im privaten Bereich haften Sie voll!

Sie wollen wissen, wie Sie da wieder rauskommen? Kommen Sie am besten erst gar nicht rein! Laut Bundesgerichtshof haften Sie nämlich in einem solchen Fall für alles, was mit Ihrem Account angerichtet wird. Die Entscheidung vom 11. März 2009 ist unter den Stichworten BGH Halzband (genau so geschrieben!) mit jeder Suchmaschine sofort zu finden. Das Risiko kann schnell in die Tausende gehen.

Wie sieht es aber in der Arbeit aus? Was kann Ihnen hier passieren, wenn Sie Ihr Passwort weitergeben?

Sie haben versprochen, das Daten-geheimnis zu beachten!

Jedem dürfte klar sein, dass es gegen den Datenschutz verstößt, wenn der Kollege/die Kollegin mit dem Passwort auf personenbezo-

gene Daten zugreifen kann, die ihn bzw. sie nichts angehen, weil der Zugriff ganz bewusst auf den jeweiligen Sachbearbeiter beschränkt ist.

Vielleicht erinnern Sie sich noch, dass Sie irgendwann einmal darauf verpflichtet wurden, das Datengeheimnis einzuhalten? Und dass Sie diese Verpflichtung auch unterschrieben haben? Dazu passt es natürlich nicht, wenn Sie Passwörter anderen überlassen.

Im Extremfall drohen Abmahnung oder sogar noch Schlimmeres!

Solange nichts passiert, gilt sicher der Grundsatz "Wo kein Kläger, da kein Richter". Aber wenn es einmal nicht gut ausgeht? Dann kommt das böse Stichwort "Abmahnung" ins Spiel. Von schlimmeren Folgen, die arbeitsrechtlich denkbar wären, ganz zu schweigen.

Doch es gibt andere Möglichkeiten!

Jetzt sagen Sie sich vielleicht: Ja, aber was soll ich denn sonst machen, als jemandem mein Passwort zu geben für den Fall, dass ich es vergesse? Nun, im beruflichen Bereich ist das nicht schlimm. Glauben Sie es ruhig: Das passiert öfter, als Sie denken! Es ist auch keine Schande! Die EDV-Administration hilft Ihnen dann weiter.

Mein Account - dein Account

Im privaten Bereich hilft dagegen nur das Prinzip: Mein Account - dein Account, und zwar beide schön getrennt. Und wenn Sie den Account im Augenblick noch teilen, fällt Ihnen doch sicher eine gute und den Anderen nicht verletzende Begründung ein, um das zu ändern. Bloß: Diesen Beitrag sollten Sie dann lieber für sich behalten.

Impressum

Redaktion:
Jan Wandrey
Datenschutzbeauftragter

Anschrift:
wandrey GbR
Andrea Wandrey, Jan Wandrey
Krusauer Strasse 98
12305 Berlin
Telefon: 030 720 10 22 - 30
E-Mail: dsb@wandrey.biz

Spam ist mehr als lästig!

Wenn Sie heute noch keine Spam-Mail bekommen haben, sollten Sie sich diesen Tag im Kalender rot anstreichen. Inzwischen sind 95 Prozent der weltweit versandten E-Mails Spam. Diese lästigen Plagegeister sind aber nicht nur unerwünschte Werbung in Form von E-Mails. Spam ist eine reale Bedrohung für Ihre Daten!

Verlockende E-Mails

Sie haben gewonnen!, Tolles Video vom Traum-Tor oder Re: Ihre Bestellung - die Betreffzeilen von Spam-Mails sind einfallreich, machen neugierig und verleiten dazu, die E-Mail zu öffnen. Der Absender ist angeblich eine Lotteriegesellschaft, ein bekannter Online-Shop, ein Paketdienst oder ein Online-Nachrichtenportal.

Spam-Mails am besten nicht öffnen

Vieles spricht scheinbar dafür, solche Mails zu öffnen. Schließlich wartet ein Gewinn auf Sie, oder Sie können das im Fernsehen verpasste Fußball-Tor sehen, oder aber Sie wollen erfahren, was Sie denn angeblich bestellt haben sollen. Fallen Sie aber nicht auf die Tricks der Spammer herein!



In der Spam-Mail befindet sich meist eine Internetadresse, die Sie anklicken sollen, um die Informationen zur Bestellung oder das Fußball-Video zu sehen. Die Internetadresse würde Sie jedoch im besten Fall zu einem Online-Shop führen, der Ihnen fragwürdige, überbeuerte Produkte andrehen möchte. In der Regel kommt es aber schlimmer.

Trojaner statt Fußball-Video

Die Internetadresse aus der Spam-Mail führt Sie meist zu einer mit Schadsoftware verseuchten Webseite, oder Sie laden sich sofort einen Trojaner auf Ihren Rechner. Dieses böartige Programm nistet sich dann in Ihrem Computer ein und schreibt zum Beispiel Ihre Passwörter mit, kopiert Ihre Adressbücher im E-Mail-Programm und versendet E-Mails in Ihrem Namen, um weitere Opfer zu finden.

Keine Werbung, sondern reale Gefahr

Sie sollten Spam-Mails deshalb nicht mit einer ärgerlichen Werbung verwechseln, die in Ihrem E-Mail-Postfach steckt anstatt unter dem Scheibenwischer Ihres Autos. Bei Spam-Mails ist Vorsicht geboten. Dazu gehört, dass Sie Spam-Mails am besten erst gar nicht öffnen, die darin enthaltenen Internetadressen in jedem Fall nicht anklicken und auch mögliche Dateianhänge wie die angebliche Bestellbestätigung oder Rechnung nicht öffnen.

Spammer werden immer professioneller

Doch wie erkennt man, ob es sich nicht doch um eine echte E-Mail handelt, werden Sie sich jetzt sicherlich fragen. Früher war die Antwort leicht, denn Spam-Mails hatten viele Rechtschreibfehler, richteten sich nicht direkt an den Empfänger und waren fast immer auf Englisch. Heute sind die Spammer wesentlich besser und deshalb noch gefährlicher geworden. Fast jede dritte Spam-Mail nennt den Empfänger beim Namen und nutzt die direkte Anrede genauso geschickt wie eine echte Werbe-Mail.

Anrede und Nachnamen zu der E-Mail-Adresse liefern viele Spam-Opfer selbst, zum Beispiel in ihren Profilen in sozialen Online-Netzwerken wie Facebook oder MySpace.

Wie Sie Spam-Mails trotzdem erkennen

Auch wenn Sie in einer perfekten und auf Deutsch verfassten E-Mail persönlich angesprochen werden, sollten Sie also auf der Hut sein. Achten Sie auf verdächtige Kennzeichen wie:

- konkrete Fragen in der E-Mail zu personenbezogenen Daten, Passwörtern und Bankdaten
- angebliche Support-Mails, die ein Update für die bei Ihnen eingesetzte Software anbieten
- Gewinne, für die Sie nur noch die Bankverbindung angeben müssen

10 Goldene Regeln zum richtigen Umgang mit Spam

1. Überlegen Sie sich zweimal, wem Sie Ihre E-Mail-Adresse geben und wo Sie die E-Mail-Adresse im Internet veröffentlichen. Die Spammer warten schon.
2. Verwenden Sie in privaten sozialen Netzwerken und Online-Foren nicht Ihre Haupt-E-Mail-Adresse, sondern legen Sie sich eine zweite, kostenlose E-Mail-Adresse für diesen Zweck an.
3. Klicken Sie keine Internetadressen in verdächtigen E-Mails an und öffnen Sie keine E-Mail-Anhänge, ohne sie vorher mit einem aktuellen Virens Scanner zu prüfen.
4. Schenken Sie den Angeboten in ungewollten E-Mails keinen Glauben.
5. Misstrauen Sie Newslettern, die Sie nicht abonniert haben.
6. Denken Sie daran, dass der angezeigte E-Mail-Absender gefälscht sein kann.
7. Antworten Sie niemals auf Spam-Mails, auch wenn der Spammer Sie verärgert.
8. Nutzen Sie den lokalen Spam-Filter in Ihrem E-Mail-Programm.
9. Melden Sie Spam-Mails, die Sie regelmäßig im Unternehmen bekommen, Ihrem Mail-Administrator, der den Spam-Filter entsprechend anpassen kann.
10. Melden Sie private Spam-Mails, die regelmäßig kommen, der Internet-Beschwerdestelle unter www.internet-beschwerdestelle.de.

- Bestellbestätigungen oder Rechnungen, die Sie kontrollieren sollen, obwohl Sie nichts bestellt haben
- Antworten auf E-Mails, die Sie nie verschickt haben

Wehret den Anfängen

Viele haben sich an Spam-Mails bereits so gewöhnt wie an Stubenfliegen. Machen Sie es anders und greifen Sie zur digitalen Klatsche! Wie Sie sich vor Spam-Mails am besten schützen, zeigen Ihnen die 10 Goldenen Regeln.

Was ist eigentlich im Umgang mit Kundendaten zulässig?

Sie sind selbst Kunde, etwa wenn Sie Kleider kaufen, und Sie haben in unserem Unternehmen mit Menschen als Kunden zu tun. Wahrscheinlich haben Sie in der letzten Zeit gelesen, dass die Vorschriften für den Umgang mit Daten von Kunden verschärft worden sein sollen. Was ist da dran, worauf sollten Sie privat und im Unternehmen achten?

Das Ganze ist an sich harmlos, aber Sie fragen sich trotzdem, ob das wirklich so sein darf: Kürzlich haben Sie in einem großen Modegeschäft in der Stadt eine Hose gekauft. Die war zu lang, also haben Sie sie nach dem Kauf im Laden gelassen, damit sie gekürzt wird. Dabei wurde Ihre Adresse aufgeschrieben.

Über den kleinen Schreibfehler beim Straßennamen haben Sie geschmunzelt, aber Sie wollten die nette Verkäuferin, eine junge Ausländerin, nicht belehren. Jetzt halten Sie schon den zweiten Werbefrief in Händen, bei dem genau dieser Schreibfehler in der Adresse auftaucht.

Der Zweck, für den Ihre Daten bestimmt sind, wurde geändert

Damit ist Ihnen klar: Die Anschrift, die Sie eigentlich nur angegeben haben, weil die Hose kürzer zu machen war, wird jetzt verwendet, um Ihnen Werbung zu schicken, die Sie sonst nie bekommen hätten. Ihre Adresse wird also für einen Zweck genutzt, den Sie nicht erkennen konnten, als Sie die Adresse im Geschäft genannt haben.

Das Gesetz enthält dazu eine eigene Regelung

Alles bloß rechtliche Spitzfindigkeiten? Dem Gesetzgeber war das Ganze immerhin so wichtig, dass er genau zu dieser Frage eine eigene Regelung in das Bundesdatenschutzgesetz aufgenommen hat! Sie lautet im Ergebnis: Wenn Sie die Adresse eines Kunden nutzen, um für die Produkte des eigenen Unternehmens zu werben, ist das in Ordnung.

Unternehmen dürfen Daten austauschen - aber es besteht dann eine Hinweispflicht

Wie sieht es aber aus, wenn ein anderes Unternehmen die Daten bekommen soll? Nehmen wir einmal folgendes Beispiel: Sie stehen umsatzmäßig etwas unter Druck. Neue Kunden müssen her. Ein befreundetes Unternehmen hat interessante Adressen und wäre auch bereit, sie ausnahmsweise sogar

gratis zur Verfügung zu stellen. Geht das?

Vorsicht! Beide Unternehmen sind rechtlich selbstständig. Es geht also nicht um Werbung für Produkte des eigenen Unternehmens, sondern um die Produkte eines anderen Unternehmens. Dass beide befreundet sind, ist im Datenschutzrecht ohne Bedeutung.

Herkunft der Daten muss erkennbar sein

Für diesen Fall sagt das Bundesdatenschutzgesetz: Die Daten dürfen zwar weitergegeben werden. Aber für den Adressaten der Werbung muss zu erkennen sein, woher sie stammen. Ob das den Werbeeffekt stört oder nicht, spielt dabei keine Rolle.

Beide Unternehmen müssen also überlegen, ob sie damit leben können, dass der Adressat durch einen Zusatz im Anschreiben oder einen ähnlichen Hinweis erfährt, dass seine Daten weitergegeben wurden. Oft wird ihm das egal sein - aber man muss sich das vorher überlegen, bevor er vielleicht verärgert ist.

Der Adressat der Werbung kann künftige Werbung verhindern

Vielleicht sagen Sie sich nun: Na und, ist er halt verärgert, das stört mich nicht. Doch auch hier gilt: Vorsicht! Der Adressat von Werbesendungen kann nämlich jederzeit mitteilen, dass seine Daten nicht mehr für Zwecke der Werbung verwendet werden dürfen. Dann muss seine Adresse in allen Datenbanken des Unternehmens gesperrt werden.

Das macht einigen Aufwand und ist vor allem dann ärgerlich, wenn das Unternehmen dafür bezahlt hat, dass es die Daten von einem anderen Unternehmen bekommt. Dann heißt es: Außer Spesen nichts gewesen!

Die Regelungen gelten noch nicht für alte Adressbestände

Ihnen kommt das alles recht neu vor? Kein Wunder, die entsprechenden Vorschriften wurden erst im Jahr 2009 eingeführt. Entscheidender Stichtag war der 1. September 2009. Für alte Adressbestände, die an diesem Tag schon vorhanden waren, gelten noch ältere, viel großzügigere Regelungen. Allerdings nur bis längstens 31. August 2012 - also nicht einmal mehr zwei Jahre.

Ab dann gilt ohne jede Ausnahme: Die neuen Regeln müssen beachtet werden, damit es nicht zu einstweiligen Verfügungen durch die Konkurrenz und Ärger mit dem Verbraucherschutz kommt!

Wissenstest Kundendaten: Wer darf was?

1. Sie hinterlassen Ihre Adresse in einem Geschäft, damit Ihnen eine Ware zugeschickt werden kann, die nicht vorrätig war. Darf das Geschäft diese Adresse verwenden, um Ihnen Kataloge zuzuschicken?

Antwort: Ja. Damit werden die Daten zwar für einen anderen Zweck verwendet. Das lässt das Bundesdatenschutzgesetz aber ausdrücklich zu, wenn das Geschäft für eigene Produkte wirbt, die es selbst beschafft und liefert.

2. Sie wollen sich von einem befreundeten Unternehmen Adressen geben lassen, um sie für die Werbung zu nutzen. Was müssen Sie beachten?

Antwort: Sie müssen klären, ob die Adressen aus einem Bestand stammen, der am 1. 9. 2009 schon vorhanden war. Davon hängt es ab, welche Vorschriften gelten. Wurde der Adressbestand erst nach diesem Tag angelegt, müssen Sie den Adressaten der Werbung darüber informieren, dass die Adressen von dem anderen Unternehmen stammen.

3. Können Sie als Adressat von persönlicher Werbepost verlangen, dass Ihre Adresse nicht mehr für Werbung genutzt wird?

Antwort: Ja, jederzeit, und zwar ohne dass Sie dafür Gründe nennen müssen!