

Datenschutz Now!

13

Das Datenschutz-Infoblatt



Liebe Leserin, lieber Leser,

bleibt die Kundenakte geöffnet auf dem Schreibtisch liegen, könnte schon der nächste Besucher mehr sehen, als er sehen darf. In dieser Ausgabe erhalten Sie deshalb Tipps, wie der Datenschutz in Ihrem Büro aussehen sollte. Zusätzlich erfahren Sie, welche Gefahren von scheinbar harmlosen PDF-Dateien ausgehen, die Sie als E-Mail-Anhang bekommen oder als digitales Dokument von einer Webseite herunterladen.

Nach Feierabend sollten Sie den Datenschutz weiterhin im Blick behalten, sonst könnten Sie etwa an der Haustür selbst schnell in den Fokus anderer geraten. Lesen Sie in dieser Ausgabe, was bei der Videoüberwachung erlaubt ist und was nicht. Testen Sie auch unbedingt, ob Sie schon wissen, was es mit den besonders sensiblen Daten auf sich hat.

Ich wünsche Ihnen viele wichtige Erkenntnisse mit dieser Ausgabe und stehe gerne für Rückfragen zur Verfügung! Ihr *Gilbert Staffler, Datenschutzbeauftragter*

Machen Sie reinen Tisch!

Ordnung im Büro ist nicht das halbe Leben, aber grundlegend für den Schutz personenbezogener Daten. Komplette Kundenlisten im Papierkorb, vertrauliche Akten offen auf dem Schreibtisch: Ihr Beitrag zum Datenschutz sollte anders aussehen!

Endlich Feierabend!

Die Bearbeitung der Kundenanfrage dauert wieder einmal lange. Bald ist Feierabend. Gleich morgen früh wollen Sie die Arbeit fortsetzen. Eigentlich könnten Sie doch die Akte gleich auf dem Schreibtisch liegen lassen ...

Kommen Ihnen diese Gedanken bekannt vor? Schnell ist man versucht, den Schreibtisch so zu verlassen, dass es am nächsten Tag gleich weitergehen kann. Doch Vorsicht! Sie haben vielleicht Feierabend. Datendiebe und Industriespione fangen jetzt erst an.

Nicht nur eine Frage der Organisation

Wenn Sie vor der Mittagspause, vor dem Feierabend und immer dann, wenn Sie länger nicht im Büro sind, Ihren Schreibtisch aufräumen, ist dies nicht nur ein Zeichen für eine gute persönliche Organisation. Ein aufräumter Schreibtisch gehört zum zwingend nötigen Schutz für vertrauliche Daten.

Statt die Kundenakte, die Visitenkarten-Box oder die Telefonliste auf dem Schreibtisch liegen zu lassen, sollten Sie alle Unterlagen, die

personenbezogene Daten wie Namen, Adressen und Telefonnummern enthalten, wegräumen. Allerdings reicht es nicht, vertrauliche Papiere in die Schublade oder in den Schrank zu legen, Sie sollten auch abschließen und den Schlüssel nicht stecken lassen.



Kein Vorbild für den Datenschutz im Büro ...

Tafeldienst nicht nur in der Schule

Wenn Sie Informationen, die nicht für die Öffentlichkeit bestimmt sind, auf einer Tafel oder einem Flipchart notieren, sollten Sie auch diese Datenspuren beseitigen. Man kann nie wissen, wer diese Informationen andernfalls zu Gesicht bekommt.

Mobile Geräte bitte verschließen

Wenn Sie ein Notebook als Arbeitsplatzrechner verwenden, sollte es gegen Diebstahl

gesichert sein, zum Beispiel mit einem Notebook-Schloss. USB-Sticks und Smartphone lassen Sie ebenfalls nicht einfach im Büro liegen, wenn Sie es verlassen. Schließen Sie mobile Geräte und Speichermedien weg, wenn Sie sie nicht mitnehmen. Das gilt auch für CDs und DVDs.

Schlüssel nicht vergessen

Bei den Schlüsseln für Schreibtisch, Schrank und Bürotür ist es wie mit Ihren elektronischen Passwörtern: Vergessen oder liegen lassen bringt personenbezogene Daten in Gefahr. Denken Sie deshalb immer an Ihre Schlüssel, die Sie sicher aufbewahren sollten.

Schredder statt Papierkorb

Alte Kundenlisten oder Telefonverzeichnisse sind nicht einfach Altpapier für den Papierkorb. Nutzen Sie den nächstgelegenen Schredder, um die Daten auf den alten Papierdokumenten unleserlich zu machen. Datendiebe durchsuchen nicht nur Büros, die unaufgeräumt verlassen wurden, sie durchwühlen auch bevorzugt den Papiermüll!

Datensicherheit besteht nicht nur aus Verschlüsselung, Antivirenschutz und sicherem Löschen. Der Schutz personenbezogener Daten beginnt bereits auf dem eigenen Schreibtisch. Aufräumen, Wegschließen und Schreddern gehören zum Datenschutz unbedingt dazu!

PDF: Weit verbreitet und brandgefährlich!

Sie sehen auf dem Bildschirm aus wie gedruckt und lassen sich auf den meisten Computern öffnen. PDF-Dateien sind ideal für den Austausch von Dokumenten. Doch leider sind sie auch perfekt als Angriffswerkzeug.

Trojaner statt Konferenzeinladung

Endlich kam die Bestätigung zur Tagung in Las Vegas, an der das Rüstungsunternehmen im Auftrag des US-Verteidigungsministeriums teilnehmen wollte. Die E-Mail des Konferenzveranstalters verwies auf das angehängte PDF, worin sich weitere Informationen befinden sollten. Ein Klick auf die PDF-Datei öffnete ein Memo zur Tagung - doch die Information war gefälscht, und das PDF-Dokument trug einen Trojaner in sich. Die Industriespionage konnte beginnen.

PDF-Attacken passieren laufend

Dieser Angriff fand ganz gezielt statt, doch PDF-Attacken sind keine Seltenheit. Dokumente im PDF-Standard (Portable Document Format) werden inzwischen für mehr als 25 Prozent aller Angriffe mit Schadprogrammen genutzt.

Das hat einen guten Grund: PDF-Dateien lassen sich durch die hohe Verbreitung des Adobe-Reader-Programms auf mehr als 90 Prozent aller Computersysteme öffnen und lesen. Damit besteht ein enormes Potenzial für PDF-Attacken, das sich die Datendiebe nicht entgehen lassen.

PDFs sind nicht nur digitale Ausdrücke

Die Beliebtheit von PDF-Dateien bei Anwendern und bei Datendieben zugleich hat noch einen weiteren Grund: PDFs sehen aus wie die digitalen Abbilder eines Ausdrucks und werden deshalb bevorzugt für Produktbroschüren, Verträge oder Einladungen verwendet. Der Absender einer PDF-Datei weiß mit großer Sicherheit, wie seine digitale Publikation beim Empfänger aussehen wird. Der Empfänger jedoch ahnt meist nicht, was alles in einer PDF-Datei stecken kann, zur Freude der Hacker und Datendiebe.

Mächtige Funktionen, hohes Risiko

So beliebt PDF-Dokumente auch sind, die meisten Anwender unterschätzen sie. Eine PDF-Anwendung wie der Adobe Reader ist kein einfaches Anzeigeprogramm für digitale Dokumente. Vielmehr sollten Sie sich PDF-Programme vorstellen wie vollwertige Browser, nur dass sie PDF-Dateien statt Web-

seiten anzeigen. Genau wie eine Webseite kann eine PDF-Datei Video-Elemente, Flash-Animationen und Hyperlinks ins Internet enthalten. Die Multimedia-Elemente, die Animationen und die Links in den PDFs können ebenso verseucht sein wie bei einer Webseite.

Das gilt natürlich auch für alle PDF-Dateien, die Sie auf Ihrem Privatrechner daheim öffnen.



Mit den richtigen Einstellungen sind Sie auch bei PDFs auf der sicheren Seite

Kennen Sie schon die sicheren PDF-Einstellungen?

Um sich vor Angriffen über PDF-Dateien besser zu schützen, sollten Sie bestimmte Einstellungen bei Ihrem PDF-Programm vornehmen. Vielen Anwendern sind diese weder bekannt, noch wird die Notwendigkeit zur Absicherung des Adobe Reader gesehen. Machen Sie es anders und wehren Sie sich gegen die zunehmenden PDF-Attacken, auch auf Ihrem Privat-PC:

- PDF-Dateien können gefährliche Befehle in sich tragen, die den Computer manipulieren und Daten stehlen wollen. Dazu missbrauchen die Angreifer die JavaScript-Funktion in Adobe Reader. Stellen Sie diese Funktion bei Ihrem Adobe Reader deshalb ab (Bearbeiten > Voreinstellungen > JavaScript > bei "Acrobat JavaScript aktivieren" den Haken entfernen).

- Öffnen Sie PDF-Dateien nicht, ohne sie zuvor mit Ihrem Antivirenprogramm geprüft zu haben, ganz gleich, woher Sie die PDF-Datei erhalten haben. Auch wenn der

Absender der E-Mail und die Quelle der PDF-Datei scheinbar bekannt und seriös sind, beide Angaben können leicht gefälscht sein.

- Klicken Sie in den Trefferlisten der Suchmaschinen nicht einfach auf Ergebnisse im PDF-Format. Dadurch würden Sie die jeweilige PDF-Datei automatisch öffnen oder herunterladen. Nutzen Sie vorab eine Software zur Prüfung des Suchtreffers (Link-Scanner).

- Achten Sie darauf, dass auch Ihr Adobe Reader automatisch aktualisiert wird (Menüpunkt Bearbeiten > Voreinstellungen > Updater).

- Nutzen Sie die Hilfefunktion in Adobe Reader, um darüber ein Update zu starten, wenn Sie von Ihrem Systemadministrator erfahren, dass der Adobe Reader aktualisiert werden muss. Klicken Sie nicht auf den Link in einer E-Mail, die Ihnen angeblich ein Update oder eine neue Version für Adobe Reader anbietet.

- Prüfen Sie, ob Sie auf Ihrem Rechner bereits die aktuellste Version des Adobe Reader verwenden. Ab der Version Adobe Reader X werden PDF-Dateien nur noch im sogenannten geschützten Modus gestartet. Dadurch können manipulierte PDF-Dateien nicht mehr ohne Weiteres auf kritische Bereiche Ihres Rechners zugreifen, was frühere Versionen im Standard nicht verhinderten.

- Nutzen Sie das Internet nicht, wenn Sie als lokaler Administrator an Ihrem Computer angemeldet sind. Andernfalls könnte eine PDF-Attacke Ihre Zugriffsrechte auf dem Rechner übernehmen.

Wenn Sie diese Sicherheitshinweise beachten und eine aktive Firewall sowie ein aktuelles Antivirenprogramm einsetzen, können Sie die offensichtlichen Vorteile von PDF-Dokumenten nutzen, ohne ein Opfer von Datendieben zu werden!

Impressum

Redaktion:
Gilbert Staffler
Datenschutzbeauftragter

Anschrift:
EHS-Datentechnik
Uhlendahlweg 24
45279 Essen
Telefon: 0201-530091
E-Mail: info@ehs-datentechnik.de

Überwachung von Mietern mit Video - ist so etwas zulässig?

Wenn Sie als Mieter in einer Wohnanlage mit Videokameras überwacht werden, kann das reine Schikane sein. Andererseits: Manchmal fühlt man sich dadurch sogar sicherer. Ein neues Urteil zeigt recht deutlich, wo die Grenze zwischen "erlaubt" und "verboten" verläuft.

Plötzlich sind überall Kameras

Sie haben eine Wohnung in einer größeren Wohnanlage gemietet. Aus beruflichen Gründen sind Sie einige Wochen im Ausland. Als Sie wiederkommen, stellen Sie fest, dass der Eingangsbereich des Gebäudes und die Briefkastenanlage mit Videokameras überwacht werden. Sie fragen nach und erfahren, dass die Eigentümerversammlung das so beschlossen hat.

Geht das so einfach, oder hätte man Sie und die anderen Mieter um Erlaubnis fragen müssen?



Videoüberwachung in Wohnanlagen ist nur unter ganz bestimmten Voraussetzungen zulässig

Hätten die Eigentümer die Erlaubnis der Mieter haben müssen?

Genau vor dieser Frage stand das Amtsgericht Saarbrücken. Es hakte genauer nach, warum die Kameras eigentlich installiert worden waren. Dabei stellte sich heraus, dass es in der Wohnanlage immer wieder zu Vandalismus gekommen war. Mal wurden Briefkästen aufgebrochen, in einigen Fällen gab es Einbrüche in Wohnungen. Einige Wohnungen wurden dabei komplett verwüstet.

Die angerichteten Schäden waren erheblich

Vor diesem Hintergrund hatte das Gericht durchaus Verständnis für den Beschluss der Eigentümerversammlung. Dabei fiel ins Gewicht, dass die angerichteten Schäden erheblich waren. Seit die Kameras installiert waren, hatte es jedenfalls an der Briefkastenanlage keinerlei Beschädigungen mehr gegeben. Auch die sonstigen Beschädigungen in der Wohnanlage waren stark zurückgegangen. Beides registrierte das Gericht sehr aufmerksam.

Die Interessen der Mieter werden durchaus berücksichtigt

Allerdings ist nicht zu übersehen, dass die Kameras schon zu einem gewissen Überwachungsdruck gegenüber den Mietern führen. Wer will sich schon jedes Mal filmen lassen, wenn er durch die Haustür geht oder wenn er an der Briefkastenanlage seine Post abholt? Deshalb fragte das Gericht auch danach, wie die Kameras denn im Einzelnen arbeiten. Dabei stellte sich Folgendes heraus:

- Die Kameras speichern zwar Bilder. Sie sind seitens der Wohnungsverwaltung jedoch nicht an Bildschirme angeschlossen, auf denen man die Bilder anschauen könnte.

- Lediglich dann, wenn Beschädigungen vorgekommen sind und die Polizei deshalb die Bilder sehen möchte, werden die gespeicherten Bilder entweder an die Polizei übergeben oder nach deren Vorgaben von dem Unternehmen, das die Kameras installiert hat, ausgewertet.

- Nach einer Woche werden die Aufzeichnungen jeweils durch neue Aufzeichnungen überspielt (früher als Endloschleife bezeichnet) und sind dann nicht mehr sichtbar zu machen.

Eine Erlaubnis der Mieter war nicht nötig

Auf dieser Basis hält das Gericht die Videoüberwachung für zulässig, ohne dass es not-

wendig war, die Mieter vorher um Erlaubnis zu fragen. Die Interessen der Mieter seien ausreichend gewahrt. Davon geht das Gericht deshalb aus, weil die Mieter erkennen können, dass eine Überwachung stattfindet.

Hinzu kommt, dass die Bilder schon nach einer Woche wieder gelöscht werden. Kommt es nicht zu Beschädigungen, findet auch keine Auswertung statt.

Die Entscheidung ist kein Freibrief für die Eigentümer

Nur auf den ersten Blick kann die Entscheidung des Gerichts so wirken, als könnte eine Eigentümerversammlung künftig einfach beschließen, wegen eher harmloser Beschädigungen überall Videokameras aufhängen zu lassen. Genau besehen besagt die Entscheidung jedoch gerade das Gegenteil!

Nur weil die Beschädigungen erheblich waren und auch längere Zeit andauerten und weil die Aufzeichnungen nur dann ausgewertet werden, wenn dazu wirklich Anlass besteht, hat das Gericht die Überwachung für zulässig erklärt. Hinzu kam, dass eine Auswertung durch die Wohnungsverwaltung selbst in keinem Fall erfolgt.

Letzte Instanz bleibt die Polizei

Stets hat die Polizei sozusagen die Hand darauf, ob und was ausgewertet wird. Und die Polizei hält sich an die Spielregeln, die in den Gesetzen für Maßnahmen der Strafverfolgung vorgesehen sind. Von einem Freibrief kann also keine Rede sein!

Haken Sie als Mieter nach!

Sollten Sie deshalb feststellen, dass in Ihrer Wohnanlage plötzlich Kameras auftauchen, fragen Sie ruhig einmal genauer nach!

Fragen Sie, wer das beschlossen hat, was genau aufgezeichnet wird, wer die Aufzeichnungen ansehen kann, unter welchen Voraussetzungen eine Auswertung erfolgt und wer die Auswertung vornimmt.

Wenn das alles zufriedenstellend beantwortet wird, können Sie die Kameras mit einem guten Gefühl akzeptieren.

Was sind eigentlich "besonders sensible Daten"?

Der Begriff ist weit verbreitet. In den Datenschutzgesetzen findet er sich freilich nicht. Dort ist die Rede von "besonderen Arten personenbezogener Daten". Und für solche Daten gelten besonders strenge Vorschriften. Unter anderem ist eine "Vorabkontrolle" vorgesehen. Aber um welche Daten geht es eigentlich? Und was soll eine Vorabkontrolle? Erfahren Sie hier mehr!

Das persönliche Empfinden ist sehr unterschiedlich

Welche Daten über eine Person als besonders sensibel anzusehen sind, hängt sehr von den Umständen und stark vom persönlichen Empfinden ab. Dazu ein Beispiel: Der eine möchte auf keinen Fall, dass jemand erfährt, in welcher Gewerkschaft er ist. Der andere erwähnt das bewusst überall und versucht beständig aktiv, neue Gewerkschaftsmitglieder zu gewinnen.

Das Gesetz muss von genauen Begriffen ausgehen

Weil die Auffassungen so unterschiedlich sind, kann das Gesetz es nicht vom Einzelfall abhängig machen, welche Daten es als besonders sensibel bewertet. Maßstab kann vielmehr nur sein, welche Daten von den meisten Menschen als besonders heikel angesehen werden.

Diesen Weg geht das Bundesdatenschutzgesetz in § 3 Absatz 9. Der Absatz lautet: "Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben."

Das Gesetz bewertet nur bestimmte Daten als besonders sensibel

Für das Beispiel der Mitgliedschaft in einer Gewerkschaft gilt somit: Diese Angabe wird vom Gesetz als besonders sensibel bewertet, mögen die Meinungen darüber auch geteilt sein. Dasselbe gilt für die Mitgliedschaft in einer Partei, denn sie berührt "politische Meinungen".

Nicht besonders sensibel wäre dagegen die Angabe der Nationalität, also etwa die Angabe "Herr A besitzt die italienische Staatsangehörigkeit." Anders sieht es aus, wenn gesagt wird: "Herr A ist ein dunkelhäutiger Afrikaner." Das weist nämlich auf seine rassische oder ethnische Herkunft hin.

Dass Angaben über die Gesundheit besonders sensibel sind, dürfte jedem klar sein. Und das Sexualleben geht natürlich erst recht niemand anderen etwas an.

Bei sensiblen Daten ist eine Vorabkontrolle nötig

Schön und gut, sagen Sie sich nun vielleicht. Aber welche praktische Bedeutung hat es denn etwa im Unternehmen, wenn mit "besonderen Arten personenbezogener Daten" umgegangen wird? Zunächst einmal hat dies formale Folgen, auf die zu achten ist. Wenn beispielsweise irgendein EDV-Verfahren solche Daten enthält, muss der Datenschutzbeauftragte des Unternehmens eine Vorabkontrolle durchführen.

Die Vorabkontrolle soll die Beachtung schwieriger Datenschutzvorschriften sicherstellen

Wie der Begriff schon sagt, muss diese Überprüfung stattfinden, bevor das Verfahren eingesetzt wird, also nicht erst dann, wenn es etwa zu Beschwerden kommt.

Das hat seinen guten Grund: Für die Daten, die das Gesetz als besonders sensibel ansieht, gelten nämlich in vielfacher Hinsicht besondere Vorschriften. Sie sind im Einzelnen recht kompliziert, und deshalb muss der Datenschutzbeauftragte schon im Vorfeld ganz besonders darauf achten, dass sie beachtet werden.

Das liegt im Interesse des Unternehmens

Bedenkt man, wie empfindlich die Öffentlichkeit inzwischen auf angebliche oder wirkliche "Datenschutzskandale" reagiert, dann ist ein solches Verfahren keine Förmlichkeit, die nur den Betrieb aufhält. Vielmehr sorgt es dafür, dass es erst gar nicht zu Pannen kommt.

Was hat es mit "besonders sensiblen Daten" auf sich?

Frage: Ihr schwerbehinderter Kollege hat bei einem Unfall beide Beine verloren und benutzt einen Rollstuhl. Schwerbehinderte mit Rollstuhl erhalten Parkplätze besonders nahe am Eingang. Welche Mitarbeiter diese Berechtigung haben, ist in einer besonderen "Parkliste Schwerbehinderte" in der EDV festgehalten. Handelt es sich um eine Liste mit besonderen Arten personenbezogener Daten?

- a) Nein, die Angabe der Schwerbehinderung ist nicht besonders sensibel, denn jeder sieht ja auf den ersten Blick, dass der Kollege im Rollstuhl sitzt.
- b) Eigentlich ja, aber das spielt keine Rolle, weil die Liste den dort registrierten Kollegen ja nur Vorteile bringt.
- c) Ja, denn das Merkmal Schwerbehinderung sagt etwas über die Gesundheit der in der Liste erfassten Kollegen aus.

Lösung: Ausschließlich richtig ist hier Antwort c). Es kommt lediglich darauf an, dass das Merkmal objektiv etwas über die Gesundheit aussagt.

Frage: Muss eine solche Liste dem Datenschutzbeauftragten vorgelegt werden, damit er eine "Vorabkontrolle" durchführen kann?

- a) Ja, denn es muss zum Beispiel genau überprüft werden, wer alles auf diese Liste zugreifen kann.
- b) Nein, das wäre bloß eine sinnlose Formalität, weil die Angabe der Schwerbehinderung ja zutrifft.
- c) Ja, das Gesetz legt das für Fälle, in denen es um Gesundheitsdaten geht, schematisch und ohne Ausnahme so fest.

Lösung: Richtig sind die Antworten a) und c). Antwort c) beschreibt, wie die Rechtslage ist, und Antwort a) nennt einen der Gründe dafür, warum eine solche Regelung geschaffen wurde.