Infobrief Datenschutz
Ausgabe 12 | 2010

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

das Thema Datenschutz ist ein Dauerbrenner in den Medien. Aber fühlen Sie sich umfassend informiert? Wissen Sie zum Beispiel, unter welchen Voraussetzungen es erlaubt ist, Firmenfahrzeuge zu orten, und wann nicht? Über den neuen elektronischen Personalausweis haben Sie sicherlich schon viel in den Medien gehört. Aber wurden auch alle für den Datenschutz relevanten Aspekte genannt?

Ebenfalls kaum aus den Schlagzeilen kommen Suchmaschinen wie Google. Doch kennen Sie zum Beispiel bereits das Datenrisiko, das in den Links der Trefferlisten versteckt sein kann? Für weitere Unklarheit sorgen sogar Sicherheitsfunktionen wie der Private Modus Ihres Webbrowsers. Bietet Ihnen diese Funktion wirklich eine sichere Privatsphäre im Internet, oder verspricht sie zu viel?

Durchblick bei solch sensiblen Fragen verschafft Ihnen diese Ausgabe Ihrer Mitarbeiterzeitung. Für Rückfragen stehe ich Ihnen gerne zur Verfügung, Ihr *Udo Wenzel, Datenschutzbeauftragter*

Das war nicht ich - es war nur mein Personalausweis!

Seit dem 1. November 2010 gibt es einen neuen Personalausweis. Billig ist er nicht, im Normalfall kostet er 28,80 Euro. Dafür hat er zusätzliche Funktionen, vor allem eine Online-Ausweisfunktion. Sollten Sie diese Funktion lieber von der Ausweisbehörde ausschalten lassen? Oder können Sie sie risikolos benutzen?

Einen Personalausweis muss jeder Deutsche besitzen, so steht es im Gesetz. Einzige Ausnahme: Ein gültiger Reisepass ersetzt auch den Personalausweis.

Es gibt drei Zusatzfunktionen

Wenn Sie seit dem 1. November einen neuen Ausweis beantragen, werden Sie recht überrascht sein. Beim Beantragen des Ausweises werden Sie nämlich darüber informiert, dass mit dem Ausweis jetzt viel mehr möglich ist als früher:

1. Wer will, kann (ohne Zusatzkosten) Fingerabdrücke auf dem Ausweis speichern lassen. Wenn man Glück hat, kann diese hoheitliche Biometriefunktion Grenzkontrollen beschleunigen.

2. Wer bei einem entsprechenden privaten Anbieter zusätzlich Geld investiert, kann auf dem Ausweis eine qualifizierte elektronische Signatur speichern lassen. Diese Unterschriftsfunktion steht rechtlich gesehen einer klassischen Unterschrift gleich.

3. Schließlich gibt es (ohne Zusatzkosten) eine Online-Ausweisfunktion. Sie ist herstellerseitig aktiviert, wird aber auf Ihren Wunsch von der Behörde ausgeschaltet.

Die Online-Ausweisfunktion können Sie auf verschiedene Arten nutzen

In der Offline-Welt lässt sie sich verwenden, um bei Versicherungsanträgen und Ähnlichem die Basisdaten - vor allem Name und Anschrift - rasch und fehlerfrei in Formulare zu übernehmen. In der Online-Welt des Internet lässt sie sich zum Beispiel benutzen, um das Alter nachzuweisen.

Für die Online-Funktion müssen Sie eine sechsstellige PIN festlegen

Das Ganze funktioniert nur, wenn Sie als Ausweisinhaber eine sechsstellige PIN festlegen und sie bei jeder Benutzung des Ausweises eingeben. Bevor Sie den Ausweis bei Ihrer Gemeinde abholen können, erhalten Sie per Post einen PIN-Brief. Er enthält eine fünfstellige PIN. Nachdem Sie diese Transport-PIN eingegeben haben (bei der Gemeinde oder über ein eigenes Lesegerät auch zuhause), können Sie diese Transport-PIN durch eine sechsstellige PIN ersetzen. Erst mit ihr lässt sich die Online-Ausweisfunktion verwenden.

Wer die PIN hat, kann so tun, als sei er Sie!

Die beiden PINs dienen der Sicherheit. Doch wehe, wenn ein Unbefugter Ausweis *plus* PIN in die Finger bekommt! Gelingt ihm das mit der Transport-PIN, kann er eine sechsstellige PIN festlegen, die Sie gar nicht kennen, und damit unter Ihrem Namen handeln! Haben Sie schon eine sechsstellige PIN festgelegt, kann er ebenfalls unter Ihrem Namen loslegen.

In beiden Fällen ist der perfekte Identitätsdiebstahl mithilfe eines amtlichen Dokuments geglückt!

So sieht der neue Personalausweis aus (Bild: BMI)

Schützen Sie sich!

Gegen solche Manipulationen helfen nur zwei Dinge: Entweder Sie lassen die Funktion ausschalten, wenn Sie den Ausweis abholen. Oder Sie passen auf, dass niemand außer Ihnen die beiden PINs erfährt.

Ihr Webbrowser: Löchrig wie ein Sieb?

Surfen ohne jede Datenspur, das versprechen moderne Browser wie Mozilla Firefox mit der Funktion "Private Browsing". Das klingt verlockend, denn für Ihre Daten gibt es sehr viele Interessenten im Internet. Leider hat Ihr Browser daheim trotzdem Datenschutz-Löcher so groß wie Scheunentore, wenn Sie ihn nicht aktiv absichern.

Privater Modus reicht nicht

Warum regen sich eigentlich so viele Nutzer über Datenmissbrauch im Internet auf, denkt sich so mancher Web-Surfer. Wenn man im Browser die Funktion "Private Browsing" aktiviert, werden doch alle Spuren der Internetbesuche gelöscht. Man muss beim Firefox-Browser nur unter dem Menüpunkt "Extras" den sogenannten Privaten Modus wählen, und schon ist die Privatsphäre geschützt. Das stimmt aber leider nicht!

Gelöscht werden nur lokale Spuren

Wenn Sie diesen Privaten Modus bei Ihrem Browser einmal aktivieren, sollten Sie auf den Warnhinweis im Browserfenster achten. Dort steht insbesondere, dass nur lokale Datenspuren, also die Nutzungsspuren auf Ihrem Rechner, automatisch gelöscht werden, nicht aber die Spuren, die Sie im Internet selbst hinterlassen. Aber das ist noch nicht alles.

Aber auch nicht alle lokalen Spuren werden gelöscht

Der Private Modus beseitigt erfreulich viele Datenspuren, die ansonsten Ihre Surfgewohnheiten verraten könnten. Werden der Browserverlauf, die Text-Cookies und die zwischengespeicherten Dateien nicht gelöscht, könnten andere Personen an Ihrem Rechner sehr viel über Ihr Online-Verhalten erfahren. Dafür müssen diese Personen noch nicht einmal direkt an Ihren PC kommen: Hackern gelingt es sogar aus dem Internet, diese lokalen Datenspuren auszulesen.

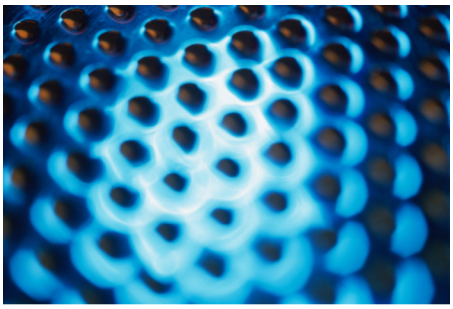
Private Browsing dünnt die lokalen Datenspuren massiv aus, es werden aber nicht alle gelöscht!

Flash weiß mehr über Sie

Zu den besonders hartnäckigen Datenspuren und Verrätern Ihrer Surfgewohnheiten gehören die sogenannten Flash-Cookies. Sie werden meist auf Ihrem Rechner abgelegt, wenn Sie eine Webseite mit Flash-Animationen öffnen. Flash-Animationen sind zum Beispiel Online-Werbeanzeigen, die wie ein Film ablaufen. Tatsächlich sind die meisten Online-Anzeigen inzwischen Flash-Animationen. Die damit verbundenen Flash-Cookies sind also sehr verbreitet.

Flash-Cookies können riesig werden

Im Gegensatz zu den herkömmlichen, gut bekannten Cookies haben die Flash-Cookies etwa zwanzig Mal so viel Speicherplatz und könnten so einiges über Ihr Online-Verhalten dokumentieren. Aber Sie sind den Flash-Cookies nicht völlig ausgeliefert.



Die Lücken in Ihrem Browser sind höchstwahrscheinlich größer, als Sie denken!

Neuer Flash-Player verschafft Abhilfe

Während bisher der Private Modus keine Löschung der Flash-Cookies vorsah, kann diese Funktion Ihres Browser nun auch Flash-Cookies zu Leibe rücken, allerdings nur, wenn Sie einen neuen Adobe Flash Player ab Version 10.1 nutzen. Wie aktuelle Untersuchungen zeigen, nutzt aber mindestens ein Viertel aller Internetsurfer noch einen alten Flash-Player, der sich nicht an den Privaten Modus Ihres Browsers hält.

Welche Version nutzen Sie?

Prüfen Sie deshalb, ob Sie bei Ihrem Browser daheim bereits den neuesten, kostenlosen Adobe Flash Player nutzen. Das können Sie feststellen, indem Sie den Mauszeiger über eine animierte Online-Werbung auf einer Webseite Ihrer Wahl positionieren und einen Rechtsklick mit der Maus machen.

In dem sich öffnenden Menü finden Sie "Über Adobe Flash Player". Wenn Sie dies auswählen, zeigt Ihnen der Flash-Player seine Version an, die mindestens 10.1 sein muss.

Aber Ihr Browser hinterlässt weitere Fingerabdrücke

Selbst wenn Sie an Ihrem Heim-PC endlich die Flash-Cookies losgeworden sind, haben Sie noch nicht alle Spuren Ihrer Internetnutzung verwischt. Ihr Browser und damit Sie selbst können immer noch sehr gut im Internet identifiziert werden. Wie eine Untersuchung der Bürgerrechtsorganisation EFF (Electronic Frontier Foundation) gezeigt hat, hinterlassen 84 Prozent aller Browser trotz Private Browsing und neuem Flash-Player immer noch individuelle "Fingerabdrücke" im Internet.

Eine nahezu einmalige Kombination unter anderem aus Browserversion, installierten Zusatzprogrammen, deren Versionen und den vom Nutzer gewählten Browsereinstellungen bildet ein verräterisches Identifikationsmuster, das jeder Browser ungefragt ins Internet überträgt.

Stopfen Sie die Datenschutz-Löcher

Um auch diesen Browser-Fingerabdruck als mögliches Datenschutz-Loch zu beseitigen, sollten Sie in Ihren Browsereinstellungen insbesondere JavaScript deaktivieren. Beim Firefox-Browser klappt dies mit dem Menüpunkt Extras > Einstellungen > Inhalt > JavaScript. Leider werden dadurch verschiedene nützliche Funktionen von Webseiten eingeschränkt. Sie müssen also abwägen, ob Sie lieber Komfort oder ein möglichst spurloses Surfen im Internet wollen.

Wenn Sie Fragen dazu haben oder wissen wollen, wie der Browser an Ihrem Arbeitsplatz eingestellt werden soll, fragen Sie Ihren Datenschutzbeauftragten und Ihre Systemadministration.

Impressum

Redaktion:
Udo Wenzel
Datenschutzbeauftragter

Anschrift:
agentia wirtschaftsdienst
Dipl.-Inform. Udo Wenzel
10787 Berlin
Telefon: 030 / 2196 4390
E-Mail: udo.wenzel@agentia.de

So wird ein Fahrzeug geortet - aber der Fahrer nicht ausspioniert!

Zu Ihnen kommt ein Kundendienstfahrzeug, weil etwas im Haus repariert werden muss? Danach gibt es Ärger, weil Sie meinen, so viele Stunden, wie auf der Rechnung stehen, hätte das Ganze sicher nicht gedauert? Und die berechnete Anfahrstrecke sei viel zu lang? Beides lässt sich nachprüfen, wenn das Unternehmen ein modernes Ortungssystem für seine Kundendienstfahrzeuge einsetzt. Das wiederum ist möglich, ohne gegen den Datenschutz zu verstoßen.

GPS macht es möglich: Wo sich ein Fahrzeug befindet, lässt sich stets sofort feststellen, wenn es über Mobilfunk an ein entsprechendes System angebunden ist. Das hat viele Vorteile. Allerdings können solche Systeme auch zum gläsernen Mitarbeiter führen. Dazu kommt es nicht, wenn bestimmte Grenzen beachtet werden.

GPS-Systeme halten alle wichtigen Daten fest

Wenn ein Unternehmen Kundendienste zu noch bezahlbaren Stundensätzen anbieten will, muss jeder Leerlauf vermieden werden. Dabei helfen GPS-Ortungssysteme. Sie halten vor allem folgende Daten fest:

1. Standort des Fahrzeugs zu jedem Zeitpunkt während seines Einsatzes

2. Fahrtunterbrechungen (Ort und Zeit)

3. zurückgelegte Fahrtstrecken zwischen den Fahrtunterbrechungen

Die Daten dienen zur Routenoptimierung

Diese Daten lassen sich vor allem zur optimalen Routenplanung nutzen:

- Entsprechende Programme rechnen aus, in welcher Reihenfolge der Fahrer die Kunden anfahren muss, damit die Zahl der zurückgelegten Gesamtkilometer möglichst niedrig ist.

- Geht ein dringender Auftrag ein, lässt sich feststellen, welches gerade verfügbare Kundendienstfahrzeug am nächsten beim Kunden ist.

Auch die Abrechnung wird erleichtert

Außerdem kann das Unternehmen die Daten verwenden, um mit dem Kunden abzurechnen:

- Der Kunde muss die Zeit zahlen, die als Fahrtunterbrechung an seiner Adresse ausgewiesen ist.

- Ihm werden die Kilometer in Rechnung gestellt, die das Fahrzeug seit dem letzten Zwischenstopp beim vorhergehenden Kunden zurückgelegt hat.

Beide Werte lassen sich elektronisch in das Abrechnungssystem übernehmen. Das spart Zeit und vermeidet Fehler.

Der Datenschutz muss beachtet werden!

Freilich haben solche Systeme auch eine andere Seite, die durchaus Bedenken bei Datenschützern auslösen. Zwar geht es nur darum, Daten des Fahrzeugs zu erfassen. Aber in jedem Fahrzeug sitzt ein Fahrer. Und deshalb sind alle Daten des Fahrzeugs immer auch Daten des Fahrers. Damit ist der Datenschutz gefordert, wenn aus dem Mitarbeiter nicht ein gläserner Fahrer werden soll.

Die Datenschutzbehörden machen eine Reihe von Vorgaben

Aus diesem Grund haben die Datenschutzbehörden bestimmte Vorgaben festgelegt, die beim Einsatz von Ortungssystemen zu beachten sind. Dabei sind vor allem folgende Punkte wichtig:

1. Die betroffenen Mitarbeiter werden informiert, welche Daten über sie gespeichert werden.

2. Wenn das Fahrzeug auch privat genutzt werden darf, findet während der Zeit privater Nutzung keine Speicherung von Daten statt.

3. Es gibt ein schriftliches Konzept dafür, welche Daten für welche Zwecke genutzt werden.

4. Es gibt ein Konzept dafür, wann die gespeicherten Daten gelöscht werden.

Der Teufel steckt dabei im Detail!

Wenn diese Punkte umgesetzt werden, sind oft viele Details zu beachten. Das zeigt sich vor allem bei dem Punkt "Löschung der Daten". Auf den ersten Blick könnte man meinen, dass alle Daten, die zur Abrechnung mit dem Kunden gebraucht werden, sofort gelöscht werden können, wenn die Abrechnungen geschrieben sind.

Fahrzeugortung per GPS ist heute gang und gäbe

Zu früh gelöscht - Reklamation nicht mehr zu überprüfen!

Das gäbe allerdings Probleme, wenn ein Kunde reklamiert, weil er zum Beispiel meint, ihm seien zu viele Kilometer in Rechnung gestellt worden. Die Daten müssen deshalb so lange gespeichert werden, wie noch mit Reklamationen zu rechnen ist. Dabei kommt man in der Praxis nicht darum herum, gewisse Erfahrungswerte zugrunde zu legen. Das können dann durchaus mehrere Monate sein.

Ihr Datenschutzbeauftragter kümmert sich

Wer stellt sicher, dass die Vorgaben des Datenschutzes wirklich eingehalten werden? Dazu dienen gesetzliche Regelungen. Sie schreiben vor, dass Ortungssysteme vom Datenschutzbeauftragten des Unternehmens überprüft werden müssen, bevor sie erstmals zum Einsatz kommen.

Eine solche Überprüfung macht relativ viel Aufwand. Er lohnt sich aber. Denn so können alle Beteiligten sicher sein, dass es nicht irgendwann Ärger mit der Datenschutzaufsicht gibt. Das nützt dem Unternehmen, den Fahrern und letztlich auch den Kunden.

Schadsoftware: Wer suchet, der findet

Gerade vor Weihnachten werden Millionen von Internetnutzern passende Geschenke im Internet suchen. Besonders hilfreich sind dabei die Internetsuchmaschinen, die schnell zu jedem Suchbegriff eine Vielzahl von Ergebnissen liefern. Doch unter den Treffern sind immer häufiger Links zu Webseiten enthalten, die mit datenhungrigen Schadprogrammen verseucht sind.

Beliebte Begriffe, beliebte Angriffsziele

In der Adventszeit kreist vieles um Winterurlaub und Geschenke. Das sieht man in der Fernsehwerbung genauso wie im Internet. Auch die Suchbegriffe, die in die Internetsuchmaschinen wie Google, Yahoo und Bing eingegeben werden, drehen sich verstärkt um diese Themen. Das wissen Datendiebe und Hacker und nutzen diese Suchvorlieben im Internet ganz gezielt aus.

Jeder will nach oben auf der Trefferliste

Bekanntlich haben diejenigen Suchergebnisse die größte Chance, angeklickt zu werden, die auf der Trefferliste der führenden Suchmaschinen weit oben stehen. Deshalb unterziehen Online-Händler ihre Webseiten einer sogenannten Suchmaschinenoptimierung (Search Engine Optimization, SEO). Mit raffinierten Techniken werden die Webseiten so gestaltet, dass Suchmaschinen sie als möglichst relevant einstufen und bei den wichtigen Suchbegriffen nach oben in der Trefferliste positionieren.

Auch Datendiebe nutzen SEO-Techniken

Genau wie seriöse Online-Händler nutzen inzwischen auch Datendiebe solche Optimierungstechniken, um die von ihnen mit Schadprogrammen präparierten Webseiten weit nach oben in die Trefferlisten zu katapultieren. Die Folgen für Sie als Internetnutzer können fatal sein.

Bis zu 50 Prozent verseuchte Treffer

Je nach Suchbegriff und Saison können die Trefferlisten in den Suchmaschinen mit bis zu 50 Prozent gefährlich manipulierter Links durchsetzt sein, so das Ergebnis einer Untersuchung des Sicherheitsanbieters Zscaler. Im Durchschnitt sind 15 bis 20 Prozent der ersten 100 Treffer verseucht.

Auch Sponsored Links sind betroffen

Wenn Sie nun glauben, dass es sicher ist, die bezahlten Links, auch Sponsored Links genannt, zu nutzen, irren Sie leider. Das Geschäft mit den gestohlenen Daten ist so lukrativ, dass die Internetkriminellen sogar kostenpflichtige Schein-Anzeigen schalten, um möglichst viele Opfer zu finden.

Renommierte Webseiten werden gekapert

Eine andere Angriffsvariante ist es, seriöse Webseiten, die bei Suchmaschinen gut platziert sind, zu kapern und sie mit Schadsoftware auszustatten. Die Besucher renommierter Webseiten vertrauen dem Webseitenanbieter und ahnen nicht, dass die Webangebote trotz des guten Rufs gefährlich sein können, wenn Hacker den Webserver des Anbieters knacken konnten.

So finden Sie keine Schadprogramme, sondern Ihre Geschenke

Sicherlich möchten Sie nicht darauf verzichten, weiterhin im Internet zu recherchieren und Ihre Weihnachtsgeschenke zu suchen. Deshalb sollten Sie auch Trefferlisten von Suchmaschinen kritisch sehen und nicht einfach jeden Link anklicken. Nutzen Sie vielmehr Anti-Viren-Programme, die auch Trefferlisten von Suchmaschinen untersuchen, und zwar bevor Sie den Link angeklickt haben. Solche Schutzsoftware bekommen Sie bei den großen Anti-Malware-Anbietern meist kostenlos als Erweiterung für Ihren Webbrowser.

Sind Sie gerüstet gegen Suchmaschinen-Angriffe?

Frage: Sind Sie geschützt gegen die hinterlistigen Suchmaschinen-Attacken, wenn Sie eine der führenden Suchmaschinen nutzen und kleinere Suchanbieter meiden?

a) Ja, denn die großen Suchanbieter prüfen die Links, bevor diese auf die Trefferliste kommen.
b) Nein, das Risiko solcher Angriffe besteht bei jeder Suchmaschine. Die bekannten Suchmaschinen werden sogar von den Datendieben für ihre Angriffe bevorzugt.

Lösung: Antwort b) ist richtig, denn die Datendiebe wollen möglichst viele Opfer und optimieren deshalb für ein hohes Ranking bei den großen Suchmaschinen. Und selbst die großen Suchmaschinen können nicht alle gefährlichen Links rechtzeitig erkennen.

Frage: Sind Sie geschützt gegen die SEO-Angriffe, wenn Sie ein Anti-Viren-Programm installiert haben?

a) Nein, nicht jedes Anti-Viren-Programm bietet einen Online- und Echtzeit-Schutz und prüft jeden Link schon vor dem Öffnen. Dafür gibt es aber Spezialprogramme.
b) Ja natürlich, denn eine Sicherheitssoftware reicht für die Abwehr jedes Angriffs aus dem Internet.

Lösung: Antwort a) stimmt. Sehen Sie sich deshalb den Leistungsumfang Ihrer Anti-Malware-Software an. Im Zweifel können Ihnen die Systemadministration und Ihr Datenschutzbeauftragter helfen.

Frage: Wenn Ihre Sicherheitssoftware anzeigt, dass ein Link in der Trefferliste sicher ist, können Sie dann von der betreffenden Webseite alle Dateien sorglos herunterladen?

a) Natürlich, denn die Webseite ist ja sicher.
b) Nein, zur Sicherheit werde ich jeden Download von der Webseite nochmals mit meinem Anti-Viren-Scanner prüfen.

Lösung: Antwort b) ist richtig. Die Link-Prüfung basiert teils auf einer sogenannten Schwarzen Liste der bekannten Risiko-Webseiten. Ganz neue Webseiten, deren Verseuchung noch unbekannt ist, werden nicht von jedem Link-Scanner erkannt. Downloads sollten also nochmals geprüft werden.