

# Newsletter Datenschutz

## Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

der Datenschutz spielt in allen Bereichen unseres Lebens eine wichtige Rolle: Ob beim scheinbar einsamen Spaziergang durch den Wald, bei zwischenmenschlichen Beziehungen, beim Online-Shopping oder beim Umgang mit PDF-Dokumenten. Immer stellt sich die Frage, ob die Privatsphäre gewahrt bleibt, oder ob unsere persönlichen Daten ohne unser Einverständnis genutzt werden.

Die aktuelle Ausgabe zeigt Ihnen nicht nur diese Bandbreite des Datenschutzes im Privatleben und im Beruf, sondern bietet auch zahlreiche Tipps, was Sie selbst tun können, um Ihre Daten besser zu schützen. Manchmal reichen dazu schon einfache Softwareeinstellungen, ein anderes Mal muss der Weg zum Gericht beschriftet werden. In jedem Fall aber lohnt es sich, die eigene Privatsphäre zu verteidigen.

Wir wünschen Ihnen wieder viele hilfreiche Einsichten!

Ihre Datenschutzbeauftragten der agentia wirtschaftsdienst

## Kameras mitten im Wald - darf das sein?

**Sie wollen sich entspannen und gehen im Wald spazieren. An einem Baum hängt ein merkwürdiger kleiner Kasten. Sie gehen näher heran und können es kaum glauben: Es handelt sich eindeutig um eine Kamera! So hatten Sie sich die Waldeinsamkeit nicht vorgestellt. Sind solche Kameras in freier Landschaft erlaubt?**

### 30.000 Kameras allein in Rheinland-Pfalz

Das überraschte selbst den Landesbeauftragten für den Datenschutz Rheinland-Pfalz: Nach seinen Recherchen sind allein in diesem Bundesland etwa 30.000 "Wildkameras" in Wald und Flur installiert. Einfache Modelle kosten kaum 100 Euro. Das verlockt offensichtlich vor allem Jäger dazu, auch mehrere solcher Kameras in ihrem Revier zu installieren.

### Böse Absichten? Durchweg nicht!

Dunkle Zwecke verfolgen sie dabei in aller Regel nicht. Oft sind die Kameras auf den Eingang von Wildhöhlen gerichtet ("Dachsbau-Kameras"). Manchmal halten sie das Geschehen in Nestern fest (so etwa die beliebte Wanderfalken-Live-Cam auf der Nürnberger Burg, die im Internet leicht zu finden ist). Bisweilen sollen sie klären helfen, welche Tiere einen Wildwechsel benutzen.

### Liebespaare ungewollt im Visier

Freilich gab es auch schon Fälle, in denen Liebespaare auf der Suche nach einem ruhi-

gen Platz in das Visier solcher Kameras gerieten. Zumindest einer dieser Fälle war - ohne Namen und ohne Bilder - sogar Gegenstand der Berichterstattung in den Medien.

### Feld und Wald als "öffentlich zugängliche Räume"

- Dort, wo aller Erfahrung nach mit Wandern und Spaziergängern zu rechnen ist, also etwa an Wald- und Wanderwegen, sind solche Kameras unzulässig.  
- Erlaubt sind sie in Bereichen, die - etwa wegen des dichten Bewuchses - von Wan-

derern und Spaziergängern im Regelfall nicht betreten werden. Zusätzliche Voraussetzung ist allerdings selbst dann, dass es ein "plausibles Interesse" für eine Wildbeobachtung gibt. Typisches Beispiel ist die Beobachtung des Geschehens an einem Dachsbau.  
- Aufnahmen, bei denen Menschen ungewollt in das Blickfeld der Kamera geraten sind, sind zu löschen.  
- Manche Aufsichtsbehörden erlauben Kameras auch zu dem Zweck, Diebstahlfahrten abzuwehren, etwa bei Holzstapeln.

### Bilder im Internet könnten strafbar sein

Dass Betreiber solcher Kameras Aufnahmen von Menschen weitergeben oder gar ins Internet stellen, scheint bisher noch nicht vorgekommen und ist auch wenig wahrscheinlich. Darin läge nämlich eine Straftat (Verletzung des Rechts am eigenen Bild), die mit Freiheitsstrafe bis zu einem Jahr bestraft werden kann.

### Im Ernstfall: Gespräch oder notfalls Beschwerde

Falls Sie sich tatsächlich einmal durch eine Wildkamera unzulässig beeinträchtigt fühlen sollten, wäre ein Gespräch mit dem Betreiber der Kamera sinnvoll. Falls Sie ihn nicht ermitteln können, empfiehlt es sich, die Kamera zu fotografieren, ihren Standort so genau wie möglich festzuhalten und sich an die Datenschutzaufsichtsbehörde Ihres Landes zu wenden.



*Wildkameras gibt es mittlerweile schon beim Discounter (Bild: PlazacCameraman/iStock/Thinkstock)*

## Wenn Cookies gestohlen werden, ist die Identität in Gefahr

**Datendiebe versuchen, Cookies von den Rechnern ihrer Opfer auszulesen. Dahinter steckt mehr als ein Ausspionieren der Nutzervorlieben: Cookie-Diebstahl kann Identitätsdiebstahl bedeuten. Es ist daher höchste Zeit, die Sicherheit der Cookies zu erhöhen.**

### Cookies sind ein Klassiker im Datenschutz

Die Zeiten, in denen Sie bei dem Wort "Cookies" nur an Schokokekse gedacht haben, sind sicher längst vorbei. Zweifellos haben Sie schon davon gehört, dass Cookies in Verbindung mit Webbrowsern verwendet werden. Bei der Internetnutzung speichern viele Betreiber von Webseiten Cookies als kleine Textdateien auf den Rechnern der Besucher. Die Online-Werbung zum Beispiel wertet solche Cookies aus, um daraus die besuchten Webseiten und damit die Interessengebiete des Nutzers abzulesen.

Diese möglichen Nutzerprofile sind der Grund dafür, dass Datenschützer empfehlen, Cookies am Ende der Internetsitzung automatisch zu löschen, da sich so langfristige Nutzerprofile auf Cookie-Basis verhindern lassen. Möglich wird das automatische Löschen durch entsprechende Einstellungen im Cookie-Manager Ihres Browsers.

### Cookies helfen nicht nur beim Tracking

Vielleicht haben Sie sich einmal gefragt, warum man nicht einfach komplett auf Cookies verzichtet und sie einfach blockiert.

Der Grund ist die Vielseitigkeit von Cookies: Nicht alle Cookies werden für das Nachverfolgen der Webseiten-Besuche genutzt. Viele Cookies helfen zum Beispiel dabei, beim Online-Shopping das Einsammeln von Artikeln im Online-Warenkorb technisch möglich zu machen. Sogar bei der Anmeldung in einem Online-Shop oder bei einer anderen zugangsgeschützten Website spielen Cookies eine wichtige Rolle - so wichtig, dass sie ein begehrtes Diebesgut sind.

### Datendiebe klauen Cookies

Internetkriminelle haben es ganz gezielt auf Cookies abgesehen. Dabei geht es meist nicht darum, über die Cookies den betroffenen Nutzer im Internet zu verfolgen. Stattdessen versuchen die Datendiebe, über die Cookies die Online-Identität des Nutzers zu stehlen.

Cookies haben nämlich eine entscheidende Bedeutung bei Anmeldungen für Online-Dienste.

Um zu vermeiden, dass Sie sich auf jeder einzelnen Seite einer zugangsgeschützten Website anmelden müssen, wird die einmal erfolgte Anmeldung in Form eines Cookies bis zur Abmeldung gespeichert. Wenn Sie die Webseite nach der Anmeldung wechseln, prüft die Folgeseite jeweils anhand des Cookies, ob Sie bereits angemeldet sind.

### Mit dem Cookie an die Daten

Gelingt es einem Datendieb, ein entsprechendes Cookie zu stehlen, kann er damit vortäuschen, dass sich der berechtigte Nutzer angemeldet hat. Der Angreifer übernimmt mit dem Cookie die Anmeldung und damit die digitale Identität des Betroffenen.

Leider wird diese Gefahr häufig übersehen, sodass Cookies und die Übertragung der Cookie-Dateninhalte nur unzureichend geschützt werden.

### Cookie-Diebstahl mittels "Lauschangriff"

Vielleicht fragen Sie sich jetzt, wie Angreifer denn Cookies überhaupt von Ihrem PC, Tablet oder Smartphone stehlen können.

Der Datendieb muss dazu weder Zugang zu Ihren Geräten haben noch einen klassischen Hackerangriff auf Ihren Rechner starten. Es reicht leider meist aus, die Datenübertragung ins Internet zu belauschen: Cookies werden oftmals noch ohne Verschlüsselung übertragen, die Cookie-Inhalte lassen sich leicht auspähen.

### Wann Cookie-Diebstahl droht

Übertragen werden die Cookie-Inhalte immer dann, wenn Sie die nächste Webseite innerhalb eines Online-Shops oder innerhalb eines anderen Dienstes ansteuern, nachdem Sie sich einmal angemeldet haben. Die Übertragung der Cookie-Daten geschieht also sehr oft und zudem auf riskantem Weg ohne Verschlüsselung.

### Beispiel: ungeschütztes WLAN

Ein Beispiel: Stellen Sie sich vor, Sie sitzen in einer Hotellobby und nutzen dort den kostenlosen WLAN-Hotspot, um bei einem Online-Händler das Buch zu erwerben, das der Referent zuvor in der Tagung empfohlen hat. Ohne Verschlüsselung der Verbindung werden die Cookie-Daten zu Ihrer Anmeldung ungeschützt im WLAN-Netz übertragen. Ein Angreifer könnte die Cookie-Inhalte und damit Ihre Anmeldung beim Online-Shop übernehmen und in Ihrem Namen bestellen.

### Das hilft gegen den Cookie-Diebstahl

Denken Sie deshalb daran:

- Personenbezogene und andere vertrauliche Daten sollten Sie nie im Internet übermitteln, wenn keine SSL-Verschlüsselung vorliegt.

- Achten Sie darauf, dass die SSL-Verschlüsselung auch nach der Anmeldung besteht, sonst könnten Angreifer die Cookie-Daten zur Anmeldung abfangen und Ihre Identität stehlen.

- Nach Abschluss Ihrer Online-Sitzung sollten Sie sich immer abmelden und den Browser schließen, damit der entsprechend eingestellte Cookie-Manager die Cookies auch tatsächlich löscht und sich Ihre Anmeldung nicht missbrauchen lässt.

### Impressum

agentia wirtschaftsdienst  
dipl.-inform. udo wenzel  
budapester straße 31  
10787 berlin

tel.: 030 2196 4390  
fax: 030 2196 4393

udo.wenzel@agentia.de  
thorsten.ritter@agentia.de

## Was PDF-Dateien alles verraten können

PDF-Dokumente sehen aus wie gedruckt, haben es aber in sich. So können PDF-Dateien eine eigene Verbindung ins Internet aufbauen und lassen sich sogar für das Tracking von Nutzeraktivitäten einsetzen. Seien Sie deshalb auch bei PDF-Dokumenten vorsichtig!

### Von wegen digitales Papier!

Es ist immer ärgerlich, wenn man ein Dokument am Computer erstellt, es ausdruckt und das Resultat dann in gedruckter Form anders aussieht als am Bildschirm. Besonders unschön ist dieses Phänomen, wenn man ein digitales Dokument verschickt, im guten Glauben, dass der Kunde beim Ausdruck auch das Angebot so sieht, wie man sich dies eigentlich dachte.

Zum Glück aber gibt es ja PDF-Dateien, die den großen Vorteil haben, dass sie auf nahezu allen Geräten in gleicher Form angezeigt und ausgedruckt werden.

Dieser große Vorteil von PDF-Dokumenten führt einerseits dazu, dass sie sehr weit verbreitet sind. Andererseits verleitet er aber auch dazu, dass man PDF-Dateien als Bilder oder digitales Papier ansieht. In Wirklichkeit aber sind PDF-Dateien mit zahlreichen Funktionen ausgestattet. Der sogenannte PDF-Reader ist deshalb auch kein Bildbetrachter, sondern vielmehr eine Software, die sich mit der Funktionsvielfalt eines Webbrowsers vergleichen lässt.

### Von Schadprogrammen ...

Wegen ihrer Beliebtheit und der großen Verbreitung sind PDF-Reader und -Dateien auch beliebte Angriffsziele und -Werkzeuge. So können PDF-Dateien, die einer E-Mail beiliegen oder als Download im Internet angeboten werden, durchaus Schadfunktionen in sich tragen. PDF-Dateien sollten mit Antivirensoftware geprüft, die PDF-Reader regelmäßig aktualisiert werden.

### ... und versteckten Kommentaren

Aber es kann noch mehr in einer PDF-Datei stecken als ein Trojaner: Werden zum Beispiel Word-Dateien in PDF-Dokumente umgewandelt, können gegebenenfalls vorhandene Kommentare und Vermerke aus der Word- in die PDF-Datei übertragen werden, ohne dass Sie dies gleich erkennen. Mitunter erhält dann der Empfänger der Datei weitaus mehr Informationen, als er sollte.

### Vom PDF gleich ins Internet

PDF-Dateien können auch Hyperlinks in sich tragen. Ein Klick auf einen Link führt bei bestehender Online-Verbindung und fehlender Sicherheitseinstellung gleich ins Internet. So könnte ein Klick auf einen Link innerhalb eines PDF-Dokuments auch zum Download von Schadsoftware führen.

Die Internet-Funktion der PDF-Dateien lässt sich aber auch für das Nachverfolgen der Nutzeraktivitäten, also für das Tracking, nutzen. Verwendet der Nutzer keine Sicherheitsoptionen, könnte ein PDF-Dokument über die Internetverbindung mitteilen, dass der Nutzer einer bestimmten IP-Adresse nun dieses PDF-Dokument geöffnet und den darin enthalte-

nen Link angeklickt hat. PDF-Dateien können also auch Informationen für ein Nutzerprofil liefern, nicht nur Webbrowser. Diesem möglichen PDF-Tracking sollten Sie einen Riegel vorschieben.

### Das können Sie gegen PDF-Tracking tun

1. Wählen Sie im PDF-Reader unter "Bearbeiten" den Bereich "Voreinstellungen".
2. Prüfen Sie unter "Berechtigungen" den Bereich "Internetzugriff über PDF-Dateien außerhalb des Webbrowsers", ob Zugriff nicht etwa für alle Webseiten zugelassen wurde.
3. Geben Sie entweder nur vertrauenswürdige Webseiten für Internetverbindungen frei oder wählen Sie besser die Option "Blockieren".
4. Wenn Sie einen Hyperlink innerhalb eines PDF-Dokuments auswählen, aktivieren Sie nicht die Option "Gewählte Aktion für diese Webseite für alle PDF-Dokumente speichern".
5. Deaktivieren Sie unter "JavaScript" die Option "Adobe JavaScript".

## Wissen Sie, wie Sie Tracking bei PDF-Dateien verhindern? Testen Sie Ihr Wissen!

**Frage:** Das Nachverfolgen von Nutzeraktivitäten mit präparierten PDF-Dateien ist nur möglich, wenn das PDF-Dokument im Webbrowser geöffnet wird. Stimmt das?

- a) Ja, denn Tracking findet immer über den Browser statt.
- b) Nein, es reichen eine bestehende Internetverbindung und das Öffnen der PDF-Datei mit einem PDF-Reader.

Lösung: Die Antwort b) ist richtig. Der PDF-Reader kann selbst die Internetverbindung nutzen. Über versteckte Skripte in PDF-Dateien kann ein Tracking des Nutzers stattfinden, ganz ohne Start des Browsers.

**Frage:** Sie prüfen eine PDF-Datei mit Ihrem Virens scanner. Besteht keine Gefahr für PDF-Tracking, wenn der Virens scanner nicht anschlägt?

- a) Wenn der Virens scanner nichts findet, ist die PDF-Datei ungefährlich.
- b) Bei einer Suche nach Schadsoftware wird nicht automatisch auch nach Tracking-Skripten gesucht. Auch ohne Trojaner kann eine PDF-Datei also ein heimlicher Datensammler sein.

Lösung: Die Antwort b) ist richtig. Der Virens scanner ist sehr wichtig, hilft aber nicht gegen alle Datenrisiken. Deaktivieren Sie in Ihrem PDF-Reader deshalb unter "Bearbeiten" im Bereich "Voreinstellungen" und dort unter "JavaScript" die Option "Adobe JavaScript", denn JavaScript könnte für ein heimliches PDF-Tracking missbraucht werden. Prüfen Sie in Ihrem PDF-Reader im Programmmenü unter "Bearbeiten" im Bereich "Voreinstellungen" und dort unter "Berechtigungen" den Bereich "Internetzugriff über PDF-Dateien außerhalb des Webbrowsers", ob der Zugriff nicht etwa für alle Webseiten zugelassen wurde. Sonst erhalten Sie keine Warnung mehr, wenn eine PDF-Datei auf das Internet zugreifen will.