agentia wirtschaftsdienst

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

es muss kein Privatdetektiv auf Sie angesetzt sein, damit Ihre Privatsphäre bedroht ist. Im Alltag gibt es viele Situationen, in denen Sie mehr Daten von sich preisgeben als erforderlich. In dieser Ausgabe finden Sie deshalb Ihr persönliches Trainingsprogramm, wie Sie die unnötige Weitergabe Ihrer Daten vermeiden können. Aber auch die Überwachung durch Detektive ist wieder ein Thema.

Zusätzlich erfahren Sie, wie Sie mögliche Sicherheitsvorfälle und Datenpannen am Computer besser erkennen können und das richtige Gespür dafür entwickeln. Den Abschluss dieser Ausgabe bilden die zunehmend beliebten Smart-TVs und Smartwatches. Sie sind nicht nur besonders komfortabel, sondern bedrohen unter Umständen auch Ihre persönlichen Daten.

Wir wünsche Ihnen spannende Erkenntnisse...

Ihre Datenschutzbeauftragten der agentia wirtschaftsdienst

Ihr privates Programm zur Datenvermeidung

Datenschutz einfach mal selbst gemacht! Was können Sie tun, damit Ihre persönlichen Daten nicht überall herumschwirren? Mehr, als Sie denken!

Sie selbst als Datenquelle

Die meisten Daten über Sie stammen weder von Unternehmen noch von Behörden, sondern von Ihnen selbst. Das glauben Sie nicht? Dann prüfen Sie einmal kritisch, ob Sie sich in den nachfolgenden Beispielen aus dem Alltag nicht doch wiederfinden!

Der Klassiker: Preisausschreiben

Oft gibt es ein rotes Auto zu gewinnen, weil die Aussicht auf ein Fahrzeug dieser Farbe nach psychologischen Erkenntnissen die höchste Aufmerksamkeit beim Betrachter auslöst. Und schon ist die Teilnahmekarte ausgefüllt, vor allem wenn sie ausdrücklich auch ohne Briefmarke losgeschickt werden darf.

Alles völlig harmlos, schließlich haben Sie außer Vorname, Name und Anschrift nichts angegeben? An sich schon. Aber: Aus Ihrem Vornamen lässt sich Ihr Geburtsjahr oft recht genau erschließen, denn es gibt umfangreiche Statistiken dazu, in welchen Jahren welche Namen beliebt waren. Und Ihr Geschlecht liefert Ihr Vorname ohnehin mit. Gewiss alles kein Drama, aber in der Summe ein ganz guter Ansatz für zielgenaue Werbung.

Richtig in: Online-Accounts

Einkäufe im Internet von A wie Autobatterie bis Z wie Zahncreme sind so beliebt wie noch nie. Und natürlich kaufen Sie immer da, wo das Gewünschte gerade am billigsten ist. Schließlich wollen Sie ja sparen. Viele Anbieter verlangen, dass Sie beim Kauf einen Account einrichten. Ohne persönliche Daten geht das natürlich nicht. Und da ein und derselbe Anbieter selten zweimal hintereinander der billigste ist, kaufen Sie ständig woanders. Wenn Sie dann jedes Mal einen neuen Account einrichten, kommen sehr schnell ein paar Dutzend zusammen.

Es muss nicht immer der Kauf per Kreditkarte sein. Ein Kauf auf Rechnung gibt wesentlich weniger persönliche Daten preis (Bild: Thinkstock/LDProd)

Selbstverständlich müssen Sie dabei jedes Mal ein Passwort vergeben. Und natürlich ist es jedes Mal dasselbe, sonst könnten Sie sich die vielen Passwörter gar nicht alle merken! Und natürlich ist genau das auch jedem Hacker klar. Hat er einmal Ihr Standardpasswort in die Finger bekommen, stehen ihm alle Accounts offen, die er von Ihnen findet. Die Alternative? Mehr und mehr Online-Händler bieten eine Bestellung als Gast an, sodass Sie wegen eines einmaligen Einkaufs nicht gleich einen Account einrichten müssen.

Bezahlen? Natürlich, aber ...

Achten Sie stets darauf, wie der Bezahlvorgang abläuft. Häufig ist ein Dienstleister zwischengeschaltet. Das ist im Prinzip kein Problem, denn die meisten Dienstleister sind seriöse Profis. Dennoch: Wenn Sie zum Bezahlen auf eine andere Seite geleitet werden, und Sie haben mit dem Dienstleister, dessen Seite dann auftaucht, keinerlei Erfahrung - geben Sie einfach bei Google die Frage ein: Wer hat Erfahrungen mit X? Dann wissen Sie meist sofort, ob der Dienstleister vertrauenswürdig ist. Alternativ wäre ein Kauf per Rechnung zu überlegen. Gar nicht so wenige Online-Händler bieten auch dieser Variante an.

Alles einfacher als gedacht?

Wenn Sie diese Beispiele etwas weiterdenken, fällt Ihnen sicher noch so manches ein, was Sie zur Datenvermeidung tun können.

Überwachung der Ex - mit GPS nein, mit Detektiv schon?

Die Sache ist ein Dauerbrenner: Darf ein Mann seine Ex-Ehefrau überwachen (oder überwachen lassen), weil er den Unterhalt kürzen will? Zwei neue Urteile des Bundesgerichtshofs schaffen Klarheit - mit teils überraschenden Folgen für die Beteiligten!

Ein Mann will nicht mehr zahlen

Vielleicht erinnern Sie sich noch an den Fall. Er wurde vor gut zwei Jahren schon einmal überall diskutiert, auch hier im Newsletter. Die wesentlichen Fakten in Kürze: Ein unterhaltspflichtiger Mann muss monatlich 680 Euro an seine frühere Frau zahlen. Falls er ihr nachweisen könnte, dass sie eine neue Lebensgemeinschaft eingegangen ist, könnte er den Unterhalt zumindest kürzen oder vielleicht sogar ganz streichen.

Er lässt seine Ex mit GPS überwachen

"Falls" - mit diesem kleinen Wort begannen für ihn die Probleme. Denn wie sollte er so etwas nachweisen? Ein Detektiv half ihm weiter. Er installierte am Auto der Frau ein GPS-Gerät. Das geschah natürlich, ohne dass sie etwas davon wusste.

Die Frau gibt vor Gericht klein bei

Das so erstellte Bewegungsprofil sprach für sich. Es zeigte sonnenklar, dass sich die Frau einem neuen Partner zugewandt hatte und mit ihm zusammenlebte. Deshalb wollte der unterhaltspflichtige Mann nun mit einer Abänderungsklage erreichen, dass seine Unterhaltspflicht künftig entfällt. Diese Klage hatte unerwartet raschen Erfolg. Als er seine Ex nämlich mit den Ergebnissen der GPS-Überwachung konfrontierte, erkannte sie sofort an, dass keine Unterhaltspflicht mehr besteht.

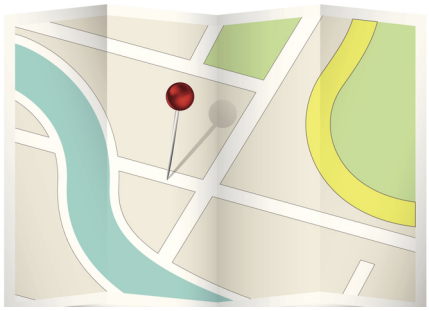
Jetzt geht es um den Ersatz der Kosten

Gestritten wird nun noch darüber, ob die frühere Ehefrau die Kosten für die GPS-Überwachung in Höhe von insgesamt 3.710,42 Euro tragen muss oder nicht. Ihr früherer Mann argumentiert, dass seine Klage nur dank dieser Überwachung Erfolg hatte. Sie hält dagegen, dass die Überwachung ihr Persönlichkeitsrecht unzulässig beeinträchtigt habe. Dieser Rechtsverstoß dürfe nicht auch noch damit belohnt werden, dass sie jetzt die Kosten der rechtswidrigen Überwachung zu tragen habe.

Diese Kosten muss die Frau nicht zahlen

Im Ergebnis gibt der Bundesgerichtshof der Frau Recht. Sie muss die Überwachungskosten nicht tragen. Dabei geht das Gericht von folgenden Kerngedanken aus:

Eine Überwachung mit GPS greift in das Recht auf informationelle Selbstbestimmung ein, das der Frau zusteht. Allerdings erfolgt die Observation nur im öffentlichen Raum (also außerhalb der Wohnung oder des privaten Grundstücks), sodass sie jedenfalls die Intimsphäre nicht berührt.



Die GPS-Überwachung war in diesem Fall rechtswidrig, da eine mildere Möglichkeit der Überwachung bestanden hätte (Bild: Thinkstock/veritycz)

Der Mann hat ein durchaus legitimes Interesse daran, an Beweise zu kommen, die er vor Gericht gegen seine frühere Frau verwenden kann. Dieses Interesse allein reicht aber nicht aus, um die Beeinträchtigung der Rechte der Frau zu rechtfertigen. Es müssen noch weitere Aspekte hinzukommen. Ein solcher Aspekt könnte hier darin liegen, dass der Ex-Frau möglicherweise ein versuchter Prozessbetrug vorzuwerfen ist. Denn immerhin wusste sie genau, dass sie sich in einer neuen Lebensgemeinschaft befindet und deshalb keinen Unterhaltsanspruch mehr hat.

Dennoch ist der Eingriff, der in einer Überwachung mittels GPS liegt, nach Auffassung des Gerichts im vorliegenden Fall nicht gerechtfertigt. Das liegt daran, dass der Unterhaltspflichtige ein gleich wirksames, aber milderes Mittel als die permanente GPS-Überwachung zur Verfügung hatte.

Er hätte nämlich einen Detektiv damit beauftragen können, die Ex-Ehefrau stichprobenweise persönlich zu beobachten, zum Beispiel - so das Gericht wörtlich - zu Abend- und Nachtzeiten sowie am Wochenende am Anwesen des vermutlichen Lebensgefährten. Da der Unterhaltspflichtige das nicht beachtet hat, kann er keine Kostenerstattung für die Überwachung verlangen.

Anders wäre es bei einer persönlichen Beobachtung gewesen

Dieses Ergebnis ist gewöhnungsbedürftig. Es bedeutet nämlich im Klartext Folgendes:

- Der Unterhaltspflichtige durfte durchaus einen Detektiv zur Überwachung seiner früheren Frau beauftragen.

- Ein solcher Detektiv hätte die Frau auch persönlich beobachten und überwachen dürfen, indem er sich etwa in der Nähe des Grundstücks ihres neuen Lebensgefährten versteckt und von dort aus beobachtet, wann sie eintrifft und wann sie wieder wegfährt.

- Über diese Umstände hätte der Detektiv dann als Zeuge vor Gericht aussagen können.

- Die Kosten für den Detektiv hätte die Ex-Ehefrau ersetzen müssen, und zwar auch dann, wenn sie möglicherweise sogar etwas höher liegen als die Überwachung per GPS.

Ob die persönliche Überwachung für die Frau angenehmer gewesen wäre?

Das hört sich alles sehr logisch an. Ob es die betroffene Frau allerdings wirklich als einen geringeren Eingriff empfunden hätte, wenn ein Detektiv in allen Einzelheiten berichtet hätte, wie sie ihren neuen Partner begrüßt und was sie mit ihm sonst so gemeinsam tut? Darüber lässt sich sicher schön diskutieren!

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

Ein gutes Gespür hilft gegen Datenpannen

Moderne IT-Sicherheitslösungen unterstützen dabei, Internetattacken und Datenpannen möglichst frühzeitig zu erkennen. Doch es kommt auch auf Sie als Nutzer an, auf Ihre Aufmerksamkeit und Wachsamkeit.

Falscher Alarm oder echter Angriff?

Wenn Ihr Antivirenprogramm Alarm schlägt, ist immer Vorsicht angezeigt. In den meisten Fällen wurde tatsächlich ein gefährliches Schadprogramm entdeckt. Manchmal aber liegt auch ein guter Antivirenschutz falsch und verdächtigt eine harmlose Datei.

Nicht immer liegen Antivirenprogramme richtig mit ihren Meldungen (Bild: Thinkstock/Nuno André)

Sie als Nutzer sollten jede Warnung und Alarmmeldung ernst nehmen und sich so verhalten, wie es Ihr Unternehmen für den Fall einer Virenwarnung vorsieht. Manchmal aber übersehen Sicherheitslösungen mögliche Gefahren und tatsächliche Attacken. Hier sind Sie gefragt, die Augen offen zu halten.

Der Nutzer als Gefahrensensor

Keine noch so gute Software kann es mit der menschlichen Intelligenz aufnehmen, heute und wahrscheinlich auch in Zukunft nicht. Eine Sicherheitslösung kann immer nur auf Basis der Regeln reagieren, die in der Anwendung hinterlegt sind. Selbst die Analysen, die verdächtiges Verhalten von Dateien und Programmen entdecken und bewerten, arbeiten immer auf einer definierten Grundlage.

Neuartige Angriffe stellen für technische Lösungen deshalb immer eine große Herausforderung dar. Das trifft natürlich auch für uns Nutzer zu. Doch wir können mit unserem Gespür für mögliche Risiken zur Gefahrenabwehr beitragen.

Vorsichtig sein, aber nichts übertreiben

Nun sollen Sie natürlich nicht immer gleich einen Angriff vermuten, wenn etwas scheinbar Ungewöhnliches am PC, Smartphone oder Drucker passiert. Aber es ist wichtig, vorsichtig und aufmerksam zu sein, denn auch bei installierter und aktivierter Sicherheitssoftware könnten Angreifer versuchen, personenbezogene Daten einzusehen, zu manipulieren und zu stehlen.

Ein Gespür für mögliche Anzeichen eines Angriffs oder einer Sicherheitspanne können Sie entwickeln, indem Sie sich angewöhnen, auf Vorkommnisse zu achten, die ein Alarmzeichen sein können, aber nicht müssen.

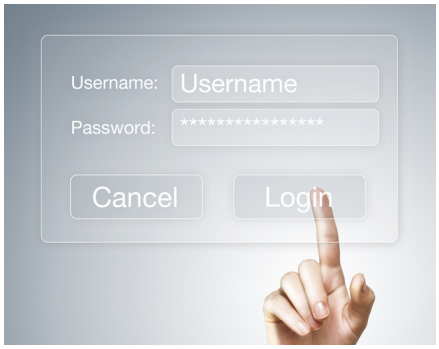
Wer hat die Datei versteckt?

Wenn Sie zum Beispiel feststellen, dass eine von Ihnen erstellte Datei plötzlich an anderer Stelle im Netzwerk liegt und Sie sie nur noch über eine Suche finden, könnte dahinter eine Ihnen nicht bekannte Maßnahme der Systemadministration stecken, zum Beispiel im Rahmen einer Reorganisation.

Es könnte aber auch ein unerlaubter Zugriff eines Dritten vorliegen. Fragen Sie deshalb zur Sicherheit nach, wenn Ihre Dateien plötzlich wandern.

Wenn ein Passwort nicht mehr funktioniert

Vielleicht müssen Sie aber auch feststellen, dass eines Ihrer Kennwörter nicht mehr gültig zu sein scheint. Dann könnte aus Sicherheitsgründen ein Zurücksetzen der Passwörter erfolgt sein, oder Sie haben vergessen, gemäß Passwortrichtlinie ein neues Passwort zu wählen. In aller Regel wären Sie dann aber zuerst intern informiert worden.



Melden Sie unerklärliche Passwortprobleme an Ihre IT (Bild: Thinkstock/NemanjaZs)

Möglich ist aber auch, dass ein Angreifer Ihr Benutzerkonto geknackt hat und Sie nun aussperrt, indem er ein neues Passwort vergeben hat. Um dieses Risiko nicht einzugehen, sollten Sie Passwortprobleme, die sich nicht offensichtlich erklären lassen, an Ihre Systemadministration melden.

Weitere Warnzeichen

Weitere mögliche Warnzeichen für Internetangriffe sind:

- plötzliche Veränderungen an Ihren Dateien, die Sie sich nicht erklären können

- E-Mails im Gesendet-Ordner, die nicht von Ihnen stammen

- Veränderungen an Einstellungen und Optionen bei Software und Geräten, die Sie sich nicht erklären können

- unerklärliche Fehler beim Versuch der Benutzeranmeldung

- eine plötzliche Verschiebung oder Umverteilung von Dateien

- unerwartete, gehäufte Störungen bei Ihren Endgeräten

Nicht auf Kundenreaktionen warten

Damit die Folgen eines möglichen IT-Sicherheitsvorfalls so gering wie möglich bleiben, sind im Verdachtsfall schnelle, aber besonnene Reaktionen wichtig. Es sollte nicht so sein, dass eine Datenpanne im Unternehmen erst auffällt, wenn sich die betroffenen Kunden beschweren.

Informieren Sie Systemadministration und Datenschutzbeauftragten

Wenn Sie denken, dass etwas nicht stimmt und vielleicht ein Angriff oder eine andere Datenpanne vorliegen könnte, melden Sie dies der Systemadministration. Wenn es um personenbezogene Daten geht, wenden Sie sich bitte **zusätzlich** an Ihren Datenschutzbeauftragten.

Keine eigenen Ermittlungen!

Starten Sie aber keine eigenen Ermittlungen oder nicht abgestimmte Abwehrversuche! Verstehen Sie sich als zusätzlichen Gefahrensensor und nicht als aktive Abwehr. Dafür gibt es die Spezialisten und in den meisten Fällen die IT-Sicherheitssoftware.

Smartwatch: Der Spion am Handgelenk?

Smartphones wurden schon häufig als Spione in der Hosentasche bezeichnet. Was aber ist mit den Smartwatches und Smart-TVs? Droht hier ebenfalls eine heimliche Überwachung?

Was smarte Produkte auszeichnet

Haben Sie sich schon einmal gefragt, was ein Smartphone von einem klassischen Handy unterscheidet? Der Internetzugang und die E-Mail-Funktion können es ja nicht sein, denn sie gab es schon bei vielen Mobiltelefonen. Das Smarte an den Smartphones ist, dass sie wie Computer vielfältige Funktionen übernehmen können und durch die Apps so flexibel sind.

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) geht in ihrer Definition von smarter Technologie noch weiter und führt aus, dass smarte Geräte über Anwendungen verfügen, die Daten sammeln, auf die Entwicklungen reagieren und die Resultate anderen Diensten oder dem Nutzer mitteilen. Was so kompliziert klingt, bedeutet letztlich, dass smarte Geräte auf den Nutzer bzw. die aktuelle Umgebung reagieren, ihre Dienste also zum Beispiel an Ihren aktuellen Standort anpassen können.

Datensammlung und -auswertung

Smartphones mit ihren Apps und Ortungsfunktionen werden oftmals als Datensammler, ja als Spione bezeichnet, weil die Sammlung und Analyse der Daten häufig ohne Wissen und Zustimmung der Nutzer geschieht. Da stellt sich die Frage, ob dies für andere smarte Produkte wie Smartwatches und Smart-TVs auch gilt. Steht also in Ihrem heimischen Wohnzimmer ein Spion, oder tragen Sie statt einer Uhr einen Spion um Ihr Handgelenk?

Smartwatches: Viel mehr als Uhrzeit und Wetterbericht

Je nach Modell und Anbieter kann eine Smartwatch eine Armbanduhr sein, die neben der Uhrzeit noch zusätzliche Informationen aus dem Internet anzeigt, wie zum Beispiel die Wettervorhersage für den aktuellen Standort. Eine Smartwatch kann aber auch E-Mails empfangen, Zugang zu Facebook bieten und Apps beherbergen, die Daten zur körperlichen Fitness des Trägers sammeln, analysieren und sogar bei Online-Diensten veröffentlichen.

Da Uhren ihre Benutzer noch häufiger begleiten als Smartphones, könnten Smartwatches Bewegungsprofile rund um die Uhr aufzeichnen. Wenn man als Nutzer dies nicht ahnt und nicht möchte, es aber trotzdem geschieht, hätte man tatsächlich eine Dauerüberwachung am eigenen Handgelenk.

Smart-TVs: Wer ist hier der Zuschauer?

Bei den intelligenten Fernsehern, den Smart-TVs, sind bereits kritische Funktionen aufgefallen. Um zum Beispiel Videotelefonate am TV-Gerät zu ermöglichen, haben viele Smart-TVs eine eingebaute Kamera. Sicherheitsforscher konnten zeigen, dass bei unzureichend gesicherten Smart-TVs die integrierte Webcam gehackt werden könnte. Dann wird der Zuschauer schnell zum Beobachtungsobjekt.

Ebenfalls bemängelt wurde, dass verschiedene Smart-TVs Daten über die Interessen und Sehgewohnheiten sammeln könnten - hochinteressant für Werbung, bei der TV- und Online-Werbung verschmelzen. Für den Nutzer jedoch bedeutet dies, dass sein TV-Erlebnis in heimliche Überwachung ausarten könnte. Je nach App sind weitere Datensammlungen und heimliche Analysen denkbar, genau wie bei Smartphones.

Neuartige Funktionen immer hinterfragen

So komfortabel und spannend die Funktionen der smarten Geräte sind: Sie sollten die Funktionen auch als mögliche Risiken für Ihre Privatsphäre sehen. Das gilt für Smartphones genauso wie für Smart-TVs oder Smartwatches. Suchen Sie deshalb nach den Datenschutz- und Sicherheitseinstellungen bei Ihren smarten Geräten und nutzen Sie sie!

Kennen Sie die Risiken der neuen smarten Produkte?

Frage: Sie haben sich zu Weihnachten endlich eine dieser tollen Smartwatches geleistet. Kann dies Folgen für Ihre Privatsphäre haben?

a) Nein, wieso? Es ist doch nur eine Uhr mit Zusatzfunktionen.
b) Leider ja. Es könnten zum Beispiel Apps darauf laufen, die heimlich meinen Standort protokollieren.

Lösung: Die Antwort b) ist richtig. Bei den Apps der Smartwatches bestehen ganz ähnliche Risiken wie bei den Smartphones. Wenn man nicht aufpasst, könnte aus der scheinbar harmlosen Uhr ein Überwachungsgerät werden.

Frage: Sie sehen sich Ihren Lieblingskrimi auf dem Smart-TV an. Besteht die Gefahr, dass Sie von Kriminellen dabei beobachtet werden?

a) Ja, Sicherheitsforscher warnen vor Angriffen auf die Kameras, die in Smart-TVs eingebaut sind.
b) Unsinn. Die Kriminellen sind im Film, nicht im Fernseher.

Lösung: Antwort a) ist richtig. Genau wie die Webcam im PC, Notebook oder Smartphone kann auch die Kamera in einem Smart-TV angegriffen und missbraucht werden.

Frage: Ihr Filmgeschmack ist Ihre Privatsache. Kann es passieren, dass Ihre TV-Gewohnheiten Dritten bekannt werden?

a) Nur wenn ich an entsprechenden Umfragen teilnehme.
b) Manche Smart-TVs haben schon protokolliert, was die Nutzer anschauen.

Lösung: Die Antwort b) ist richtig. Auf die Kritik von Sicherheitsforschern hin hat ein bekannter Anbieter von Smart-TVs bereits ein Update bei den Fernsehern eingespielt, das die Protokollierung abstellen soll. Durch den Internetanschluss der Smart-TVs besteht also die generelle Gefahr, dass Nutzungsdaten in die Hände Dritter gelangen könnten.