agentia wirtschaftsdienst

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

wenn Ihr Nachbar eine private Flug-Drohne über Ihr Grundstück fliegen lässt, kann Neugierde dahinterstecken. Wenn Ihre Bank wissen will, welcher Religion Sie angehören, hat das andere Gründe. Lesen Sie in dieser aktuellen Ausgabe, was mit einer fliegenden Kamera erlaubt ist und was nicht, und erfahren Sie, was es mit der möglichen Frage Ihrer Bank zu Ihrer Religionszugehörigkeit auf sich hat.

Antworten auf die ebenfalls sehr aktuellen Fragen, wie sich die Sicherheit bei der Facebook-Nutzung erhöhen lässt und worauf es bei der Verschlüsselung von Daten in der Cloud ankommt, erhalten Sie in den weiteren Beiträgen Ihrer neuen Datenschutz-Zeitung. Sie werden sehen, dass sich noch einiges für Ihre Sicherheit in sozialen Netzwerken tun lässt, aber auch, dass noch weitaus mehr für die Sicherheit von Daten in Clouds getan werden muss.

Wir wünsche Ihnen eine spannende Lektüre,

Ihre Datenschutzbeauftragten der agentia wirtschaftsdienst

Warum interessiert sich die Bank plötzlich für meine Religion?

Banken, aber auch Bausparkassen und andere Finanzinstitute verschicken neuerdings Mitteilungen, in denen sie ankündigen, dass sie beim Bundeszentralamt für Steuern (BZSt) die Religionszugehörigkeit ihrer Kunden abfragen. Was steckt dahinter?

Regelabfrage und Anlassabfrage

Regelabfrage und Anlassabfrage beim Bundeszentralamt für Steuern - schon die Begriffe wecken vielfach Misstrauen. Doch genau sie tauchen in Hinweisblättern auf, die Finanzinstitute neuerdings an ihre Kunden verschicken. Kann es richtig sein, dass Banken & Co. beim Bundeszentralamt nach der Religion ihrer Kunden fragen dürfen? Und wozu das Ganze, bisher ging es offensichtlich doch auch ohne diese Angaben?

Lücken im System der Kirchensteuer

Wie so oft bildet das liebe Geld den Hintergrund für die Änderung. In diesem Fall geht es um die Kirchensteuer auf Kapitalerträge (also vor allem auf Zinsen). Dass für Kapitalerträge genauso Kirchensteuer gezahlt werden muss wie für andere Einkünfte (etwa für den Arbeitslohn), galt auch schon bisher. Allerdings hat sich in den letzten Jahren gezeigt, dass die Abführung der Kirchensteuer in der Praxis nicht funktioniert, wenn Kapitalerträge über die "Abgeltungssteuer" versteuert werden.

In diesem Fall zieht das Finanzinstitut pauschal einen gesetzlich vorgeschriebenen Steuersatz von den Kapitalerträgen ab, überweist den Betrag an die Finanzverwaltung, und für den Steuerpflichtigen ist die Versteuerung der Kapitalerträge damit erledigt.

Bisher: keine pauschale Kirchensteuer

So weit, so gut. Was die meisten Steuerpflichtigen jedoch nicht wissen: Die Pauschalversteuerung betrifft nur die Lohnsteuer/Einkommensteuer, nicht die Kirchensteuer.

Ab 2015 müssen Banken die Kirchensteuer, die auf Kapitalerträge anfällt, direkt an die Religionsgemeinschaften abführen (Bild: Thinkstock/filmfoto)

Die Folge: Die Kirchen gingen bei der Pauschalversteuerung von Kapitalerträgen bisher regelmäßig leer aus. Denn kaum ein Steuerpflichtiger meldete sich beim zuständigen Kirchensteueramt und zahlte die Kirchensteuer von sich aus nach.

Ab 1. Januar 2015 kommt die pauschale Kirchensteuer

Genau ein solches Pauschalverfahren soll deshalb ab 1. Januar 2015 auch für die Kirchensteuer eingeführt werden.

Dazu müssen die Banken allerdings wissen, ob ein Kunde steuerpflichtig ist, und falls ja, welcher Kirche er angehört. Aus diesem Grund müssen sie 2014 erstmals bei der Steuerverwaltung nachfragen, ob ihr Kunde Angehöriger einer Steuer erhebenden Religionsgemeinschaft ist. Das ist gesetzlich ausdrücklich geregelt in § 51a Einkommensteuergesetz.

Ein Sperrvermerk hält die Bank außen vor

Wer nicht möchte, dass die Bank seine Religion erfährt, kann einen Sperrvermerk beim Bundeszentralamt für Steuern eintragen lassen. Das hierfür vorgeschriebene amtliche Formular "Erklärung zum Sperrvermerk" ist online erhältlich und muss per Post eingeschickt werden: http://kurzlink.de/formular_bzs. Der Abzug der Kirchensteuer erfolgt dann über das Finanzamt und nicht pauschal durch die Bank.

Beobachtung des Nachbarn mit einer privaten Drohne - erlaubt oder nicht?

Quadrocopter, Quadcopter, Microcopter oder schlicht Drohne - so heißen ferngesteuerte Flugobjekte mit Kamera. Sie sind im Internet leicht zu haben: einfache Geräte gebraucht mit etwas Glück schon für 100 Euro, neue Geräte mit allen technischen Schikanen und einer Top-Kamera für knapp unter 2.000 Euro. Ein nettes Spielzeug, wenn man es mag. Aber kann es damit auch Ärger geben?

Auf dem eigenen Grundstück kein Problem

Damit von vornherein keine unnötigen Befürchtungen aufkommen: Solange sie über dem eigenen Grundstück fliegen, sind Drohnen sicher kein Problem des Datenschutzes. Wer Freude daran hat, kann selbstverständlich sein eigenes Haus von oben fotografieren. Dasselbe gilt für Vögel, die sich am Futterhäuschen versammelt haben - wenn sie nicht wegen des Lärms oder wegen der für sie bedrohlich wirkenden Silhouette des Fluggeräts nicht schon längst Reißaus genommen haben.

Möglicherweise spielt der Nachbar sogar mit

Selbstverständlich spricht auch nichts dagegen, dem mehr oder weniger staunenden Nachbarn die Neuerwerbung vorzuführen und ihm vorzuschlagen, doch auch einmal sein Haus von oben zu fotografieren. Wahrscheinlich wird er aus Gründen der Höflichkeit selbst dann "ja" sagen, wenn er innerlich den Kopf schüttelt.

Heimliche Aufnahmen sind jedoch tabu

Deutlich weniger lustig wird es, wenn der Nachbar oder seine Familie ohne ihr Wissen von oben fotografiert werden. Das ist angesichts der leistungsfähigen Kameras, über die manche Drohnen verfügen, inzwischen durchaus möglich, ohne dass es die Betroffenen bemerken. Dabei beginnt der Ärger keineswegs erst, wenn sich die Nachbarin - im Glauben, vor Blicken anderer geschützt zu sein - "oben ohne" auf der Liege im Garten sonnt.

Das eigentliche Datenschutzrecht schweigt zum Thema

Das eigentliche Datenschutzrecht (vom Bundesdatenschutzgesetz bis zu den Landesdatenschutzgesetzen) hilft bei der Frage, was erlaubt ist und was nicht, erstaunlicherweise allerdings nicht weiter. Der Anwendungsbereich dieser Regelungen ist nämlich beschränkt. Er klammert ausschließlich persönliche Tätigkeiten aus, also etwa die Ausübung eines Hobbys. Genau darum geht es hier jedoch.

Drohnen mit ihren Kameras eignen sich wunderbar, um auch einmal einen Blick in Nachbars Garten zu werfen - doch Vorsicht!
(Bild: Thinkstock/andreart)

Das Strafgesetzbuch enthält aber klare Aussagen

Das bedeutet jedoch nicht, dass sich der Einsatz von Drohnen im rechtsfreien Raum abspielen würde. Ganz im Gegenteil! Wer nicht aufpasst, kann sogar mit dem Strafrecht in Berührung kommen. Dort gibt es nämlich eine Vorschrift, die eine Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen untersagt. Sie verbietet unbefugte Bildaufnahmen von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet (§ 201a Strafgesetzbuch). Wer dagegen verstößt, riskiert im Extremfall also ein Strafverfahren.

Finger weg von geschützten Räumen!

Aufnahmen von einer Person in ihrer Wohnung wird man mit einer Drohne kaum herstellen können. Anders sieht es aus mit Aufnahmen von Personen, die sich in einem gegen Einblick besonders geschützten Raum befinden. Dazu zählt die hoch gelegene Dachterrasse ebenso wie der Liegeplatz im Garten, der von so hohen Hecken umgeben ist, dass unter normalen Umständen niemand hineinschauen kann.

Wichtig: Das gilt auch dann, wenn die Situation an sich völlig harmlos ist und der Nachbar zum Beispiel am Gartentisch sitzt und dort Zeitung liest. Es muss sich also keineswegs um eine peinliche Situation handeln.

Im Ernstfall gleich an eine Entschuldigung denken!

Von solchen Versuchungen sollte man also in jedem Fall die Finger lassen. Dies gilt auch und vor allem für Jugendliche, die der Faszination eines fliegenden Geräts besonders schnell erliegen. Denn auch wenn Strafverfahren wegen Aufnahmen mit Drohnen bisher noch nicht bekannt geworden sind, sind die Nachbarin oder der Nachbar im Zweifelsfall jedenfalls nachhaltig verstimmt, wenn sie bemerken, dass sie heimlich fotografiert worden sind. Hier kann man dann nur zu einer raschen Entschuldigung und einem Blumenstrauß raten, um rechtliche Folgen erst gar nicht zum Thema werden zu lassen.

Vorsicht in der Nähe von Flughäfen!

Fernab vom Datenschutz sollte man stets bedenken, dass Fluggeräte aller Art andere nicht behindern oder gar bedrohen dürfen. Wer eine Drohne in der Nähe von Flugplätzen (auch kleinen Flugplätzen, etwa nur für Segelflugzeuge) aufsteigen lassen will, sollte daher ganz besonders das Motto beachten: Erst denken, dann starten!

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

Soziale Netzwerke: So wird Facebook sicherer

Wo viele Internetnutzer zusammenkommen, wird es für Datendiebe besonders interessant. Facebook & Co. sollten deshalb nicht ohne besondere Sicherheitsmaßnahmen genutzt werden.

Die volle Bandbreite an Chancen und Risiken

Wer heute als Internetnutzer zugibt, (noch) nicht auf Facebook oder einem anderen sozialen Netzwerk zu sein, könnte schnell als rückständig angesehen werden. Selbst Unternehmen möchten zunehmend, dass man sie auch auf Facebook & Co. findet. Tatsächlich nutzen bereits viele Unternehmen in Deutschland die geschäftlichen Möglichkeiten von Facebook, setzen sich dabei aber einer Vielzahl von Gefahren aus.

Kaum ein Angriffstyp fehlt auf Facebook

Die Europäische Agentur für Netz- und Informationssicherheit ENISA hat zusammengestellt, mit welchen Gefahren man bei Cloud Computing, Mobile Computing und auch sozialen Netzwerken rechnen muss.

Für soziale Netzwerke wie Facebook oder Twitter reichen die Online-Bedrohungen von ungewollter oder verbotener Veröffentlichung vertraulicher Informationen über Trojaner und Spyware bis hin zu Spam, Passwortdiebstahl (Phishing) und Identitätsdiebstahl.

Endgeräte, auf denen ein soziales Netzwerk läuft, könnten missbraucht und heimlich ferngesteuert werden, wenn die nötige IT-Sicherheit fehlt.

Doch es gibt spezielle Sicherheitslösungen

Wie bei der Nutzung anderer Online-Dienste auch sollte der eingesetzte Webbrowser oder die entsprechende mobile App aktuell sein, ebenso das jeweilige Betriebssystem des Endgeräts. Eine Anti-Malware-Software auf dem PC, Notebook, Tablet oder Smartphone darf auch nicht fehlen.

Aber Sie können noch mehr tun, wenn Sie die Sicherheit bei der Verwendung eines sozialen Netzwerks steigern möchten. Dabei ist es eigentlich keine Frage des Wollens: Die aktuellen Bedrohungen und Angriffe über soziale Netzwerke wie Facebook machen besondere Sicherheitsmaßnahmen zur Pflicht, wenn Sie nicht auf Facebook & Co. verzichten.

Scannen der Downloads reicht nicht

Wenn Sie eine Datei aus einem sozialen Netzwerk herunterladen wollen, die Ihnen ein Kontakt geschickt hat, können und sollten Sie diese Datei vor dem Öffnen mit Ihrem Antiviren-Programm prüfen, genau wie E-Mails.

Doch Schadsoftware kann nicht nur in den Dateianhängen von Facebook-Nachrichten stecken. Auch die Online-Werbeanzeigen und die Bilder auf Online-Profilen in Facebook könnten verseucht sein. Der Trojaner könnte bereits beim Betrachten der Bilder oder Werbung übertragen werden (Drive-by-Download).

Deshalb ist es mehr als sinnvoll, Facebook-Werbung und -Profile bereits vor dem Anschauen untersuchen zu lassen. Dafür gibt es spezielle, meist kostenlose Sicherheitstools wie ESET Social Media Scanner, Defensio 2.0, Bit-Defender Safego oder Norton Safe Web.

Diese Lösungen können Ihnen zum Beispiel dabei helfen, Facebook sicherer zu nutzen:

- AVG CrowdControl (https://www.facebook.com/AVG)

- BitDefender Safego (https://apps.facebook.com/bd-safego/)

- Websense Defensio 2.0 (http://www.defensio.com/)

- ESET Social Media Scanner (http://www.eset.com/de/social-media-scanner/)

- Norton Safe Web (https://www.facebook.com/appcenter/nortonsafeweb)

- Zscaler Likejacking Prevention (http://www.zscaler.com/zscaler_likejacking.php)

Verschiedene Sicherheitslösungen versprechen, soziale Netzwerke sicherer zu machen
(Bild: Thinkstock/VLADGRIN)

Spam kommt nicht nur per E-Mail

Viele der speziellen Sicherheitswerkzeuge für Facebook-Nutzer suchen nicht nur nach Malware, sondern auch nach Spam. So ist zu beobachten, dass die Zahl der Spam-Nachrichten in sozialen Netzwerken deutlich zunimmt. Spam-Filter im E-Mail-Programm aber können diese Spam-Nachrichten nicht erkennen. Hierzu sind Spam-Filter in den Nachrichten-Funktionen der sozialen Netzwerke notwendig, aber auch verfügbar.

Datenschutzeinstellungen verbessern

Laut einer Umfrage des Hightech-Verbands BITKOM haben immerhin fast 70 Prozent der Nutzer sozialer Netzwerke die Datenschutzvoreinstellungen bei Facebook & Co. abgeändert. Das ist sehr erfreulich, doch teilweise bieten die sozialen Netzwerke die gewünschten Datenschutz-Optionen gar nicht. Deshalb können Tools wie AVG CrowdControl helfen: Damit lässt sich zum Beispiel noch genauer festlegen, welcher Kontakt Statusmeldungen, gepostete Videos oder Fotos auf der persönlichen Pinnwand sehen darf, ohne die zu sperrenden Kontakte löschen zu müssen.

Facebook-Risiken reduzieren

Wenn Sie also Facebook privat nutzen oder betrieblich einsetzen, sollten Sie die großen Risiken für Ihre und andere personenbezogene Daten im Blick haben. Dazu gehört es, spezielle Sicherheitstools einzusetzen, die den besonderen Gefahren von Facebook & Co. gezielt begegnen. Sprechen Sie deshalb mit Ihrem IT-Administrator, welche der genannten Sicherheitserweiterungen im Unternehmen zu-gelassen sind oder werden.

Worauf es bei der Verschlüsselung in Clouds ankommt

Clouds sind viel häufiger im Einsatz, als es vielen Unternehmen und Privatpersonen bewusst ist. Dabei wird jedoch oftmals nicht auf die richtige Verschlüsselung für die Daten geachtet.

Die Verlockungen der Cloud

Obwohl sich viele Unternehmen bei Cloud Computing Gedanken um die Sicherheit ihrer Daten machen, nimmt die Cloud-Nutzung weiter zu. Die erhofften Vorteile wie eine kostengünstige und flexible Nutzung von Speicherkapazität aus dem Internet sind einfach zu groß. Manchmal ist Unternehmen auch gar nicht wirklich klar, dass sie eine Cloud einsetzen.

Das ist bei Privatpersonen nicht anders, im Gegenteil. So werden Cloud-Dienste als praktischer Datenspeicher genutzt, ohne sich weiter Gedanken zu machen. Bei Webmail, Foto-Speichern im Internet oder der Ablage von Dateien in den Profilen sozialer Netzwerke ist vielen Nutzern gar nicht bewusst, dass sie dabei letztlich Cloud Computing nutzen.

Das Missverständnis bei der Verschlüsselung

Cloud-Dienste werden nicht als solche erkannt oder als harmlose Online-Speicher interpretiert, und auch bei der Verschlüsselung gibt es falsche Vorstellungen. Viele Internetnutzer achten zwar inzwischen bei der Übertragung von Daten ins Internet auf die Kennzeichen einer Verschlüsselung, prüfen also, ob die Webadresse mit "https" beginnt.

Doch die Bedeutung dieser Verschlüsselung wird falsch eingeschätzt: Eine SSL- oder TLS-Verschlüsselung (Secure Sockets Layer oder Transport Layer Security) betrifft die Übertragung zwischen dem Browser und dem jeweiligen Webserver, also zum Beispiel die Übertragung vom Browser zum Server eines Online-Foto-Speicherdienstes. Über die Verschlüsselung nach der Übertragung sagt https jedoch nichts aus.

Auch gespeicherte Daten müssen verschlüsselt sein

Will man seine Daten auch nach der Übertragung vor unerlaubten Blicken und Zugriffen schützen, muss neben der Datenübertragung auch die Speicherung der Daten verschlüsselt erfolgen. Verschiedene Cloud-Speicherdienste versprechen auch, dass die gespeicherten Daten ebenfalls verschlüsselt werden. Doch ist damit dem Datenschutz Genüge getan? Kann nun wirklich kein Unbefugter auf die privaten Daten oder die betrieblichen Daten in einer so geschützten Cloud zugreifen? Leider doch.

Wer hat den Schlüssel?

Wie Sie wissen, braucht man zur Entschlüsselung von Daten den jeweiligen Schlüssel. Anders ausgedrückt, kann jeder, der den richtigen Schlüssel hat, die Daten in der Cloud entschlüsseln, vorausgesetzt, er oder sie kann auf die Daten zugreifen, kennt also zum Beispiel das Nutzerpasswort.

Es stellt sich die Frage, wer auf die Nutzerkonten zugreifen kann und wer über die Schlüssel verfügt. Die Antwort: Ohne weitere Sicherheitsmaßnahmen könnten das der Cloud-Administrator und damit der Cloud-Provider sein. Möglich ist dies insbesondere dann, wenn man die Verschlüsselung seiner Cloud-Daten einfach dem Cloud-Anbieter überlässt.

Selbst verschlüsseln ist Trumpf!

Wer Cloud-Dienste nutzt und damit seine Daten einem Dritten übergibt, sollte nicht auch noch die Sicherheit der Daten anderen überlassen. Der Cloud-Anbieter sollte sehr wohl die Übertragung sowie die Speicherung der Daten seiner Kunden und Nutzer verschlüsseln. Aber die Anwender sollten selbst ebenfalls verschlüsseln, und zwar bereits vor der Datenübertragung in die Cloud.

Die Schlüssel für diese Verschlüsselung dürfen nicht dem Cloud-Anbieter zugänglich gemacht werden, wenn denn die Vorab-Verschlüsselung wirklich zuverlässig helfen soll. Vielmehr sollten Cloud-Nutzer ihre Schlüssel jenseits der Cloud aufbewahren, zum Beispiel auf einer Smartcard. Nur mit einer vom Cloud-Anbieter unabhängigen Verschlüsselung kann man davon ausgehen, dass kein Dritter, auch kein Mitarbeiter des Cloud-Providers, die eignen Daten einsehen kann.

Verschlüsseln Sie Ihre Daten für die Cloud richtig?

Frage: Sie speichern Ihre privaten Fotos bei einem Internetdienst. Woran erkennen Sie, dass die Daten dort sicher sind?

a) Ich achte auf "https" in der Adresszeile meines Browsers, dann sind die Daten verschlüsselt und sicher.
b) Ich kann nicht ohne Weiteres sehen, ob meine Daten dort sicher sind.

Lösung: Die Antwort b) ist richtig. Natürlich ist es wichtig, auf eine Verschlüsselung bei der Datenübertragung zu achten. Ob die Daten nach der Übertragung sicher sind, erkennt man aber an "https" nicht.

Frage: Sie nutzen einen Cloud-Speicherdienst, der in seiner Leistungsbeschreibung versichert, dass die Daten nur verschlüsselt gespeichert werden. Reicht Ihnen diese Zusage?

a) Nein, denn es kommt darauf an, wer den Schlüssel zur Entschlüsselung hat. Nur wenn der Schlüssel vor Missbrauch geschützt ist, ist die Verschlüsselung wirklich ein Mehrwert.
b) Ja, natürlich, vorausgesetzt, die Datenübertragung mit dem Browser erfolgt ebenfalls verschlüsselt.

Lösung: Antwort a) ist richtig. Wenn Sie die Verschlüsselung dem Cloud-Anbieter überlassen und nicht selbst (zusätzlich) verschlüsseln, haben Sie ohne Weiteres keine Kontrolle über den Schlüssel und damit über die Sicherheit Ihrer Daten.