Newsletter Datenschutz
Ausgabe 08 | 2015

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

Fotos sollen eine schöne, bleibende Erinnerung, etwa an einen Urlaub, sein. Doch was ist, wenn man Bilder oder andere Daten wieder löschen will? Bei vielen Android-Smartphones gibt es Probleme mit dem Löschen von Daten, wie diese Ausgabe zeigt. Zudem erfahren Sie, ob Sie zum Beispiel Anspruch darauf haben, aus einem Film Ihres früheren Arbeitgebers gelöscht zu werden.

Diese Ausgabe erklärt auch, wie sich die Daten Verstorbener aus dem Internet löschen lassen. Doch das Internet hält weitere Fragen bereit: Wissen Sie, wie Sie eine gefährliche Webseite von einer harmlosen unterscheiden können? Die Antwort darauf finden Sie auf dieser Seite.

Ich wünsche Ihnen wieder viele wertvolle Einsichten in den Datenschutz!

Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

Wie erkennt man eine gefährliche Webseite?

Jeden Tag entdeckt die Suchmaschine Google fast zehntausend neue Webseiten, von denen Gefahr ausgeht. Die Opfer dagegen brauchen Monate, um einen Angriff festzustellen. Spezielle Tools können helfen, bösartige Internetseiten zu enttarnen.

Gefälschte Webauftritte stehlen Ihre Daten

Nicht nur Schmuck, teure Kleidung oder Banknoten werden gefälscht - auch die Internetauftritte seriöser Unternehmen und Organisationen sind vor Fälscherbanden nicht sicher. Das Ziel solcher Online-Fälschungen ist fast immer der Diebstahl von Zugangsdaten, sei es für das Online-Banking, für Webshops oder auch für Cloud-Speicherdienste.

Professionell gefälschte Webseiten haben Erfolg: Laut einer Google-Studie lassen sich 45 Prozent der Internetnutzer davon täuschen. Selbst weniger gute Online-Fälschungen haben bei weiteren 17 Prozent kriminelles Glück. Hat die Online-Attacke funktioniert, haben die Diebe viel Zeit, ihre Datenbeute zu missbrauchen. Schon einen Tag nach dem Diebstahl der Daten wurden 70 Prozent der Zugangskonten missbraucht. Im Durchschnitt dauert es aber 255 Tage, bis die Manipulation einer Webseite auffällt.

Webseiten vor der Nutzung überprüfen

Leider reicht es nicht, nach dem Öffnen einer Website im Browser festzustellen, dass die Internetseite gefährlich aussieht. Dann kann es schon zu spät sein. Webseiten können nicht nur gefälscht und auf den Diebstahl von Zugangsdaten aus sein, sie können auch Schadsoftware transportieren, die über den Browser oder über die Browsererweiterungen (Plug-ins) auf Ihren Rechner gelangen will.

Um solche Online-Attacken zu verhindern, müssen Sie bereits vor dem Besuch einer Webseite die Sicherheit kontrollieren.

Auch seriöse Seiten wie z.B. Webauftritte von Nachrichtenmagazinen können Opfer von Fälschern werden. Online-Scanner helfen dabei, sich davor zu schützen. *(Bild: Maksym Yemelynov/iStock/Thinkstock)*

Möglich ist dies durch spezielle Online-Scanner, die eine in das Suchfeld eingetragene Webseite überprüfen. Ein Beispiel ist AVG ThreatLabs (*www.avgthreatlabs.com/de-de/website-safety-reports/*).

Die geballten Informationen zahlreicher Online-Scanner erhalten Sie von dem Google-Tool VirusTotal (*www.virustotal.com/de/*). Für jede dort eingegebene Internetadresse erhalten Sie die Sicherheitsbewertung von gegenwärtig 63 Scanner-Diensten. Dabei bedeutet das Resultat 0/63, dass kein Scanner-Dienst bei der Webadresse Alarm schlägt.

Browser-Tools sorgen für dauerhafte Prüfung

Verschiedene Antivirus-Tools bieten zudem die Installation einer speziellen Browser-Erweiterung an, die meist durch ein Ampelsystem neben der Adresszeile im Browser anzeigt, ob die Webseite, die geöffnet werden soll, ungefährlich oder bedrohlich ist. Dabei wird sowohl der Verdacht auf Schadsoftware als auch eine mögliche Phishing-Attacke angezeigt.

Nutzen Sie deshalb zusätzliche Sicherheitstools für Ihren Browser vom Hersteller Ihrer Antiviren-Software, um vor gefährlichen Webseiten rechtzeitig gewarnt zu werden und um nicht erst nach mehr als 200 Tagen festzustellen, dass eine Online-Attacke stattgefunden hat.

Ein Monteur als Fotomodell des Arbeitgebers

Ein Monteur wirkt an einem Imagefilm für das Unternehmen mit, bei dem er arbeitet. Als er später aus dem Arbeitsverhältnis ausscheidet, möchte er, dass sein Ex-Arbeitgeber den Film auf der Homepage des Unternehmens löscht. Kann der Monteur das ernsthaft verlangen?

Zwei "Mini-Auftritte" in einem Imagefilm

Ein Unternehmen wollte seinen Internetauftritt neu gestalten. Dazu gehörte auch ein Werbefilm von etwa drei Minuten Länge. Die Werbeleute rieten dringend dazu, in diesem Film nur echte Mitarbeiter auftreten zu lassen, weil das authentischer wirkt. So geschah es. In dem Film sind insgesamt über 30 Arbeitnehmer des Unternehmens zu sehen, darunter auch der Monteur. Er tritt zweimal auf: Einmal steht er an einem Schaltschrank. Einmal sitzt er auf einem Stuhl. Beide Szenen sind jeweils etwa drei Sekunden lang.

Schriftliche Einwilligung im Vorfeld

Das Unternehmen hatte alle Mitarbeiter, die in dem Film zu sehen sein sollten, vorher um eine schriftliche "Einverständniserklärung" gebeten. In der Erklärung heißt es, dass die Filmaufnahmen zur freien Nutzung im Rahmen der Öffentlichkeitsarbeit des Unternehmens verwendet werden dürfen.

Um unnötigen Aufwand zu vermeiden, hatte das Unternehmen nicht jeden einzelnen Arbeitnehmer eine eigene Erklärung unterschreiben lassen. Vielmehr war der Einverständniserklärung eine Unterschriftsliste beigefügt, auf der alle betroffenen Arbeitnehmer - darunter auch der Monteur - unterschrieben hatten. Diese Unterschriftsliste trug die Überschrift "Thema: Filmaufnahmen".

Widerruf der Einwilligung beim Ausscheiden aus dem Unternehmen

Als der Monteur drei Jahre später aus dem Unternehmen ausschied, forderte er seinen früheren Arbeitgeber auf, das Video von der Homepage zu entfernen. Gleichzeitig widerrief er seine "möglicherweise erteilte Einwilligung betreffend die Filmaufnahmen".

Dennoch kein Anspruch auf Löschung des Films

Das Unternehmen kam seinem Wunsch sogar nach und entfernte den Film von seiner Internetseite. Gleichzeitig behielt es sich jedoch vor, die Aufnahmen erneut zu veröffentlichen. Deshalb kam es zu einem Rechtsstreit, der schließlich bis zum Bundesarbeitsgericht führte. Dort erlebte der Monteur dann eine deutliche Niederlage. Nach Auffassung des Bundesarbeitsgerichts darf sein früherer Arbeitgeber den Werbefilm einschließlich der Szenen mit dem Monteur auch künftig verwenden. Zur Begründung hebt das Gericht vor allem Folgendes hervor:

Stimmt ein Mitarbeiter Filmaufnahmen zu, kann er seine Zustimmung nicht in jedem Fall einfach zurücknehmen (Bild: kadmy/iStock/Thinkstock)

- Ob der Arbeitgeber überhaupt eine Einwilligung des Monteurs für die Aufnahmen benötigte, erscheint aus der Sicht des Gerichts zweifelhaft. Darauf komme es jedoch letztlich nicht an, weil die möglicherweise notwendige Einwilligung ohne jeden Zweifel vorhanden sei.

- Es ist aus der Sicht des Gerichts nicht notwendig, dass jeder einzelne Arbeitnehmer eine individuelle Einwilligung unterzeichnet. Die Unterschrift auf einer Unterschriftsliste genüge, wenn - so wie hier - ein eindeutiger Zusammenhang zwischen der Unterschrift und dem Einwilligungstexte bestehe.

Fortwirkung der Einwilligung auch nach dem Ausscheiden

- Das Ausscheiden aus dem Unternehmen hat nach Auffassung des Gerichts keinen Einfluss auf die Wirksamkeit der Einwilligung. Eine schriftlich erteilte Zustimmung zu Bild- oder Filmaufnahmen bleibe vielmehr auch dann wirksam, wenn das Arbeitsverhältnis beendet werde.

Widerruf nur aus plausiblem Grund möglich

- Zwar kann nach Meinung des Gerichts ein Arbeitnehmer eine einmal erteilte Einwilligung prinzipiell später widerrufen. Das gelte allerdings nur, wenn er einen plausiblen Grund für seinen Widerruf nennen könne. An einem solchen plausiblen Grund für einen Widerruf fehlt es aus der Sicht des Bundesarbeitsgerichts im vorliegenden Fall. Jedem Arbeitnehmer müsse klar sein, dass Filmaufnahmen sehr kostenaufwendig sind und nicht ständig neu erstellt werden können, nur weil einzelne Personen, die im Film zu sehen sind, aus dem Unternehmen ausscheiden.

Lebensnahe Argumentation des Gerichts

Die Argumente des Gerichts sind lebensnah und vernünftig. Wer in untergeordneter Rolle an einem Imagefilm mitwirkt, kann nicht erwarten, dass der Film nur deshalb gelöscht wird, weil er aus dem Unternehmen ausscheidet. Ohne dass diese Formulierung böse gemeint wäre, ist ein solcher Arbeitnehmer "austauschbar". Der Betrachter eines solchen Films erwartet nämlich lediglich, irgendeinen "echten" Mitarbeiter zu sehen. Wer dieser Mitarbeiter konkret ist, ist dem Betrachter dagegen gleichgültig.

Alternative für Betroffene: bei Filmaufnahmen nicht mitwirken!

Wenn jemand diese Überlegungen nicht für überzeugend hält, bleibt ihm selbstverständlich immer noch die Freiheit, nicht an Filmaufnahmen mitzuwirken. Zwingen kann und wird ihn dazu niemand.

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

Digitaler Nachlass - ein Sommerthema?

Sie liegen am Strand. Sie versenden gerade über WhatsApp oder Facebook schöne Sommerfotos. Und da sollen Sie darüber nachdenken, was mit Ihren Nachrichten und Ihren persönlichen Profilen geschehen würde, wenn ...? Warum eigentlich nicht? Wo steht geschrieben, dass solche Themen nur in den November gehören?

Fast jeder am Strand nutzt WhatsApp & Co.

Vermutlich über 80 % aller Touristen, die an einem Strand liegen, haben einen Account bei Facebook, schreiben Nachrichten über WhatsApp oder haben Bilder bei flickr.com oder ähnlichen Diensten hochgeladen. Das gehört heute zum Leben und macht oft viel Freude. Was aber ist, wenn das eigene Leben irgendwann endet? Was wird dann aus den Bildern, Texten und Nachrichten?

Viele bilden ihr ganzes Leben im Netz ab

Diese Frage ist schon deshalb wichtig, weil beispielsweise so mancher Facebook-Nutzer alle wesentlichen Stationen seines Lebens in Bild und Text hochgeladen hat. Diese Daten sind dann etwas ganz Wesentliches, das von ihm bleibt. Oder auch nicht, wenn alles einfach gelöscht wird. Natürlich kann man das Thema verdrängen. Aber ob das wirklich eine so gute Idee ist? Irgendwann wird es präsent sein. Das weiß jeder, der zum Beispiel schon einmal miterleben musste, wie in seinem Umfeld ein junger Mensch tödlich verunglückt ist.

Eine schriftliche Anordnung schafft Klarheit

Wer nichts dazu festlegt, was mit den eigenen Daten nach dem Tod geschehen soll, hinterlässt vor allem eines: Unsicherheit. Wenn Ihnen das Thema wichtig ist, sollten Sie deshalb schriftlich festhalten, was zum Beispiel mit Ihrem Facebook-Account geschehen soll. Soll er gelöscht werden? Oder wollen Sie das ganz bewusst nicht? Niemand kann dies ahnen, wenn es keine Festlegung gibt.

Beachten Sie Formvorschriften

Eine solche Anordnung kann selbstverständlich Teil eines Testaments sein. Sie kann aber auch unabhängig von einem Testament getroffen werden. Auch in diesem Fall sollten Sie jedoch die Formvorschriften für eigenhändige Testamente einhalten (handschriftlicher Text! Ort und Datum angeben! Unterschrift nicht vergessen, möglichst mit Vor- und Nachnamen!). Das vermeidet spätere Streitigkeiten.

Sorgen Sie dafür, dass die Anordnung gefunden wird

Die sorgfältigste Anordnung hilft nichts, wenn sie keiner kennt und wenn sie nach dem Tod nicht gefunden wird. Dieses Problem lässt sich auf unterschiedliche Art und Weise lösen:

- Falls die Anordnung Teil eines eigenhändigen Testaments ist, sollte das Testament möglichst in "öffentliche Verwahrung" gegeben werden. Jedes Amtsgericht gibt hierzu die nötigen Hinweise (auch telefonisch). Die Kosten betragen einmalig ungefähr 60 bis 80 Euro.
- Eine weniger sichere Alternative ist die Aufbewahrung in der eigenen Wohnung. Dann sollte möglichst jemand ins Vertrauen gezogen werden. Er kann sich dann später darum kümmern, dass die Anordnung auch gefunden wird.

Bald steht der Sommerurlaub an? Durchaus eine Gelegenheit, einmal über das Thema "digitaler Nachlass" nachzudenken (Bild: anyaberkut/iStock/Thinkstock)

Ohne Account-Übersicht geht es nicht

Viele Internetnutzer haben nicht nur einen Account, sondern mehrere. Dann stellt es oft ein Problem dar, sämtliche Accounts zu finden. Ideal wäre es deshalb, wenn Sie eine Übersicht mit allen Accounts anfertigen. Noch idealer wäre es, wenn Sie diese Liste immer wieder aktualisieren. Die Praxis zeigt, dass vor allem die Aktualisierung oft unterbleibt. Doch ist eine nicht ganz aktuelle Übersicht immer noch besser als keine. Die Übersicht sollte Ihrer Anordnung beigefügt werden.

Auch der Benutzername ist wichtig

Zu jedem Account sollte jedenfalls der Benutzername, der im Internet sichtbar ist, festgehalten werden. Nur so ist sichergestellt, dass klar ist, um welchen Account es jeweils geht. Die Anordnung "Mein Facebook-Account soll nach meinem Tod gelöscht werden" geht mit hoher Sicherheit ins Leere, wenn die Inhaberin beispielsweise im realen Leben Susanne Müller heißt, der Account aber die Bezeichnung "munich_cat" trägt.

Vorsicht bei Kennwörtern!

Fragwürdig erscheint dagegen der Ratschlag, auch das jeweilige Kennwort festzuhalten. Daraus ergeben sich nicht nur Sicherheitsprobleme für die Aufbewahrung der Übersicht. Vielmehr ist es auch nicht unbedingt nötig, das Kennwort nennen zu können, wenn man den Account eines anderen nach dessen Tod löschen lassen will.

Sofern die Anordnung des Verstorbenen im Original vorgelegt werden kann, ist eine Löschung auch dann möglich, wenn das Kennwort nicht genannt werden kann. Anders sieht es aus, wenn Sie möchten, dass jemand in Ihrem Auftrag den Account löschen kann, ohne dazu den Provider fragen zu müssen. Dann müsste er natürlich über das Kennwort verfügen. Eine echte Vertrauenssache!

Weiterführende Tipps im Internet

Sie möchten weiterführende Informationen zum Thema lesen? Dann können Sie zum Beispiel auf Tipps der Verbraucherzentrale Rheinland-Pfalz zurückgreifen. Sie sind im Internet abrufbar unter *http://www.verbraucherzentrale-rlp.de/mediabig/233739A.pdf*

Löschen mobiler Daten: Was funktioniert - und was nicht?

Wird ein Smartphone ausgemustert, versuchen viele Nutzer, ihre alten Daten durch Zurücksetzen des Geräts zu löschen. Leider funktioniert das oftmals nur teilweise. Ergebnis: Vertrauliche Daten bleiben zurück.

Handy-Recycling kann zum Datenleck werden

Etwa 100 Millionen Alt-Handys liegen ungenutzt in deutschen Haushalten. Ihre früheren Nutzer haben sich für ein neueres Modell entschieden. Da erscheint es sinnvoll, die Altgeräte anderweitig zu verwenden oder aber einem Recycling zuzuführen. Bevor Sie aber ein Smartphone oder Handy entsorgen oder einem Dritten geben, müssen Sie die noch brauchbaren Daten darauf zur weiteren Verwendung sichern und alle anderen Daten löschen.

Der übliche Sicherheitshinweis in diesem Fall lautet, das mobile Endgerät auf den Werkszustand zurückzusetzen. Das soll sämtliche Datenspuren vernichten. Tatsächlich aber können große Teile des mobilen Datenbestands übrig bleiben und unter Umständen von Unbefugten missbraucht werden.

Neue Studie belegt Löschprobleme bei Smartphones

Forscher der Universität Cambridge haben herausgefunden, dass die Funktion "Zurücksetzen" (Factory Reset) bei vielen Android-Smartphones nicht richtig funktioniert. Betroffen sind insbesondere Smartphones, die mit einer Android-Version unter 4.4 laufen, und das sind weltweit mehr als 500 Millionen Geräte.

Die Sicherheitsexperten bemerkten bei ihren Tests, dass die Speicher der Geräte nach dem Zurücksetzen nicht vollständig geleert waren. Tatsächlich fanden sie auf den gebrauchten Smartphones noch Bilder, Kontaktdaten, Passwörter, mitunter sogar Bankverbindungen der Vorbesitzer. Aus dem Handy-Recycling wird dann die ungewollte Weitergabe vertraulicher Daten.

Selbst Löschfunktionen von Security-Apps arbeiten teils lückenhaft

Nutzer, die besonders vorsichtig sind und nicht nur auf das Zurücksetzen auf den Anfangszustand des Geräts vertrauen, verwenden oftmals die Löschfunktionen ihrer Security-Apps. Diese Löschfunktionen versprechen

- das sichere Löschen des kompletten internen Speichers,
- das Löschen der Speicherkarte oder auch
- das gezielte Löschen vertraulicher Informationen, wie zum Beispiel der heruntergeladenen Online-Kontoauszüge.

Wie die Untersuchung aus Cambridge ergab, arbeiten aber auch viele Löschfunktionen für Android-Smartphones unzuverlässig. Selbst nach Ausführung bestimmter Lösch-Programme für Android-Smartphones oder der Löschfunktionen einiger mobiler Sicherheits-Apps konnten die Forscher noch zahlreiche Daten auf den gebrauchten Smartphones nachweisen.

Aktuelle Android-Versionen oder professionelle Lösch-Apps

Erst Smartphones mit einer Android-Version ab 4.4 oder 5.0 zeigten die Löschergebnisse beim Zurücksetzen, die ein Nutzer von der entsprechenden Funktion auch erwarten würde. Welche Lösch-Apps im Test nur unvollständige Ergebnisse erzielten, können interessierte Leserinnen und Leser in der Studie aus Cambridge erfahren (*http://t1p.de/studie-cambridge*). Generell lässt sich sagen, dass professionelle Lösch-Apps, die nur eine Löschfunktion anbieten, eher einen Löscherfolg versprechen als Antivirus-Apps, die Löschen als eine Funktion von vielen aufweisen.

Die Lösung: ein neues Gerät?

Da viele Android-Smartphones keine Möglichkeit bieten, auf die aktuelle Android-Version zu wechseln, könnte man geneigt sein, sein altes Smartphone aufzugeben und auf ein neueres Modell zu wechseln, da es dann besser mit dem Löschen und Zurücksetzen klappt. Aber Vorsicht: Denken Sie daran, dass Ihr altes Gerät trotzdem vorher wirklich sauber gelöscht werden muss!

Löschen Sie die Daten auf Ihrem Android-Smartphone richtig? Testen Sie sich!

Frage: Mit dem Zurücksetzen des Smartphones sind alle Daten gelöscht. Die Weitergabe oder Entsorgung ist dann problemlos möglich. Stimmt das?

a) Ja, denn dann ist mein Android-Smartphone auf dem Anfangszustand.
b) Nein, Forscher haben gezeigt, dass Android-Smartphones bis zur Android-Version 4.3 zusätzlich mit professionellen Lösch-Apps bearbeitet werden müssen.

Lösung: Die Antwort b) ist richtig. Erst ab Android-Version 4.4 oder 5.0 arbeitet das Zurücksetzen als ein vollständiges Löschen der Daten. Ältere Android-Smartphones werden beim Zurücksetzen nicht komplett von Bestandsdaten befreit.

Frage: Ihre Security-App hat eine integrierte Löschfunktion. Können Sie sie zum Löschen vertraulicher Daten auf Ihrem Smartphone nutzen?

a) Eine Untersuchung aus Cambridge ergab, dass viele Security-Apps nur unvollständig löschen können.
b) Natürlich, eine Security-App löscht sicher, darauf ist Verlass.

Lösung: Die Antwort a) ist richtig. Leider kann nicht jede Security-App auch wirklich zuverlässig löschen. Je nach Hersteller gab es im Test Probleme mit dem Löschen von Media-Dateien wie etwa Fotos, gespeicherten Passwörtern, dem Verlauf im mobilen Browser, den WLAN-Daten, dem Browser-Cache und den eigenen Dateien des Nutzers, um einige Beispiele zu nennen. In der Regel sollten also spezielle Löschprogramme genutzt werden, die sich in unabhängigen Sicherheitstests bewährt haben.