

Datenschutz Now!

11

Die Informationsschrift zum Datenschutz



Liebe Leserin, lieber Leser,

mehr als 700 Millionen Menschen nutzen das soziale Netzwerk Facebook. Selbst wenn Sie nicht dazu gehören, könnte Facebook Sie kennen, vielleicht sogar Ihr Gesicht. Lesen Sie deshalb in dieser Ausgabe, wie Sie sich vor der Gesichtserkennung bei Facebook schützen können.

Sie glauben, Sie wären für Datendiebe uninteressant? Irrtum! Auch mit Ihren Daten könnten Kriminelle Geld verdienen. Beispiele für Schwarzmarkt-Preise finden Sie im zweiten Beitrag dieser Ausgabe.

Das liebe Geld treibt auch viele Unternehmen und Nutzer dazu, Computerdienste aus dem Internet zu beziehen. Doch dieses Cloud Computing hat einige Fallstricke auf Lager, die Sie kennen sollten. Dazu gehört auch das Risiko, dass die Daten, die Sie im Internet bei einem Dienstleister speichern, plötzlich verschwunden sein könnten. Backups lösen sich dann auf wie eine Wolke.

Für Rückfragen stehe ich Ihnen gerne zur Verfügung! **Ihr Gilbert Staffler, Datenschutzbeauftragter**

"Foto-Tagging" bei Facebook: Service oder Belästigung?

Seit wenigen Wochen und ohne es vorher besonders anzukündigen, hat Facebook die Funktion "Markieren von Fotos" in Deutschland generell für alle Nutzer aktiviert. Erfahren Sie, was daran problematisch ist und wie Sie das Markieren von Fotos verhindern können.

Ein "Geschenk" für 20 Millionen Nutzer

Während Sie diesen Artikel lesen, hat die Zahl der Facebook-Nutzer in Deutschland wahrscheinlich gerade die 20-Millionen-Grenze überschritten. Wenn Facebook also automatisch eine neue Funktion einführt, betrifft das etwa ein Viertel der Bevölkerung in Deutschland direkt.

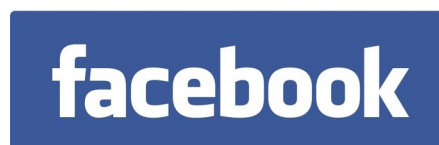
So geht es los

Damit Sie auf neu hochgeladenen Fotos markiert werden können, muss bei Facebook mindestens ein Foto vorhanden sein, auf dem Sie bereits markiert sind. Wird nun - egal von wem - ein neues Foto hochgeladen, vergleicht die Gesichtserkennungs-Software das vorhandene Foto mit dem neuen. Wenn die Software meint, auf dem neuen Foto Ihr Gesicht wiederzuerkennen, das auf dem anderen Foto bereits markiert ist, dann schlägt es vor, auch das neue Foto entsprechend zu markieren.

Sie erhalten eine Nachricht

Verfährt einer Ihrer Freunde nach diesem Vorschlag, und er markiert Sie auf dem neuen

Foto, werden Sie davon benachrichtigt. Sie können dann - wenn Sie dies wollen - die Markierung entfernen. Sollten Sie das neue Foto selbst hochgeladen haben, erhalten Sie natürlich keine Nachricht.



Der neue Foto-Tagging-Dienst von Facebook soll automatisiert Personen erkennen und Namen zuordnen (Bildquelle: facebook.com)

Was soll daran schlimm sein?

Das Ganze wirkt auf den ersten Blick ausgesprochen harmlos. Doch Vorsicht! Angenommen, Sie besuchen eine große Veranstaltung, und dort entstehen Bilder, die jemand bei Facebook einstellt. Auf jedem dieser Bilder sind Hunderte von Personen, darunter auch Sie.

Die Veröffentlichung solcher Bilder, sei es in der Zeitung oder auch im Internet, ist rechtlich ausdrücklich zulässig. Dahinter steht der Ge-

danke, dass Personen, die "Teil einer Menge" sind, in der Regel nicht erkannt werden können. Diese Überlegung ist natürlich hinfällig, wenn die Bilderkennungs-Software für 50, 100 oder auch 150 Personen, die auf einem Bild zu sehen sind, die Markierung mit dem jeweiligen Namen vorschlägt.

Die Technik schreitet rasant fort

Im Augenblick ist es noch so, dass ein recht hoher Prozentsatz solcher Vorschläge nicht stimmt oder sogar unsinnig ist, wenn etwa einer Frau der Name eines Mannes zugeordnet wird. Man sollte sich jedoch nicht täuschen: Die Software wird immer besser, und schon in wenigen Jahren werden solche Fehler die Ausnahme sein. Dann ist es mit der "Anonymität im öffentlichen Raum" vorbei.

Sie müssen selbst aktiv werden

Falls Sie nicht wollen, dass Fotos von Ihnen markiert werden, müssen Sie aktiv werden:

1. Gehen Sie bei Facebook auf das Feld "Konto".
2. Dann auf das Feld "Privatsphäre".
3. Dort auf "Benutzerdefinierte Einstellungen".
4. Im Abschnitt "Dinge, die andere Personen teilen" bei "Freunden Fotos von mir vorschlagen" das Feld "Gespart" anklicken.
5. Schließen Sie den Vorgang ab, indem Sie auf "OK" klicken.

So viel sind Ihre Daten wert

Nicht nur Spitzenpolitiker und Manager großer Konzerne stehen im Fokus der Datendiebe. Auch Ihre personenbezogenen Daten wecken Begehrlichkeiten bei Internetkriminellen. Auf dem Schwarzmarkt wird dafür bares Geld geboten.

Was wollen die mit meinen Daten?

So mancher Internetnutzer glaubt, uninteressant für Datendiebe zu sein. Denn was kann man schon mit den Daten einer Sachbearbeiterin oder eines Assistenten anfangen? Kaum jemand wird sich die Mühe machen, Daten von Personen zu beschaffen, die weder reich sind noch weit oben in der Hierarchie eines Unternehmens stehen.

Doch weit gefehlt! Wenn Sie bisher glaubten, Sie würden nicht zur Zielgruppe für Hackerangriffe und Passwortdiebstahl gehören, sollten Sie sich umgehend an neue Realitäten gewöhnen.

Jeder kann ein Opfer von Datendieben werden

Hacker und Passwortdiebe gehen zwar in den letzten Monaten immer gezielter vor bei ihren Angriffen. Dabei suchen sie aber ihre Opfer nach anderen Kriterien aus, als viele meinen.

Zum einen werden die Benutzerkonten und Computer der Assistenten und Sachbearbeiter sogar vermehrt attackiert, weil sie oftmals weniger stark abgesichert sind, dafür aber einen Zugang ins Netzwerk bieten, der Stück für Stück an die vertraulichen Daten und an die Zugänge der Manager und Administratoren im Unternehmen heranführt. Dazu nutzen die Datendiebe einfach den gekaperten Zugang und damit die Identität des ersten Opfers, um einfacher an die weiteren Opfer im Unternehmen zu gelangen.

Europol warnt vor wachsender Schattenwirtschaft im Internet

Zum anderen warnt die europäische Polizeibehörde Europol vor einer weiteren Professionalisierung bei den Internetverbrechern. Im weltweiten Netz findet inzwischen ein organisierter Datenhandel statt, der so lohnend ist, dass sich immer mehr Straftaten ins Internet verlagern.

Bis zu 60 Euro für Kreditkartendaten

Internetkriminelle können leicht und in kurzer Zeit viel Geld verdienen, wenn sie gestohlene Daten auf dem Schwarzmarkt anbieten.

Sicherheitsexperten haben bereits Vertriebswege im Internet entdeckt, über die gestohlene Daten gehandelt werden.

Bei einer Undercover-Aktion gaben sich zum Beispiel Mitarbeiter des Sicherheitsanbieters Panda Security als potenzielle Käufer gestohlener Daten aus. Das Ergebnis dieser Recherche auf dem Schwarzmarkt ist erschreckend: So werden gestohlene Kreditkartendaten für bis zu 60 Euro gehandelt, die geraubte Kreditkarte selbst kostet extra und bringt den Kriminellen sogar 130 Euro ein.

Abgefangene und manipulierte Banküberweisungen werden für 10 bis 40 Prozent des überwiesenen Betrags angeboten. Europol berichtet von 12 Euro je gestohlenem E-Mail-Zugang.



Personenbezogene Daten sind für Internetkriminelle viel wert!

Garantieleistungen für Internetgangster

Datendiebe offerieren gestohlene Zugangsdaten für Online-Banking auf dem Schwarzmarkt auch schon für etwas mehr als einen Euro. Wenn der kriminelle Kunde jedoch zum Beispiel ein garantiertes Guthaben von 56.000 Euro auf dem gestohlenen Online-Konto haben möchte, muss er dem Datendieb dafür knapp 500 Euro bezahlen.

Dabei sind die Angebote auf dem Schwarzmarkt bereits so professionell, dass die Datendiebe Online-Shops mit aktuellen Sonderangeboten, Mengenrabatt und Auftragsarbeiten betreiben. Es gibt sogar Möglichkeiten für Umtausch und Reklamation, wenn sich die Daten wider Erwarten nicht verwerten lassen. Personenbezogene Daten gibt es auf dem Schwarzmarkt auch als Paket. So konnte der Sicherheitsanbieter G Data ermitteln, dass ein

Datensatz bestehend aus einem Passwort für den Online-Bezahldienst PayPal, einem eBay-Passwort und einer E-Mail-Adresse für 10 Euro angeboten wird. Die Kombination aus PayPal-Passwort, Bankverbindung und E-Mail-Adresse kostet dagegen nur 4 Euro.

Datendiebe machen ein großes Geschäft

Wenn Sie sich nun vergegenwärtigen, dass Internet-Kriminelle oftmals Hunderte oder Tausende von Daten in kurzer Zeit erbeuten, werden Sie schnell erkennen, wie lukrativ dieses Geschäft ist. Deshalb investieren Datendiebe sogar.

Malware kaufen, Daten verkaufen

Ein Datendieb entwickelt inzwischen keine eigenen Schadprogramme mehr und betreibt auch kein eigenes Netzwerk aus gekaperten Computern. Vielmehr kauft er Trojaner ein und mietet bössartige Netzwerke für seine Angriffe.

Der Sicherheitsanbieter Kaspersky ermittelte, dass die Installation von Schadprogrammen auf 1.000 Rechnern in den USA für rund 80 Euro angeboten wird. Ein kriminelles Netzwerk, das jede Minute 1.000 Spam-Mails verschicken kann, kostet einen Datendieb zwar rund 1.400 Euro im Monat. Dafür hat er jedoch zahllose Chancen auf reiche Daten-Ernte.

Solange Internetnutzer immer noch glauben, nicht gefährdet zu sein und sich nicht ausreichend gegen Datendiebstahl schützen zu müssen, wird das Geschäft der Passwortdiebe aufgehen.

Machen Sie sich deshalb klar: Alle personenbezogenen Daten, auch Ihre eigenen, sind für Datendiebe ein lohnendes Ziel. Ohne ausreichenden Datenschutz sind Ihre Daten leichte Beute. Sie müssen kein Unternehmen leiten, um Opfer einer Hackerattacke zu werden. Passen Sie deshalb gut auf Ihre Daten auf!

Impressum

Redaktion:
Gilbert Staffler
Datenschutzbeauftragter

Anschrift:
EHS-Datentechnik
Uhlendahlweg 24
45279 Essen
Telefon: 0201-530091
E-Mail: info@ehs-datentechnik.de

Cloud Computing - eine nebulöse Sache?

Sie haben davon gehört, dass Cloud Computing sich immer mehr ausbreitet? Gleichzeitig aber auch davon, dass es vom Datenschutz her sehr problematisch sein soll? Dennoch wollen Sie es privat oder beruflich nutzen? Lesen Sie hier in aller Kürze, wo echte Probleme liegen und wo nicht.

**Der häufigste Anlass für Cloud Computing:
Die Nutzung von Software**

Jeder kennt die Situation: Für dieses eine Projekt bräuchte man wenige Tage lang eine bestimmte Software, beispielsweise eine Zeichensoftware. Sie ist sündhaft teuer, man will aber nur einige wenige Funktionen nutzen. Was tun?

Natürlich hat dann niemand Lust, diese Software zu kaufen. Der Ausweg: Man geht gegen Zahlung eines geringen Betrags auf einen externen Rechner, auf dem diese Software zur Miete angeboten wird.

Selbst wenn man den Begriff "Cloud Computing" bisher gar nicht gekannt hat, in diesem Augenblick hat man eine Variante des Cloud Computing genutzt, die als "Software as a Service" bezeichnet wird.

Die Private Cloud ist rechtlich meist unproblematisch

Rechtlich in der Regel unproblematisch ist das Ganze, wenn es sich innerhalb eines einzigen Unternehmens abspielt, beispielsweise zwischen verschiedenen Abteilungen. Der Grund: Das gesamte Netz, über das die verschiedenen Rechner zusammengebunden sind, steht unter einer einheitlichen rechtlichen Verantwortung, nämlich der Verantwortung dieses einen Unternehmens.

"Privat" wird eine solche Cloud deshalb genannt, weil kein Außenstehender daran beteiligt ist. Der Begriff bedeutet also nicht, dass hier irgendetwas von Privatpersonen betrieben werden müsste. Er grenzt lediglich danach ab, ob Außenstehende beteiligt sind oder nicht.

Schwieriger wird es bei der Public Cloud

Deutlich mehr rechtliche Überlegungen sind anzustellen, wenn es sich um eine öffentliche Cloud handelt. Allerdings muss man auch hier zunächst genau nachfragen, was damit gemeint ist.

"Öffentlich" kann tatsächlich bedeuten, dass jeder, der es will, eine bestimmte Software



Je mehr Seiten beim Cloud Computing beteiligt sind, desto komplizierter wird es

nutzen kann. Das wäre etwa der Fall, wenn ein Unternehmen eine Bildbearbeitungssoftware für jeden kostenlos zur Verfügung stellt, der sie nutzen möchte. Häufiger ist damit jedoch gemeint, dass jemand gegen Bezahlung eine Software nutzt, die in der rechtlichen Verantwortung eines anderen steht.

Sie kommt auch in Konzernen vor

Das gilt auch zwischen Unternehmen, die demselben Konzern angehören. Wenn also beispielsweise ein Konzernunternehmen die Lohnabrechnungssoftware eines anderen Konzernunternehmens nutzt, kann man das als eine Variante des Cloud Computing ansehen.

Es kann zunächst völlig offen sein, wer die Software stellt

Häufig verpflichtet sich ein Dienstleister lediglich dazu, eine bestimmte Software bei Bedarf zur Verfügung zu stellen. Er legt sich aber nicht fest, ob er diese Software selbst vorhält oder sie irgendwo zur Nutzung anmietet. Bei welchem Dienstleister er sie intern anmietet, wird dabei erst entschieden, wenn sie tatsächlich gebraucht wird.

Manche Beobachter der Szene sagen, dass lediglich diese Variante "wirkliches" Cloud Computing sei. Wie auch immer: An dieser Variante lassen sich die rechtlichen Probleme besonders deutlich zeigen.

Die rechtliche Verantwortung muss aber klar bleiben

Wer mit personenbezogenen Daten anderer Personen umgeht, muss zunächst einmal stets wissen, wo sich diese Daten befinden. Damit wäre es nicht zu vereinbaren, wenn sie irgendwo in einer Wolke verschwinden und dann irgendwann wieder auftauchen - oder auch nicht!

Schon daraus wird deutlich, dass sich kein Verantwortlicher auf Geschäftsmodelle einlassen kann, bei denen sich nicht jederzeit feststellen lässt, wo die personenbezogenen Daten hingeraten sind. Jeder Verantwortliche muss zu jeder Zeit wissen, wo sich die Daten befinden, die er verarbeiten lässt.

Die Einzelheiten der Verarbeitung müssen genau festgelegt sein

Die rechtliche Verantwortung geht jedoch weiter. Wer mit personenbezogenen Daten umgeht oder andere mit personenbezogenen Daten umgehen lässt, muss genau festlegen, wie dabei verfahren werden soll. Das gilt auch für die Frage, zu welchem Zeitpunkt vorhandene Daten gelöscht werden sollen.

Das rechtliche Stichwort lautet "Auftragsdatenverarbeitung"

Meist löst man dies über Verträge nach dem Modell der "Auftragsdatenverarbeitung". In ihnen ist unter anderem festgelegt, was genau mit den Daten geschehen soll, die verarbeitet werden.



Ein Vertrag zur Auftragsdatenverarbeitung muss viele Punkte ganz genau regeln

Beispiel: Es wird vereinbart, dass auf der Basis bestimmter Ausgangsdaten von Arbeitnehmern unter Anwendung eines bestimmten Tarifvertrags die Löhne berechnet werden. Weiteres Beispiel: Der Auftragnehmer verpflichtet sich, die Daten, die ihm zur Verfügung gestellt wurden, zwei Wochen nach Abschluss des Auftrags zu löschen.

Entsprechende Vertragsmuster stellen Verbände oft sogar kostenlos zur Verfügung. Nutzen Sie sie.

Wo ist mein Backup?

Mit wenigen Klicks kann man seine Daten über das Internet bei einem Dienstleister sichern. Die Daten landen dann irgendwo im Internet, in einer sogenannten IT-Wolke oder Cloud. Ob man sie von dort auch eines Tages wiederbekommt, ist jedoch nicht sicher. Erste Cloud-Dienste sind bereits ausgefallen.

Wenn das Backup verloren geht

Eigentlich legt man eine Datensicherung an, um im Fall eines Datenverlustes zeitnah wieder an seine Daten zu kommen. Besonders ärgerlich ist es deshalb, wenn das Backup selbst verloren geht, wo es doch als Sicherung gedacht ist. Das kann schneller passieren, als man gemeinhin glaubt.

Geht der USB-Stick verloren, sind die Urlaubsfotos weg

Stellen Sie sich vor, Sie haben von Ihrem Sommerurlaub tolle Fotos gemacht und sie zur Sicherheit auf einen USB-Stick überspielt. Die Speicherkarte der Digitalkamera quillt über, sodass Sie dort die Bilder löschen. Kein Problem, denn die Fotos sind ja noch auf dem USB-Stick. Was aber, wenn der USB-Stick aus der Tasche rutscht und verloren geht?

Flexibel und sicher durch Backup im Internet?

Da scheint es doch viel sinnvoller, seine Bilder in einem der Fotodienste im Internet zu sichern. Da kann nichts aus der Tasche rutschen und verloren gehen. Die Bilddaten werden bei einem Dienstleister gespeichert, irgendwo im Internet. Den Zugriff auf die Bilder schränkt man dann so ein, dass kein Fremder die Bilder sehen darf. Ob man die Bilder jedoch selbst jemals wieder zu Gesicht bekommt, ist leider nicht sicher.

Backup in den Wolken verschwunden

Systemausfälle wie der von Amazon Web Services im April 2011 zeigen deutlich, dass Daten, die nur im Internet gesichert werden, plötzlich weg sein könnten. Wenn der Dienstleister, der für das Backup in der Cloud gewählt wird, selbst eine unzureichende Datensicherung vornimmt, hat sich das Risiko des Datenverlusts nur verlagert und nicht etwa wie eine Wolke aufgelöst.

Backup im Internet nur als Ergänzung

Wenn Sie also zum Beispiel Ihre Urlaubsfotos schnell und einfach im Internet sichern wollen, sollten Sie zusätzlich noch eine lokale Daten-

sicherung anlegen. Da man nie wissen kann, wer im Internet auf das Backup alles zugreifen könnte, sollten Sie zudem alle Ihre vertraulichen Daten verschlüsseln, bevor Sie sie in eine Cloud übertragen.

Bitte keine eigenmächtigen Backups

Die Datensicherung ist natürlich nicht nur bei privaten Daten wie den Urlaubsfotos wichtig. Auch die Daten, die Sie für Ihren Arbeitgeber bearbeiten, dürfen nicht verloren gehen. Nutzen Sie dabei aber immer nur die Backup-Verfahren, die in Ihrem Unternehmen erlaubt

und vorgesehen sind. Wenn Backups im Internet nicht erlaubt sind, machen Sie auch keine, auch nicht zusätzlich zu einem lokalen Backup.

Besonderer Schutz für besonders vertrauliche Daten

Vergessen Sie auch nicht, die Ihnen übergebenen Daten so zu behandeln, wie es die Vertraulichkeit jeweils erfordert. So gibt es Daten, deren Verlust sehr ärgerlich wäre, denn es war viel Arbeit, sie zu erstellen. Aber es gibt auch Daten, deren Verlust den Bestand eines Unternehmens oder die berufliche Zukunft eines Menschen gefährden kann.

Deshalb rät das Bundesamt für Sicherheit in der Informationstechnik (BSI), besonders sensible Daten lieber nicht in einer öffentlich zugänglichen Cloud zu sichern, um das Risiko unbefugter Zugriffe auf die Daten so gering wie möglich zu halten.

Test: Haben Sie einen klaren Blick auf die IT-Wolke?

Frage: Sie haben einen wichtigen Kunden besucht und dort auf Ihrem Notebook einen Besuchsbericht erstellt. Dieser Bericht könnte verloren gehen, wenn das Notebook auf der Rückreise abhandenkommt. Speichern Sie den Besuchsbericht zur Vorsicht im Internet?

- a) Nein, ich mache nur eine lokale Sicherung auf einem verschlüsselten USB-Speicherstift.
- b) Wenn mein Arbeitgeber Datensicherungen im Internet erlaubt, speichere ich den Besuchsbericht verschlüsselt auf dem USB-Stick und im Internet, sicher ist sicher.
- c) USB-Sticks gehen leicht verloren. Deshalb speichere ich meine Daten immer nur im Internet.

Lösung: Antwort b) ist richtig, wenn Ihr Arbeitgeber Backups im Internet erlaubt hat. Sind Backups in der Cloud verboten, dann gilt die Antwort a).

Frage: Wer seine Daten bei einem großen, bekannten Online-Dienst speichert, braucht sich um sein Backup keine Gedanken mehr zu machen. Stimmen Sie dem zu?

- a) Leider nein, auch bei bekannten Online-Diensten sind Daten abhandengekommen.
- b) Natürlich, man muss nur den richtigen Anbieter nutzen, dann klappt es auch mit dem Backup.

Lösung: Antwort a) ist richtig. Auch wer seine Daten bei einem Dienstleister im Internet speichert, bleibt für sie verantwortlich. Deshalb sollte zusätzlich noch ein eigenes, lokales Backup gemacht werden.

Frage: Wenn man seine Daten verschlüsselt, ist man auf der sicheren Seite. Geht das Backup auf dem USB-Stick verloren, besteht für die Daten kein Risiko, oder etwa doch?

- a) Das A und O ist die Verschlüsselung, denn unehrliche Finder des USB-Sticks können dann die Daten nicht lesen.
- b) Die Verschlüsselung allein reicht nicht. Ohne ein sicheres Backup sind die Daten verloren, wenn der USB-Stick weg ist.

Lösung: Antwort b) ist richtig. Eine Verschlüsselung kann vor einem Datenverlust nicht schützen, wenn es kein Backup gibt.