Newsletter Datenschutz
Ausgabe 12 | 2013

agentia wirtschaftsdienst

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

unverschlüsselte E-Mails sind für Datendiebe wie ein offenes Buch. Wenn Sie E-Mails bislang nicht verschlüsselt haben, weil es Ihnen zu kompliziert erschien, sollten Sie sich den Tipp zur E-Mail-Verschlüsselung in dieser Ausgabe nicht entgehen lassen. Ebenso erfahren Sie, wie lange ein Arzt Behandlungsunterlagen aufbewahren muss und was vom Einsatz privater Videokameras im Straßenverkehr zu halten ist.

Doch nicht nur Videokameras können zu tiefe Einblicke in Ihre Privatsphäre ermöglichen: Neue Analyse-Tools entlocken sozialen Netzwerken wie Facebook Informationen über Sie, die Sie eigentlich nie dort veröffentlicht haben. Erfahren Sie, wie Sie sich deshalb verhalten sollten. Den Abschluss dieser Ausgabe bildet ein Wissenstest zu der so häufig vernachlässigten Verschlüsselung von E-Mails.

Wir wünschen Ihnen viele neue Einsichten!

Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

E-Mail-Verschlüsselung leicht gemacht

Die aktuellen Meldungen über die Überwachung des Internets sind ein deutlicher Warnruf, endlich seine E-Mails zu verschlüsseln. Gehen Sie daher das (vermeintliche) Problem der E-Mail-Verschlüsselung zügig an!

Geheimes per Postkarte?

Würden Sie eine ganz persönliche Nachricht als Postkarte senden, die auch andere Personen aus dem Briefkasten holen könnten? Sicherlich nicht. Bei E-Mails aber scheint jede Vorsicht vergessen zu sein. Hier werden vertrauliche Informationen verschickt, ohne daran zu denken, dass Dritte E-Mails letztlich genauso lesen können wie eine Postkarte.

Verschlüsselte E-Mails sind die Ausnahme

Eine andere Frage: Haben Sie schon privat oder beruflich eine verschlüsselte E-Mail bekommen, also eine E-Mail, die Sie zum Beispiel nur nach Eingabe eines Passworts lesen konnten? Wahrscheinlich nicht oder nur sehr selten. Laut einer BITKOM-Umfrage verwenden nur sechs Prozent der Internetanwender eine Verschlüsselungslösung für E-Mails.

E-Mails mit personenbezogenen Daten brauchen Schutz

Wenn Sie sich überlegen, was heute alles per E-Mail oder E-Mail-Anhang verschickt wird, ist schnell klar, dass eigentlich ein hoher Schutzbedarf besteht: Schließlich sind oftmals Kundendaten, vertrauliche Geschäftsinformationen oder sehr Persönliches enthalten.

Verschlüsselung gilt als kompliziert

Wenn Sie Ihre vertraulichen E-Mails bisher nicht verschlüsseln, denken Sie wahrscheinlich, Verschlüsselung sei schwierig und aufwendig. Vielleicht wissen Sie auch nicht, wie sich E-Mails verschlüsseln lassen. Die gute Nachricht: Verschlüsselung muss nicht kompliziert sein. Sie brauchen noch nicht einmal zusätzliche Software auf Ihrem Computer.

E-Mails zu verschlüsseln, ist einfacher, als viele denken (Bild: Thinkstock)

Verschlüsselung ist eigentlich einfach

Wenn Sie zum Beispiel als E-Mail-Client Mozilla Thunderbird verwenden, würde Ihnen ein E-Mail-Zertifikat reichen, das Sie nur einmal für sich und Ihre Kontakte in Ihr E-Mail-Programm laden müssen. Für Privatanwender sind solche Zertifikate, die von Trustcentern ausgegeben werden, häufig kostenlos. Allerdings ist die Option zur Einrichtung der Zertifikate gut versteckt, unter dem Menüpunkt Einstellungen - Erweitert - Zertifikate. Danach können Sie beim Erstellen einer E-Mail die Funktion "S/MIME" zur Verschlüsselung wählen. Doch es geht auch einfacher.

Tipp: Vertrauliches gehört in den Anhang

Statt die E-Mail selbst zu verschlüsseln, können Sie Ihre vertraulichen Informationen in eine Datei packen, zum Beispiel in eine Office-Datei, und dann diese verschlüsseln. Sie verschicken die E-Mail dann mit verschlüsseltem Dateianhang. Die Verschlüsselung und die Entschlüsselung klappen ganz einfach mit dem Textverarbeitungsprogramm oder bei komprimierten Dateien mit Ihrem ZIP-Programm. Bei MS Word finden Sie die Verschlüsselungsfunktion unter Datei - Informationen - Dokument schützen - Mit Kennwort verschlüsseln. Der Empfänger braucht das von Ihnen gewählte starke Kennwort, das Sie natürlich NICHT in die E-Mail schreiben, sondern zum Beispiel per Telefon mitteilen. Und schon ist Ihre Nachricht verschlüsselt.

Wie lange bewahrt mein Arzt eigentlich Behandlungsunterlagen auf?

Die meisten ärztlichen Behandlungen sind ebenso kurz wie erfolgreich. So haben Sie es selbst immer erlebt? Glückwunsch! Dann werden Sie sich auch kaum für die Behandlungsunterlagen interessieren. Wenn bei einer Behandlung allerdings einmal Fehler vorgekommen sein könnten, wird die Frage plötzlich bedeutsam: Welche Behandlungsunterlagen muss ein Arzt oder ein Krankenhaus eigentlich aufbewahren und wie lange?

Das BGB enthält neue Regelungen

So wichtig die Fragen sind - gesetzlich geregelt waren sie bisher nicht. Nur die Berufsordnung der Ärztekammer enthielten einige generelle Aussagen dazu, was in Behandlungsunterlagen stehen muss und wie lange diese Unterlagen aufzubewahren sind. Das hat sich seit Februar 2013 gründlich geändert. Seither geben neue Regelungen im Bürgerlichen Gesetzbuch (BGB) wichtige Antworten, die jeder Patient kennen sollte.

Inhalt der Patientenakte genau festgelegt

Was eine Patientenakte enthalten muss, umschreibt das Gesetz allgemein wie folgt: "Alle wesentlichen Maßnahmen und deren Ergebnisse, wenn sie aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlich sind." (§ 630f Absatz 2 Satz 1 BGB). Als konkrete Beispiele dafür, worum geht, nennt das Gesetz:

- die Anamnese (also die gesundheitliche Vorgeschichte des Patienten)
- Diagnosen
- Untersuchungen
- Untersuchungsergebnisse
- Befunde
- Therapien und ihre Wirkungen
- Eingriffe und ihre Wirkungen

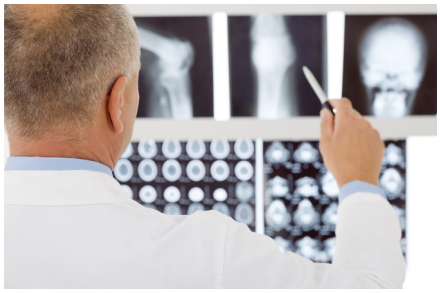
Überraschend wirkt das alles nicht. Auch dass Arztbriefe ausdrücklich in jedem Fall in die Patientenakte aufzunehmen sind, wirkt eher selbstverständlich. Bemerkenswerter erscheint es schon, dass "Einwilligungen und Aufklärungen" ebenfalls zwingend in die Patientenakte aufzunehmen sind.

Regelung bringt endlich Klarheit für alle

Insgesamt schafft die geschilderte Regelung Klarheit für alle Beteiligten. Der Arzt weiß, was in eine Patientenakte hinein muss, und der Patient erfährt, was er je nach Lage des Falls dort erwarten kann.

Elektronische Patientenakten sind ausdrücklich möglich

Der Begriff "Patientenakte" muss dabei nicht bedeuten, dass Papier verwendet wird. Vielmehr hebt § 630f Absatz 1 Satz 1 BGB ausdrücklich hervor, dass "eine Patientenakte in Papierform oder elektronisch" geführt werden kann. Damit ist nun eine ausdrückliche Rechtsgrundlage für die elektronische Patientendokumentation vorhanden. Das hatte die medizinische Praxis seit Langem gefordert.



Für Röntgenbilder gelten ganz unterschiedliche Aufbewahrungsfristen (Bild: Thinkstock/CandyBoxImages)

Die Mindestaufbewahrungsfrist beträgt stets zehn Jahre

Die Grundregel für die Aufbewahrungsdauer einer Patientenakte lautet: zehn Jahre nach Abschluss der Behandlung! So schreibt es der § 630f Absatz 3 BGB vor. Für den Patienten bedeutet dies: Er kann sich sicher sein, dass alle Behandlungsunterlagen, auch solche zu Behandlungen, die nur kurz gedauert haben, jedenfalls bis zehn Jahre nach Abschluss der Behandlung vorhanden sind.

Bagatellbehandlung heißt auch Bagatellakte!

Freilich: Sollte es um eine Bagatellbehandlung gehen, wird die zugehörige Patientenakte vom Umfang her sehr bescheiden sein. Möglicherweise besteht sie dann nur aus Notizen im Umfang von wenigen Zeilen. Auch ist keineswegs gesagt, dass der Patient selbst eine Behandlungsdokumentation verstehen kann. Sie ist - wie schon erwähnt - aus fachlicher Sicht zu führen und daher auch nur für einen Fachmann gedacht.

Für das Röntgen gelten Besonderheiten

Die Frist von zehn Jahren ist allerdings nur eine Mindestgrenze, keine Höchstgrenze für die Aufbewahrungsdauer. Das Gesetz verweist ausdrücklich darauf, dass "nach anderen Vorschriften andere Aufbewahrungsfristen bestehen" können, die möglicherweise länger sind. Praktisch bedeutsam sind insoweit die Regelungen der Röntgenverordnung. Sie legt in § 28 Folgendes fest:

1) Röntgenbilder müssen bei volljährigen Patienten zehn Jahre lang aufbewahrt werden.

2) Sollte der Patient dagegen minderjährig sein (noch nicht 18 Jahre alt), müssen Röntgenbilder bis zur Vollendung seines 28. Lebensjahrs aufbewahrt bleiben.

3) Für Unterlagen über Röntgenbehandlungen (also etwa Bestrahlungen zur Bekämpfung von Tumoren) besteht sogar eine Aufbewahrungspflicht von 30 Jahren. Dabei beginnt diese Frist erst mit Abschluss der letzten Behandlung zu laufen.

Eine generelle Frist von 30 Jahren gibt es nicht

Immer wieder wird behauptet, jedenfalls Unterlagen über Behandlungen in Krankenhäusern müssten generell 30 Jahre aufbewahrt werden. Eine ausdrückliche gesetzliche Grundlage hat diese Auffassung nicht. Gleichwohl verhalten sich viele Krankenhäuser so, weil die maximale Verjährungsfrist für Ansprüche bei fehlerhaften Behandlungen 30 Jahre beträgt (§ 199 Absatz 2 BGB). Auf diese Handhabung verlassen kann sich ein Patient jedoch nicht.

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 Facebook, Twitter & Co. über Sie verraten können

Ihre persönlichen Neigungen würden Sie nie in einem sozialen Netzwerk verraten? Brauchen Sie auch nicht. Neue Analysemöglichkeiten in sozialen Netzwerken gewähren auch so tiefe Einblicke in Ihre Person.

Online-Profile sind nicht alles

78 Prozent der Internetnutzer in Deutschland sind in einem sozialen Netzwerk angemeldet, zwei Drittel der Internetnutzer sind regelmäßig in sozialen Netzwerken aktiv, wie eine aktuelle Umfrage des BITKOM-Verbands ergab. Die Fülle an personenbezogenen Daten bei Facebook & Co. ist enorm. Bei manchem Nutzer kann man sich wirklich wundern, was alles im Internet landet.

Sicherlich sind Sie vorsichtiger bei den Angaben, die Sie in Ihrem Online-Profil machen. Die von Facebook erfragten Einstellungen zu Religion oder Politik gehen ja nicht jeden etwas an. Doch Sie müssen gar nicht ausdrücklich schreiben, was Sie denken.

Was Facebook-Likes über den Nutzer verraten können - Beispiele:

- Ob ein Nutzer Raucher ist oder nicht, ließ sich in 73 Prozent der untersuchten Fälle richtig aus "Gefällt mir"-Angaben ableiten.

- In 88 Prozent der Fälle konnte eine Homosexualität der Nutzer aus Facebook-Likes vorhergesagt werden.

- In ebenfalls 88 Prozent der Fälle ließen Facebook-Likes erkennen, ob ein Nutzer männlich oder weiblich ist.

- In 95 Prozent der Fälle konnten die Forscher die Hautfarbe eines Nutzers richtig vorhersagen.

- 85 Prozent der Berechnungen zur politischen Gesinnung der Nutzer war ebenfalls korrekt.

- Ein Drogenkonsum konnte in 75 Prozent der Fälle richtig abgeleitet werden.

"Gefällt mir" als Hinweisgeber

Ihre Vorlieben könnten sich auch zum Beispiel aus Ihren "Gefällt mir"-Angaben ableiten lassen, sogar die sexuelle Orientierung und die politische Gesinnung, wie ein wissenschaftliches Experiment zeigt.

So haben Wissenschaftler der Universität von Cambridge die "Gefällt mir"-Angaben (Facebook-Likes) von 58.000 Freiwilligen analysiert, um bestimmte Verbindungen zwischen den persönlichen Vorlieben und den Facebook-Reaktionen zu entdecken. Die Ergebnisse sind alarmierend (siehe Kasten).

Facebook-Analysen für jedermann

Nicht nur Wissenschaftler können Facebook & Co. als Informationsquelle nutzen. Im Internet gibt es zahlreiche Tools, die auf Knopfdruck Auswertungen auf Basis von Aktivitäten in sozialen Netzwerken liefern, so zum Beispiel Beevolve, Socialmention, Socialmetrix Echo, Talkwalker, oder Opinion Tracker.

Solche Tools sind nur die Spitze des Eisberges, was der Werbewirtschaft, aber auch Internetkriminellen an Analysemöglichkeiten für Informationen aus sozialen Netzwerken zur Verfügung stehen kann.

Automatische Kategorisierung Ihrer Inhalte

Soziale Netzwerke führen auch selbst umfangreiche Analysen durch. Denn sie bieten Werbeplätze an, die sich umso besser verkaufen lassen, je genauer die Zielgruppe mit der Werbung erreicht werden kann.

Bereits bei Erstellung einer Statusmeldung auf Facebook, Google+ oder Twitter werden Ihre Texte analysiert und nach Möglichkeit einer Kategorie zugeordnet. So können Dritte zum Beispiel auf einen Blick erkennen, zu welchen Themen Sie sich besonders häufig äußern. Daraus lassen sich dann durchaus Rückschlüsse auf bestimmte Einstellungen Ihrerseits ziehen.

Verknüpfung verschiedener Netzwerke

Facebook, Twitter & Co. können aber auch deshalb mehr über Sie verraten, als Sie selbst dort veröffentlichen, weil sich die sozialen Netzwerke in Analysen kombinieren lassen. Wenn Sie also in einem sozialen Netzwerk etwas über Ihre nächste Reise schreiben und in einem anderen etwas über Ihre beruflichen Aktivitäten, lassen sich diese Informationen verknüpfen. Dadurch könnte zum Beispiel eine Dienstreise, die eigentlich vertraulich sein sollte, erkennbar werden.

Vermeintlich harmlose Angaben können durch die Kombination verschiedener sozialer Netzwerke doch mehr verraten, als Ihnen lieb ist
(Bild: Thinkstock/Alexaldo)

Spezielle Suchmaschinen wie Spokeo gehen sogar so weit, dass sie zum Beispiel den in Facebook genannten Wohnort mit Immobilienanalysen verknüpfen, sodass Dritte sehen können, in was für einem Umfeld Sie denn wohnen.

Datensparsamkeit geht weiter als gedacht

Im Datenschutz lautet eine der wichtigsten Empfehlungen, nur die wirklich notwendigen personenbezogenen Angaben zu erfragen bzw. zu übermitteln. Wenn Sie also Ihr Online-Profil bei Facebook & Co. füllen, sollten Sie sparsam mit Ihren Daten umgehen.

Wie die neuen Analysemöglichkeiten für soziale Netzwerke aber zeigen, sollte Datensparsamkeit nicht nur auf die eigene Veröffentlichung von Daten bezogen werden. Auch aus Aktivitäten wie dem Anklicken von "Gefällt mir" bei Facebook oder +1 bei Google+ kann vieles über Sie abgeleitet werden, bis hin zu Ihrem Gesundheitszustand, der politischen Überzeugung, der religiösen Einstellung und sexuellen Vorlieben. Nicht ohne Grund werden diese Informationen im Datenschutz als besonders sensibel gewertet. Gehen Sie deshalb in sozialen Netzwerken besonders vorsichtig vor!

Private Videokameras im Straßenverkehr - zulässig oder nicht?

Bestimmt fürchten auch Sie diese Situation: Es kommt zu einem Autounfall, hoffentlich nur mit Blechschaden. Sie sind sich sicher, alles richtig gemacht zu haben. Aber: Neutrale Zeugen gibt es keine und der Unfallgegner stellt alles ganz anders dar! Da wünscht man sich manchmal eine Kamera hinter seiner Windschutzscheibe. Und solche Kameras gibt es tatsächlich. Aber was sagt der Datenschutz dazu?

Durch die Aufnahmen vom Meteoriteneinschlag in Russland wurden sie vor einigen Monaten allgemein bekannt, und jeder Elektronikhandel hat sie im Angebot: Dashboard-Kameras, also Kameras, die hinter der Windschutzscheibe installiert werden. Sie zeichnen jeweils einige Minuten lang Aufnahmen auf, die dann mit den nächsten Aufnahmen wieder überschrieben werden.

Radler installiert Kamera auf dem Fahrrad

Eine solche Kamera hatte ein Radler in München an seinem Fahrrad installiert. Als eines Tages ein Pkw-Fahrer vor ihm plötzlich abbremste, geriet der Radfahrer ins Straucheln und fiel hin. Den Schaden von insgesamt 3.000 Euro (Arztkosten und Reparatur des Fahrrads) wollte er vom Autofahrer wiederhaben.

Das Gericht lässt die Aufnahmen als Beweismittel zu

Als Beweismittel legte er vor Gericht Aufnahmen seiner Videokamera vor. Und tatsächlich: Das Gericht ließ diese Aufnahmen sogar als Beweismittel zu, da zum Zeitpunkt der Aufnahme mit den Aufzeichnungen noch kein bestimmter Zweck verfolgt werde. Andere Verkehrsbeteiligte müssten es akzeptieren, zufällig ins Bild zu geraten. Dies sei nichts anderes, als wenn jemand ein Gebäude fotografiere und dabei Personen zu sehen sind.

Den Radfahrer freute diese Argumentation natürlich. Endlich würde er zu seinem Recht kommen! Schon bald allerdings wird er eher an das Sprichwort gedacht haben: "Vor Gericht und auf hoher See bist du in Gottes Hand!"

Allerdings sprechen die Aufnahmen gegen den Radler

Denn leider zog das Gericht aus den Aufnahmen ganz andere Schlussfolgerungen, als er erwartet hatte. Es gelangte nämlich zu der Auffassung, dass sich aus den Aufnahmen deutlich erkennen lasse, dass er den Sicherheitsabstand zu dem Fahrzeug vor ihm nicht eingehalten habe. Deshalb sei er an dem Unfall selbst schuld. Er erhält damit keinen Cent!

Beschlagnahme von Aufnahmen denkbar

Somit zeigt dieses Beispiel vor allem, wie schnell bei Videoaufnahmen der Schuss nach hinten losgehen kann. Im Ernstfall kann es sogar noch viel dramatischer kommen, wenn etwa bei einem schweren Unfall die Staatsanwaltschaft die Aufnahmen beschlagnahmt und als Beweismittel im Strafprozess gegen den verwendet, der sie gemacht hat. Die andere Variante ist freilich auch möglich: Die Aufnahmen könnten die Unschuld beweisen.

In Österreich gilt: Finger weg von solchen Kameras!

Die österreichische Datenschutzkommission vertritt übrigens die Auffassung, dass jeder Betreiber einer Videokamera nur solche Bereiche überwachen dürfe, an denen ihm ein "hausrechtsähnliches Verfügungsrecht" zusteht. Das wäre etwa beim eigenen Haus der Fall. Bei einer öffentlichen Straße kann davon keine Rede sein. Daher lehnt die Datenschutzkommission den Einsatz solcher Kameras ab. Wer sie in Österreich dennoch verwendet, riskiert in Bußgeld von mehreren 1.000 Euro.

Verschlüsseln Sie Ihre E-Mails richtig? Testen Sie Ihr Wissen!

Frage: Sie versenden ab jetzt regelmäßig verschlüsselte Dateianhänge, wenn Sie vertrauliche Daten übermitteln wollen. Wie wählen Sie das Kennwort?

a) Ich beachte die internen Passwortrichtlinien, die auch hier gelten.
b) Ich wähle für jeden Empfänger ein anderes Passwort und nutze es dann regelmäßig.

Lösung: Die Antwort a) ist richtig. Sie sollten nicht nur für jeden Empfänger ein anderes Passwort nutzen, sondern dieses Passwort auch regelmäßig ändern. Sonst wird die Verschlüsselung unsicher, da das Kennwort beim Empfänger Dritten zugänglich sein könnte.

Frage: Sie nutzen eine Lösung zur E-Mail-Verschlüsselung. Ist dann auch die Betreffzeile verschlüsselt?

a) Nein, je nach Lösung sind nur der Nachrichtentext und der Anhang oder aber nur der Anhang verschlüsselt.
b) Natürlich, denn die ganze E-Mail ist verschlüsselt.

Lösung: Die Antwort a) ist auch hier richtig. Weder der Name des Empfängers noch die Betreffzeile werden bei der E-Mail-Verschlüsselung mitverschlüsselt. In die Betreffzeile gehören also keine geheimen Kurzbotschaften.

Frage: Sie erhalten eine verschlüsselte Nachricht von einem Empfänger, den Sie nicht kennen. Was tun Sie?

a) Ich folge der Anweisung in der E-Mail zur Entschlüsselung des Anhangs.
b) Es könnte ein Angriffsversuch dahinterstecken. Der verschlüsselte E-Mail-Anhang könnte verseucht sein.

Lösung: Die Antwort b) ist richtig. Datendiebe versenden auch angeblich verschlüsselte Nachrichten, die sich beim Anklicken eines Links oder beim Ausführen eines mitgeschickten Programms lesen lassen sollen. Dabei wird dann versucht, den Rechner des Opfers mit Malware zu verseuchen.