AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Dezember 2016 | Seite 1

www.aok-verlag.info/ds-im-blick

INHALT

Sicherer Umgang mit Passwörtern

Passwörter gehören zum täglichen Arbeitsleben dazu, dennoch werden sie von vielen als Hemmnis angesehen. Passwörter sind wesentliche Elemente bei der Zutritts-, Zugangs-, Zugriffs- und Eingabekontrolle. Je nach eingesetzten Fachverfahren und IT-Infrastruktur muss der Anwender mehrere Passwörter für die Erbringung seiner Arbeitsleistung beherrschen und regelmäßig ändern.

Dr. Sebastian Ertel

Warum Passwörter

Passwörter dienen zwei Zwecken: Einerseits der Geheimhaltung, indem sie einem allgemeinen Zugriff auf Geschäftsgeheimnisse des Unternehmens sowie auf personenbezogene Daten der Beschäftigten, Dienstleister, Kunden und Patienten entgegenwirken. Unbefugte Personen sollen durch den Einsatz von Passwörtern daran gehindert werden, auf diese Daten bzw. Informationen zuzugreifen und dadurch dem Unternehmen bzw. den Betroffenen zu schaden.

Andererseits dienen Passwörter, und das wird häufig verkannt, dem Selbstschutz des Anwenders eines Fachverfahrens. Unbefugte Personen werden durch den Passwortschutz gehindert, die im Fachverfahren hinterlegten Daten und Informationen zu manipulieren.

Derartige Manipulationen sind über das Benutzerprofil des Mitarbeiters diesem zuzuordnen. Je nach Umfang der Manipulation und deren Folgen kann der betroffene Beschäftigte hierfür arbeits-, zivil- und strafrechtlich zur Verantwortung gezogen werden.

Ein anschauliches Beispiel hierzu, das sich in ähnlicher Form in den USA ereignete:
In einem Unternehmen war ein Stellenabbau geplant. In einer Abteilung standen zwei Beschäftigte zur Auswahl, von einem sollte sich getrennt werden. Einer der beiden Betroffenen konnte die Zugangsdaten des anderen für das gemeinsam genutzte Fachverfahren in Erfahrung bringen. Er loggte sich mit diesen Zugangsdaten in das System ein und veränderte

verschiedene Datensätze. Die Manipulation wurde festgestellt und über die Log-Dateien der tatsächlichen Account-Inhaberin zugeschrieben, der daraufhin gekündigt wurde. In dem sich anschließenden Gerichtsverfahren konnte diese jedoch nachweisen, dass sie die Manipulation nicht begangen hatte: Sie befand sich zum Zeitpunkt der Datenveränderung auf einem Flug. Hierdurch konnte der Identitätsdiebstahl des anderen Kollegen aufgedeckt werden.

Ein solcher Nachweis, wie im dargestellten Beispiel, wird dem Betroffenen allerdings nicht immer gelingen.

Gruppen-Accounts

Aufgrund derselben Problematik ist der Einsatz von Gruppen-Accounts kritisch zu hinterfragen. Nutzt eine bestimmte Personengruppe für ein Fachverfahren einen einheitlichen Account, kann nicht ohne Weiteres nachgeprüft werden, welcher Beschäftigte die fehlerhafte Datenverarbeitung zu vertreten hat. Dies führt letztlich dazu, dass alle Nutzer des Gruppen-Accounts verdächtigt werden, sofern diese sich nicht auf Grund besonderer Umstände exkulpieren können. Eine Exkulpation wäre beispielsweise möglich, wenn ein Beschäftigter während des Zeitpunktes der schädigenden Handlung keinen Zugriff auf das Fachverfahren haben konnte (z. B. aufgrund einer Besprechung, Urlaub, Krankheit).

Ein weiteres Problem bei Gruppen-Accounts ergibt sich bei einer Veränderung der Nutzergruppe. Benötigt ein Nutzer den Account nicht mehr für die Erbringung seiner Arbeitsleistung oder scheidet aus dem Unternehmen aus, muss

das Passwort geändert werden, um dem Nutzer den Zugang zu den Fachverfahren bzw. den Zugriff auf die dort gespeicherten Daten tatsächlich zu entziehen.

Dies erfolgt wegen des damit verbundenen Aufwands (Benachrichtigung sämtlicher Account-Nutzer) in der Praxis kaum. Die Folge ist ein unüberschaubares Ausweiten der Zugangs- und Zugriffsrechte. Im Bereich des Patientendatenschutzes wäre wegen eines möglichen Verstoßes gegen die ärztliche Schweigepflicht sogar eine Strafbarkeit nach § 203 StGB denkbar.

Vertretbar sind Gruppen-Accounts allenfalls, wenn diese nur ein Durchgangsstadium zu den einzelnen Fachverfahren darstellen und in diesem Stadium keine Verarbeitung personenbezogener Daten möglich ist. Dies wäre beispielsweise der Fall bei Gruppen-Clients auf Betriebssystemebene, wenn der Client den Nutzern keine Rechte zuweist, die eine Verarbeitung personenbezogener Daten oder vertraulicher Informationen ermöglichen. Dem Client kommt einzig die Aufgabe zu, einen Zugang zum benötigten, seinerseits passwortgeschützten Fachverfahren zu ermöglichen.

Single Sign On

Beim Single Sign On (SSO) wird nur eine Benutzerkennung/Passwort-Kombination benötigt. Diese ermöglicht dem Anwender auf alle Applikationen Zugriff zu erhalten, für die ihm die entsprechenden Berechtigungen eingeräumt wurden. Weitere Aufforderungen zur Eingabe einer Identifikationskennung gibt es nicht.

Gelangt eine Zugangskennung zur Kenntnis eines Unberechtigten, hat dieser umfassenden Zugriff auf sämtliche Verfahren, für die auch der Account-Inhaber zugriffsberechtigt ist.
Daher muss das Passwort beim SSO besonders sorgfältig gewählt und geschützt werden.

Passwort-Standard

Welche Anforderungen an ein Passwort zu stellen sind, richtet sich nach den Parametern, die der Administrator des Fachverfahrens oder des Clients in der jeweiligen Passwortrichtlinie definiert hat. Dabei wird sich regelmäßig am IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientiert, der im Maßnahmenkatalog M 2.11 „Regelung des Passwortgebrauchs“ folgende Empfehlungen gibt:

- keine Passwörter mit persönlichem Bezug/Trivialpasswörter (z. B. Namen, Kfz-Kennzeichen, Geburtsdatum,12345678, AAAAAAA).
- Mindestens zwei der vier Zeichenarten Groß-, Kleinbuchstaben, Sonderzeichen, Zahlen sind zu verwenden.
- Mindestlänge: acht Zeichen bei alphanumerischen Passwörtern
- Das Passwort muss regelmäßig (alle 90 Tage) gewechselt werden.
- kein wiederholter Gebrauch alter Passwörter.
- Erfolglose Anmeldeversuche sollten mit einer kurzen Fehlermeldung ohne Angabe von näheren Einzelheiten abgelehnt werden.
- Nach fünf aufeinanderfolgenden fehlerhaften Passworteingaben für dieselbe Kennung sollte das Authentisierungssystem den Zugang für eine bestimmte Zeitspanne oder dauerhaft sperren.
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden.

Passwörter merken

Muss sich der Anwender mehrere Passwörter, komplexe Passwörter oder regelmäßig zu ändernde Passwörter merken, bedeutet dies für ihn regelmäßig eine große Herausforderung.

Häufig wird sich damit beholfen, dass die Passwörter in der Nähe des Computers dokumentiert werden. Häufig finden sich diese auf Post-it‘s auf der Unterseite der Tastatur oder des Schreibtisches. Oft wird das Passwort auch an einem geheimen Ort im Büro oder vor allem auf den Stationszimmern verwahrt, den regelmäßig andere Beschäftigte kennen.

Diese „Hilfen“ sind verständlich, bergen aber das erhebliche Risiko der unbefugten Benutzung und konterkarieren letztlich die Aufgabe des Passwortes.

Es gibt aber auch Möglichkeiten, sich komplexe Passwörter sicher zu merken:

Akronym-Methode

Bei der Akronym-Methode wählt man einen längeren Satz, in dem auch Ziffern vorkommen. Aus den Anfangsbuchstaben der Wörter, Ziffern und Sonderzeichen ergibt sich dann das Passwort. Der wesentliche Vorteil liegt darin, dass man sich lediglich den Satz merken muss. Das ist einfacher als das entsprechende Passwort.

Beispiel: Der Satz: „Ich muss mir schon wieder ein Passwort mit 8 Zeichen merken!“ ergibt das Passwort „ImmswePm8Zm!“

Satz-Methode

Alternativ kann man auch einen ganzen Satz (ohne Leerzeichen) als Passwort verwenden. Aus dem Satz „Mein Passwort muss 8 Zeichen haben!“ ergibt sich das Passwort: „MeinPasswortmuss8Zeichenhaben!“

Anonymität bei CIRS gewährleisten

Fast alle Krankenhäuser verfügen über ein Critical Incident Reporting System (CIRS), überwiegend in elektronischer Form. Das System dient der Meldung kritischer Ereignisse innerhalb der Einrichtung. Hieraus sollen Schlussfolgerungen gezogen und zukünftige, vergleichbare Ereignisse vermieden werden. Die Meldung wird über ein Formular der Qualitätsmanagement-Beauftragten bereitgestellt, die diese anonymisiert. Anschließend wird sie an das CIRS-Team weitergeleitet, damit dieses die erforderlichen Maßnahmen treffen kann.

Zum Teil umfassen die Meldungen auch das genaue Datum inkl. Uhrzeit und die Abteilung, in der das Ereignis stattfand. Während Letzteres für die Maßnahmenfindung regelmäßig relevant ist, ist auf die Weitergabe von Datum und Uhrzeit des Ereignisses zwingend zu verzichten. Durch diese Informationen kann mit Hilfe des Dienstplans der Kreis der möglichen beteiligten Beschäftigten so eingegrenzt werden, dass eine Anonymität nicht mehr gegeben ist.

Dies würde letztlich einem effektiven CIRS entgegenstehen.

Passwort-Karte

Eine dritte Möglichkeit bieten Passwort-Karten. Diese können von verschiedenen Anbietern im Internet gratis heruntergeladen werden, beispielsweise über http://www.saver-nova.com/de/sichere-passworter.

Die Passwortkarte ist wie ein Koordinatensystem aufgebaut, mit x- und y-Koordinaten. Der Nutzer muss sich lediglich die Startkoordinate merken und den Weg, den er auf dem Koordinatensystem zurücklegt (z. B. 2 Felder nach links, 2 Felder nach unten, 2 Felder nach links und 2 Felder nach oben). Aus den hierbei zurückgelegten Koordinaten ergibt sich dann das neunstellige Passwort (Startkoordinate und 8 Wegkoordinaten).

Selbst die Startkoordinate muss man sich nicht zwingend merken und kann diese sogar auf der Passwortkarte einzeichnen, da ohne die Wegkoordinaten eine Ermittlung des Passwortes unmöglich ist.

Die Passwortkarte muss nicht besonders aufbewahrt werden. Es ist auch möglich, diese am Monitor anzubringen. Unbefugte können aufgrund der fehlenden Zusatzinformationen aus dieser keine Rückschlüsse auf das Passwort ziehen. In diesem Fall sollte eine Kopie der Passwortkarte als „Backup“ vorgehalten werden, für den Fall, dass die Karte vom Monitor entfernt wird.

Passwortsafe

Eine weitere Möglichkeit bieten Passwortsafes. Hierbei handelt es sich um Programme oder Applikationen, mit denen sämtliche Passwörter verwahrt werden. Diese sind durch eine Verschlüsselung vor unbefugten Zugriffen geschützt. Für das Abrufen der Passwörter wird ein Masterpasswort benötigt, an welches hohe Komplexitätsanforderungen gestellt werden: Die Mindestlänge sollte 12 Zeichen betragen, empfohlen werden mehr als 20 Zeichen. Um sich diese zu merken, sollte auf eine der ersten drei Möglichkeiten zurückgegriffen werden.

Auch verlangt die Nutzung eines Passwortsafes vom Nutzer ein hohes Maß an Selbstdisziplin. Das Programm sollte nach der Verwendung unmittelbar wieder geschlossen werden. Darüber hinaus ist der Rechner, auch beim kurzzeitigen Verlassen, manuell zu sperren (Win-Taste + „L“-Taste), um Unbefugten jegliche Möglichkeit zu nehmen, auf die hinterlegten Passwörter zuzugreifen.

Vertiefungshinweis im Handbuch „Datenschutz im Gesundheitswesen“ (DSiGW):

- Datenschutz im Gesundheitswesen (AOK Verlag GmbH), Kapitel M 5.2.2 (Passwörter)

EuGH entscheidet zur Personenbeziehbarkeit von IP-Adressen

Bereits seit Jahren wird die Frage diskutiert, ob es sich bei IP-Adressen um personenbeziehbare Daten handelt oder nicht. In der juristischen Fachliteratur ist ein heftiger Meinungsstreit entbrannt, welcher jedoch durch die klare Linie der deutschen Aufsichtsbehörden im Datenschutzrecht relativiert wird. Diese vertreten beharrlich und einheitlich die Ansicht, dass IP-Adressen personenbeziehbar sind und dem Schutzbereich des BDSG sowie des TMG unterfallen. Eine Speicherung von IP-Adressen sei demnach grundsätzlich dem Verbot mit Erlaubnisvorbehalt aus § 4 Abs. 1 BDSG bzw. § 12 Abs. 1 TMG unterworfen. In einem Urteil vom 19. Oktober 2016 hat sich nun auch der EuGH mit dieser Frage befasst.

Sven Venzke-Caprarese

Der Fall

Der EuGH (Rechtssache C-582/14) hatte eine Vorlagefrage des BGH zu beantworten. Der BGH hat darüber zu entscheiden, ob Websites des Bundes die ungekürzten IP-Adressen der zugreifenden Computer speichern dürfen, um Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen. Der BGH setzte das Verfahren aus, um dem EuGH zwei Fragen im Rahmen der Vorabentscheidung vorzulegen.

Verkürzt dargestellt, handelte es sich dabei um folgende Fragen:

- Sind (dynamische) IP-Adressen von Websitebesuchern für den Betreiber einer Website personenbeziehbare Daten, auch wenn nur der Access-Provider des Besuchers über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?

- Dürfen Rechtsvorschriften grundsätzlich die Speicherung der IP-Adressen über den Nutzungsvorgang hinaus verbieten?

Die Entscheidung

Wenig überraschend vertrat der EuGH im Hinblick auf die erste Frage die Ansicht, dass IP-Adressen auch für den Anbieter einer Website personenbeziehbar sein können. Eine Personenbeziehbarkeit ergäbe sich immer dann, wenn der Websitebetreiber über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen

des Access-Providers bestimmen zu lassen. Ein solches rechtliches Mittel sei u. a. in der Möglichkeit von Websitebetreibern zu sehen, sich „im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten“.

Allerdings stellte der EuGH im Rahmen der zweiten Frage fest, dass es europarechtswidrig ist, wenn die Regelung des § 15 TMG dazu führen würde, dass eine Speicherung von IP-Adressen über den Nutzungsvorgang hinaus kategorisch ausgeschlossen sei. Denn insbesondere zur Gewährleistung der generellen Funktionsfähigkeit der Dienste könne die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus gerechtfertigt sein.

Auswirkungen für die Praxis

Die Auswirkungen für die Praxis werden jetzt durch den BGH konkretisiert werden müssen, der das ausgesetzte Verfahren fortzuführen hat. Für Websiteanbieter dürfte die Entscheidung des EuGHs ein positives Signal sein. Denn bereits in der Vergangenheit mussten Websitebetreiber aufgrund der einheitlichen Haltung der Aufsichtsbehörden in der Praxis von einer Personenbeziehbarkeit von IP-Adressen ausgehen. Problematisch war hingegen, dass viele Aufsichtsbehörden die Speicherung der IP-Adresse über den Nutzungsvorgang hinaus kategorisch ablehnten.

Mindestens drei Aufsichtsbehörden blickten in der Vergangenheit über den Tellerrand:

1.) Das Bayerische Landesamt für Datenschutzaufsicht formulierte im Tätigkeitsbericht 2009/2010, in Ziffer 4.2.1 zur Frage der Zulässigkeit der Speicherung von IP-Adressen von Websitebesuchern: „IP-Adressen können personenbezogene Daten sein. Ihre kurzfristige Speicherung zum Zweck der Gewährleistung der Integrität der technischen Systeme ist nach dem BDSG zulässig. Im Übrigen richtet sich die Zulässigkeit ihrer Erhebung, Verarbeitung und Nutzung nach dem Telemediengesetz (TMG). Dort findet sich keine Erlaubnis, IP-Adressen vorsorglich zu Strafverfolgungszwecken zu speichern.“ Das Bayerische Landesamt ging insofern von einer maximalen Speicherdauer von sieben Tagen aus.

2.) Auch die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen vertrat im 19. Datenschutzbericht 2009 in Ziffer 3.6 eine ganz ähnliche Position: „Abzugrenzen ist die Protokollierung von Kommunikationsdaten bei der Nutzung von Webangeboten von der Protokollierung im Rahmen von Intrusion-Detection-Systemen zu Zwecken der Datensicherheit. Das TMG enthält hierzu keine Regelungen. Protokollierungen zum Schutz interner Systeme und Netze sind auf der Grundlage von § 10 Datenschutzgesetz NRW oder § 9 Bundesdatenschutzgesetz zulässig.“

3.) Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz vertrat im 23. Datenschutzbericht 2010/2011, Teil II, Ziffer 1.4 ebenfalls die Ansicht, dass sich „Maßnahmen mit dem Ziel, Angriffe zeitnah zu erkennen bzw. ihnen zeitnah zu begegnen“ im Rahmen der Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungssysteme „auf § 12 Abs. 3 TMG i.V.m. §§ 9 Abs. 2, 13 Abs. 6 LDSG bzw. in analoger Anwendung auf § 100 Abs. 1 TKG stützen lassen“.

Websitebetreiber, die sich bisher auf den Standpunkt gestellt haben, dass eine streng zweckgebundene Speicherung der IP-Adressen der Websitebesucher für einen Zeitraum von maximal sieben Tagen zulässig ist, dürften durch die Entscheidung des EuGHs gestärkt worden sein. Letztendlich wird jedoch der BGH die konkreten Rahmenbedingungen definieren müssen.

Blick in Richtung Access-Provider

An dieser Stelle lohnt sich ein Blick in Richtung der Speicherung der IP-Adressen durch Access-Provider. Diese konnten bislang nach einem Urteil des BGH vom 3.7.2014 zu Az. III ZR 391/13 davon ausgehen, dass sie zum Zwecke der Abwehr von Störungen und Fehlern an Telekommunikationsanlagen IP-Adressen auch ohne konkreten Anlass für einen Zeitraum von sieben Tagen speichern dürfen. Eine Rechtsgrundlage hierfür sah der BGH in § 96 Abs. 1 Satz 2 i. V. m. § 100 Abs. 1 TKG.

Zwar unterliegen Host- und Content-Provider (Websitebetreiber) nicht den Regelungen des TKG und können sich insofern nicht auf § 100 TKG berufen. Allerdings kann sich ein ganz ähnliches Ergebnis aus der Anwendung des § 9 BDSG bzw. insbesondere auch aus dem zum 27.7.2015 in Kraft getretenen § 13 Abs. 7 TMG herleiten lassen:

- Denn wie soll ein Diensteanbieter seiner Pflicht nachkommen, sein Internetangebot sicher zu gestalten, wenn er mangels einer Speicherbefugnis gar nicht in der Lage ist, bestimmte Angriffe und Angriffsmuster zu erkennen und eine effektive Intrusion Detection zu betreiben?

- Insbesondere bei der Behandlung fehlerhafter Anmeldeversuche kann die Speicherung der IP-Adresse zudem ein wichtiges Mittel zur Abwehr von Angriffen sein: Sofern mehrmalige fehlerhafte Anmeldeversuche für ein Benutzerkonto erkannt werden, kann das zugrundeliegende Benutzerkonto gesperrt werden. Sofern von einer IP-Adresse aus mehrmalige fehlerhafte Anmeldeversuche über verschiedene Nutzerkonten festgestellt werden, kann

es darüber hinaus sinnvoll sein, die betroffene IP-Adresse für eine bestimmte Zeit zu sperren.

- Die Speicherung der IP-Adressen kann zudem erforderlich sein, um fehlkonfigurierte Scripte eines Webservers zu erkennen, die für einen ungewöhnlich hohen Traffic auf den Seiten des Websitebetreibers sorgen können.

- Umstritten ist die Erforderlichkeit der Speicherung zur Erkennung von DDoS Attacken. Spätestens bei der Abwehr werden jedoch die IP-Adressen erforderlich sein, z. B. um ein Blackholing durchzuführen, welches bestimmte IP-Adresskreise ins Leere routet.

- Möglicherweise wird der BGH vor dem Hintergrund dieser Bedrohungen auch für Content- und Host-Provider zu einem ganz ähnlichen Ergebnis kommen, wie dies bereits für Access-Provider der Fall ist.

Fazit

Das Urteil des EuGHs ist zu begrüßen. Websitebetreiber, die sich in der Vergangenheit auf den Standpunkt stellten, dass (analog zur Speicherbefugnis des Access-Providers) IP-Adressen für sieben Tage streng zweckgebunden zu Sicherheitszwecken gespeichert werden dürfen, werden gestärkt. Denn ein kategorisches Verbot der Speicherung wird sich nach dem Urteil des EuGHs von Aufsichtsbehörden nicht mehr aufrechterhalten lassen.

Rechtssicherheit wird allerdings erst das Urteil des BGH herbeiführen, welcher nun die näheren Details zu entscheiden hat.

Vertiefungshinweis im Handbuch „Datenschutz im Gesundheitswesen“ (DSIGW):

- Datenschutz im Gesundheitswesen (AOK-Verlag GmbH), Kapitel C/12.1.3 (Verarbeitung der IP-Adresse)

Hintergrundwissen:

Anonymisierung von IP-Adressen

IPv4-Adressen können durch Löschung des letzten Oktetts anonymisiert werden. Die IPv4-Adresse 91.248.52.222 könnte also anonymisiert wie folgt dargestellt werden: 91.248.52.xxx.

Komplizierter wird die Anonymisierung bei den neuen IPv6-Adressen, die aufgrund des IP-Adressmangels schrittweise eingeführt werden. Hier wird die Ansicht vertreten, dass für eine wirksame Anonymisierung nur die ersten vier Byte einer IPv6-Adresse bestehen bleiben dürfen und alles andere gelöscht werden muss. Die IPv6-Adresse fe80:0000:0000:0000:9123:4567:89ab:cdef sähe nach der Anonymisierung also wie folgt aus: fe80:0000:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

Was ist der Unterschied zwischen statischen und dynamischen IP-Adressen?

Statische IP-Adresse im engeren Sinne: Im europäischen Adressraum wurde jede IPv4-Adresse bislang von einem Internet Registrar, dem sog. Réseaux IP Européens Network Coordination Centre (RIPE NCC), an juristische und natürliche Personen vergeben – meist handelte es sich hierbei um Access-Provider, gelegentlich aber auch um natürliche Personen. In einer unter http://apps.db.ripe.net/search/ abrufbaren Adressdatenbank kann jedermann einsehen, wem die statische IP-Adresse im engeren Sinne gehört.

Dynamische IP-Adressen: Sofern ein Access-Provider statische IP-Adressen im engeren Sinne erhalten hat, kann er diese nun seinen Nutzern zuteilen. Verfügt ein Access-Provider über zu wenig IP-Adressen, ist er gezwungen, diese möglichst dynamisch seinen Nutzern zuzuweisen – z. B. solange diese tatsächlich Internetdienste nutzen. In der Praxis hat sich daher eine Zwangstrennung nach 24 Stunden und ein Wechsel der IP-Adresse etabliert. Gleichwohl finden sich in der Praxis auch immer wieder Provider, die von dieser Praxis abweichen.

Statische IP-Adresse im weiteren Sinne: Nicht immer möchten Kunden eine dynamische IP-Adresse erhalten, z. B. weil Sie die IP-Adresse als Teil der Authentisierung gegenüber zugangsgeschützten Systemen nutzen möchten etc. In diesem Fall wird der Access-Provider seinem Kunden immer wieder dieselbe IP-Adresse zuteilen.

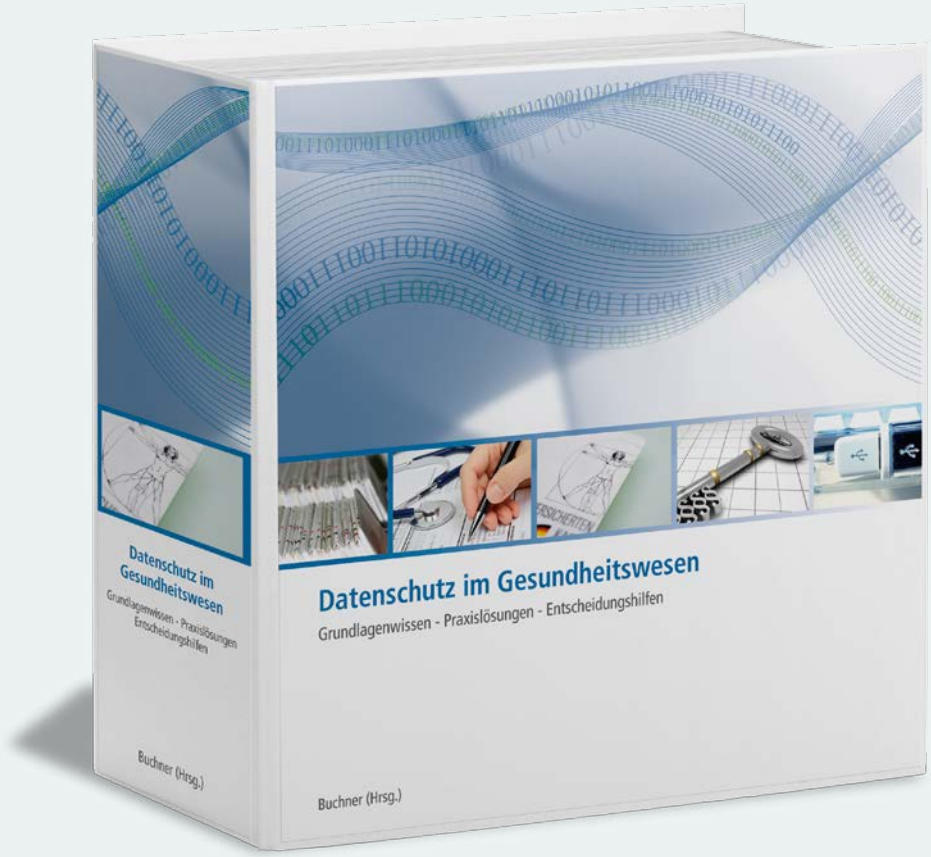
Kurznotiz:

Google Analytics wieder beanstandungsfrei nutzbar?

In unserer Juliausgabe hatten wir darüber berichtet, dass der Hamburgische Datenschutzbeauftragte eine Orientierungshilfe zum beanstandungsfreien Betrieb von Google Analytics mit Hinweis auf das EuGH-Urteil zu Safe Harbor (Rechtssache C-362/14) zurückgezogen hat.

Mittlerweile hat sich Google Inc. jedoch dem EU-U.S. Privacy Shield unterworfen und wird in der entsprechenden Liste des U.S. Department of Commerce geführt. Das EU-U.S. Privacy Shield ersetzt das bisherige Safe Harbor-Abkommen und ist in der Praxis geeignet, ein angemessenes Datenschutzniveau zu gewährleisten.

Eine Stellungnahme des Hamburgischen Datenschutzbeauftragten gibt es allerdings noch nicht. Gleichwohl dürfte nun eigentlich nichts mehr dagegen sprechen, Google Analytics, wie in der zurückgezogenen Orientierungshilfe beschrieben, zu nutzen. Den Text der zurückgezogenen Orientierungshilfe finden sie bei archive.org unter diesem Link.



Datenschutz im Gesundheitswesen

Grundlagenwissen – Praxislösungen – Entscheidungshilfen

2 Ordner mit Register im Format DIN A5,
ca. 1.500 Seiten Inhalt
ISBN: 978-3-553-43000-5
Preis 179.- inkl. MwSt.

Uneingeschränkter Online-Zugriff auf alle Arbeitshilfen inkl. 3-4 kostenpflichtige Nachtragslieferungen pro Jahr zum Preis von jeweils 74,90 Euro inkl. MwSt. und versandkostenfreier Zusendung im Inland.