

## Impressum

**Handelsblatt Fachmedien GmbH**

Grafenberger Allee 293, 40237 Düsseldorf  
Postfach 10 11 02, 40002 Düsseldorf  
www.fachmedien.de

Handelsregisternummer: AG Düsseldorf HRB 30329  
Umsatzsteuer-ID-Nummer DE 814828360

**Geschäftsführung** Claudia Michalski

**Verlagsleitung/Prokurist** Christoph Bertling

**Herausgeber**

Hans Gliss (HG)  
Pattweg 8, D - 50259 Pulheim  
Telefon 040/399 060-32, Telefax -33  
E-Mail: hans.gliss@gliss-kramer.de

**Redaktion Hamburg**

Dr. Philipp Kramer (PK), Chefredakteur  
Anna Schuster; Lena Ruge  
Erik-Blumenfeld-Platz 27a, 22587 Hamburg  
Telefon: 040/399 060-32, Telefax: -33  
E-Mail: redaktion@gliss-kramer.de  
www.datenschutz-berater.de

**Produktmanagement**

Alissa Tempelhoff  
E-Mail: a.tempelhoff@fachmedien.de

**Autoren**

Hans Gliss, Hamburg; Britta Hinzpeter, München;  
Hajo Köppen, Gießen; Dr. Philipp Kramer, Hamburg;  
Nicole Schmidt, Bad Wimpfen; Prof. Dr. Jürgen Vahle,  
Bielefeld

**Mediasales****Verkauf:**

GRUNERT Medien & Kommunikation GmbH  
Telefon: 06 21/71 78 602, Telefax: 06 21/71 78 603  
E-Mail: m.grunert@grunert-medien.de

**Disposition:**

Annette Becker  
Klambt-Verlag GmbH & Co. KG  
Telefon: 0 62 32/3 10-2 75, Telefax: 0 62 32/3 10-2 73  
E-Mail: annette.becker@klambt.de

**Kundenservice**

Handelsblatt Fachmedien GmbH  
Kundenservice  
Postfach 10 11 02, 40002 Düsseldorf  
E-Mail: kundenservice@fachmedien.de  
www.datenschutz-berater.de  
Inland: Telefon 0800/000-1637, Fax -2959 (kostenfrei)  
Ausland: Telefon +49 (0)211 887-3670, Fax -3671

**Abonnement**

Erscheint monatlich

- Einzelheft: EUR 23,90 zzgl. Versandkosten
- Jahresabo (inkl. 1 Zugang zum Online-Archiv): EUR 279,- inkl. Versand und MwSt.
- Studentenabo: EUR 147,50 inkl. Versand und MwSt.
- Studentenabo Ausland: EUR 126,72 zzgl. Versand EUR 13,20
- Auslandsabo: EUR 249,60 zzgl. Versand in Europa EUR 13,20. Angaben zu MwSt. im Ausland finden Sie unter [www.fachmedien.de/bezugspreise](http://www.fachmedien.de/bezugspreise).
- GDD Mitglieder erhalten 20% Rabatt: EUR 225,60 inkl. Versand und MwSt.

Abonnementkündigungen sind nur mit einer Frist von 21 Tagen zum Ende eines Bezugsjahres möglich. Im Falle höherer Gewalt (Streik oder Aussperrung) besteht kein Belieferungs- oder Entschädigungsanspruch.

**Copyright**

Alle Rechte vorbehalten. Der Inhalt dieser Publikation darf ohne schriftliche Genehmigung des Verlages nicht vervielfältigt oder verbreitet werden. Unter dieses Verbot fällt auch die gewerbliche Vervielfältigung per Kopie, die Aufnahme in elektronische Datenbanken sowie die Vervielfältigung auf CD-ROM.

**Layout** Sigrid Lessing

**Druck** Sächsisches Druck- und Verlagshaus AG, Dresden

**Beilagenhinweis** Haufe Lexware, Verlag C.H. Beck

**Handelsblatt**  
**FACHMEDIEN**

## Datensicherheit ist auch nach „Snowden“ möglich!



Fast täglich werden haarsträubende Details über Umtriebe und Allmachtsansprüche der Geheimdienste bekannt. Dass die Enthüllungen von Edward Snowden auf verlässlichem Datenmaterial beruhen, ist in der Fachwelt unbestritten. Offen bleibt die Frage „Was tun, wie kann man sich schützen?“. Damit sind wir beim Datenschutzbeauftragten, dem IT-Sicherheits- und dem Compliancebeauftragten sowie der Revision angelangt – und bei Vorstand, Geschäftsführung oder Behördenleitung. Es gilt Wege zu finden, eigene Positionen zu bestimmen und Maßnahmen zur Verbesserung der IT-Sicherheit abzuleiten.

Eine Bedrohungsanalyse ist neu vorzunehmen. Sie hat nach zwei Seiten zu schauen: Einerseits auf potentielle Angreifer und deren Methoden, andererseits auf installierte Sicherheitsmechanismen und die ihnen unterstellte Robustheit. Diese Sichtweise bringt neue Perspektiven: Die Mächtigkeit der Angreifer ist wesentlich höher als man es bisher annehmen konnte; Berichte über Hintertüren in IT-Komponenten sowie ausgehebelte oder vom Sourcecode her bereits bewusst manipulierte Sicherheitsfunktionen stellen letztlich die Verlässlichkeit aller IT-Komponenten in Frage.

IT-Betreiber und –Nutzer müssen sich mit einem neuen Denkansatz anfreunden: Galt es als bisher erstrebenswert, Systeme und IT-Komponenten zu verknüpfen, benutzerfreundliche Varianten zu ermöglichen (Single-Sign-On, Cloud und Mobile Computing, Bring Your Own Device ...), so kann die „erste Verteidigungslinie“ heute nur heißen „Inseln bilden, abschotten, kontrollierte Übergänge einrichten“. IT wird damit tendenziell teurer zugunsten von mehr Sicherheit, was freilich betriebswirtschaftlich nicht und „gefühl“ nur schwer kalkulierbar ist. Die IT muss stärker reglementiert werden, was die Benutzerfreundlichkeit schmälert. Damit müssen sich die Verantwortlichen auseinandersetzen – denn alles, was zur Verbesserung der Sicherheit als sinnvoll wahrgenommen wird, muss den Nutzern erklärt und begründet werden. Sicherheit kann man nie gegen die Beschäftigten durchsetzen, sondern nur, indem man diese zu Verbündeten der eigenen Sicherheitsziele macht. Dazu bedarf es einer Definition dieser „eigenen Sicherheitsziele“ – und eines Regelwerks, das auf die eigenen Belange zugeschnitten und allgemein verständlich ist.

**Hans Gliss**, Herausgeber DATENSCHUTZ-BERATER

**Links/Quellenangaben** - siehe.eu: Die Hinweise auf Quellen sind für die leichte Eingabe mit einem Shortlink (auch short URL, URL alias, Kurzlink) angegeben. Statt beispielsweise [http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Taetigkeitsberichte/Functions/TB\\_BfDl\\_Table.html?nn=408924](http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Taetigkeitsberichte/Functions/TB_BfDl_Table.html?nn=408924) muss künftig nur angegeben werden: [www.siehe.eu/xxx](http://www.siehe.eu/xxx). Das xxx steht für eine fortlaufende Zahl. Mit dieser Zahl kann die eigentliche URL/Adresse in unserer Datenbank ermittelt werden. Wenn Sie wissen wollen, was sich hinter dem Shortlink verbirgt, geben Sie den Shortlink mit einer Tilde (~) ein oder nutzen Sie eine Shortlink-Auflöser wie [www.preurl.com](http://www.preurl.com). Ob Sie auf diese Möglichkeit verzichten, obliegt Ihrer Entscheidung. Denn wir verweisen auf die Quellen, ohne diese im Detail zu prüfen.