Kompact

Last-Minute-Hilfe DSGVO vor dem 25. Mai

Fit für die DSGVO

Der neue EU-Datenschutz

Verschärfte Regeln und hohe Bußgelder

Pflichten für Webmaster, Firmen und Vereine

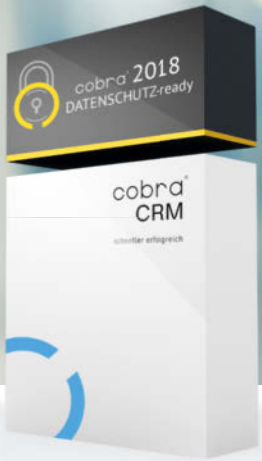
So nutzen Sie die neuen Verbraucherrechte

NEU!

Computer Bild
TRUSTED SOLUTIONS
★★★★★ 2018
Ausgabe 4/2018
cobra
IN DER KATEGORIE VERTRIEBS-/ CRM-SOFTWARE

cobra®
DATENSCHUTZ-Premium Edition

Die brandneue Komplett-Lösung von cobra für Vertrieb, Marketing und Service.



EU-DSGVO 2018 konform

- **Personenbezogene Daten erheben, verarbeiten und ausgeben**
- **Rechtskonforme Einwilligung mit Double-Opt-in-Verfahren**
- **Zeitgesteuerte Löschung personenbezogener Daten**
- **Datenschutz-Cockpit mit Dashboards und Drill-Downs**
- **E-Mail-Blacklist und cobra Sperrliste**
- **Download-Center und Newsletter-Aboverwaltung**

Download

E-Book Datenschutz!

Nur für kurze Zeit gratis unter:
www.cobra.de/Datenschutz2018

Jetzt informieren:
Telefon +49 7531 8101-66
kundenberatung@cobra.de

cobra®
schneller erfolgreich

Liebe Leserinnen und Leser,

kaum ein EU-Gesetz hat in den letzten Jahren für so viel Wirbel gesorgt wie die neue Datenschutzgrundverordnung. Angst vor Abmahnwellen und horrenden Bußgeldern herrscht bei Weltkonzernen, aber auch unter Bloggern, kleinen Firmen und Vereinen.

Was ab dem 25. Mai tatsächlich passiert, ist kaum vorherzusagen. Doch lassen sich Risiken minimieren, wenn man die Grundzüge der neuen Rechtslage kennt und notfalls auch noch kurzfristig darauf reagiert. Um Sie dabei zu unterstützen, haben wir dieses kompakte Heft erstellt. Sie erfahren die wichtigsten Neuerungen und erhalten Anregungen zur schnellen Umsetzung.

Inhalt

Gutes Gelingen wünscht Ihnen

Holger Bleich

Die DSGVO betrifft jeden

Verschärfte Regeln und heftige Bußgelder

Am 25. Mai 2018 endet nun die zweijährige Übergangsfrist: Die EU-Datenschutzgrundverordnung (DSGVO), die am 24. Mai 2016 in Kraft getreten ist, entfaltet ab diesem Datum ihre volle Wirkung. War bislang hierzulande das Datenschutzrecht zahnlos, drohen nun schon bei wenig gravierenden Verstößen erhebliche Bußgelder. Besonders schwerwiegenden Rechtsbruch von Unternehmen können die Aufsichtsbehörden jetzt mit bis zu 20 Millionen Euro ahnden, Großkonzernen drohen gar Geldstrafen von bis zu vier Pro-

zent des weltweiten Jahresumsatzes.

Den Aufsichtsbehörden kommt also ab dem 25. Mai eine wesentlich höhere Bedeutung zu als bislang. Viele EU-Staaten haben darauf reagiert und sowohl organisatorisch als auch personell aufgestockt – auch Deutschland. Zuständig für den privaten Sektor sind die Datenschutzbeauftragten der Bundesländer, nicht etwa die Bundesdatenschutzbeauftragte. Sie sollen künftig intensiver beraten, aber auch schneller Bürgerbeschwerden bearbeiten und wenn nötig Bußgelder verhängen. Einige haben bereits angekündigt, rigoros durchzugreifen.

Jeder, der mit personenbezogenen Daten hantiert, sollte folglich die neuen – europaweit nahezu einheitlichen – Regeln zumindest in groben Zügen kennen. Besonderes Augenmerk gilt allen Handlungen, die – etwa auf Websites – von außen sichtbar sind, also beispielsweise Erklärungen gegenüber Nutzern oder Kunden. Deutsche Betreiber haben vergleichsweise Glück gehabt: Weil für große Teile der DSGVO das strenge deutsche Datenschutzrecht Pate stand, müssen sie gar nicht so viel umdenken.

Weiterhin gilt beispielsweise das **Verbot mit Erlaubnisvorbehalt**. Demnach ist es untersagt, personenbezogene Daten zu erheben, zu speichern oder zu verarbeiten, wenn keine spezielle Rechtsgrundlage oder informierte Einwilligung des Betroffenen vorliegt. Die **Zweckbindung** wurde sogar erweitert: Personenbezogene Daten darf man nur für einen zuvor festgelegten Zweck erheben und schon gar nicht weiterveräußern. Generell gilt in der DSGVO wie auch im alten Bundesdatenschutzgesetz das Gebot der **Datenminimierung**, nach

dem so wenige Daten wie möglich und nur so viele wie unbedingt für den Zweck nötig erhoben werden dürfen.

Die DSGVO soll Betreiber dazu zwingen, die Verarbeitung personenbezogener Daten transparenter und sicherer zu gestalten. Von der Datenerhebung Betroffene sollen jederzeit gut informiert sein. Deshalb gelten nun **erweiterte Auskunftspflichten** und das Gebot zu klaren, **verständlichen Erklärungen**, beispielsweise für die Datenschutzerklärung und Einwilligungstexte. Um diese Prinzipien durchzusetzen, etabliert die DSGVO eine erweiterte **Rechenschaftspflicht**: Betreiber müssen einzelne Vorgänge in Verzeichnissen dokumentieren, von größeren Unternehmen fordert das EU-Recht eine fortlaufende **Risikoabschätzung** aller Datenverarbeitungsprozesse.

Mit der DSGVO ist die EU-Datenschutzreform noch nicht zu Ende. Derzeit durchläuft das Ergänzungsprojekt E-Privacy-Verordnung (E-Privacy-VO) den Gesetzgebungsprozess. Die Verordnung wird etliche eher allgemeine Vorgaben der DSGVO konkretisieren. Geplant sind etwa strenge Regeln zum Usertracking, die der werbetreibenden Industrie gar nicht schmecken. Vor 2019 ist allerdings nicht mit einer finalen Version der E-Privacy-VO zu rechnen. *hob@ct.de* c't

§ Hilfestellung

Unter dem Link **ct.de/dsgvo18** haben wir für Sie weiterführende Literatur, Musterformulare und Textgeneratoren zur DSGVO zusammengetragen. Damit sollte es Ihnen gelingen, zumindest offensichtliche DSGVO-Mängel Ihres Projekts schnell zu identifizieren und zu beseitigen.

Vertrauenswürdige IT-Sicherheit made in Germany

Wir sind immer da aktiv, wo viel auf dem Spiel steht. Wo sensible Daten und Identitäten elementare Werte von Behörden und Unternehmen sind. Wo Kunden in Sicherheitsfragen vor komplexen Herausforderungen stehen.

Unsere Spezialisten schützen Staat, Gesellschaft und Wirtschaft zuverlässig vor Cyberbedrohungen. Wir haben die IT-Sicherheitslösungen für digitale und vernetzte Infrastrukturen – und das bis zu höchsten Anforderungen an die Vertraulichkeit.

www.secunet.com

secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland

Vertragt Euch!

DSGVO für Webmaster, Unternehmen und Vereine

Nicht nur Konzerne oder Online-Händler müssen die Vorgaben der DSGVO umsetzen, sondern in vielen Fällen auch Blogger, Vereine und auch sonst jeder, der im Web personenbezogene Daten speichert – und das gilt bereits für IP-Adressen. Hier finden Sie einen Überblick zu den wichtigsten Anforderungen. Vieles lässt sich in wenigen Tagen umsetzen. Falls Sie es noch nicht getan haben: Beginnen Sie heute, um Abmahnungen und Bußgelder zu vermeiden. Diese Liste dient nur dem ersten Überblick. Im Zweifel lesen Sie unseren DSGVO-Schwerpunkt in c't 5/18 oder konsultieren Sie einen spezialisierten Rechtsanwalt.

Datenschutzerklärung: Jeder Website-Betreiber muss seine Besucher über Vorgänge aufklären, bei denen er personenbezogene Daten verarbeitet oder weitergibt. Die DSGVO erweitert den

Umfang und die Art der Pflichtangaben erheblich – und sie fordert verständliche und transparente Sprache. Es genügt nicht, die Erklärung im Impressum zu verlinken; ein Hinweis sollte auf der Homepage – etwa im Footer – leicht zu finden sein. Generatoren erleichtern es, schnell einen solchen Text zu erstellen. Vorsicht: Längst nicht alle dieser Web-Angebote sind bereits auf die DSGVO-Anforderungen aktualisiert.

Auftragsverarbeitung: Wann immer externe Dienstleister mit personenbezogenen Daten in Kontakt kommen, sollte geprüft werden, ob mit ihnen ein Vertrag zur Auftragsverarbeitung abzuschließen ist. Dieser Vertrag bestätigt dann, dass der Auftragsverarbeiter Daten „gemäß den Weisungen des für die Verarbeitung Verantwortlichen" behandelt. Bei Websites gilt diese Pflicht zum Vertrag bezüglich des Hosters oder Cloud-Anbieters bereits, wenn dieser Besucher-IP-Adressen loggt und für Analysezwecke zur Verfügung stellt. Beachten Sie auch Services wie E-Mail-Dienste, Newsletter-Versender, externe Backup-Lösungen oder die ausgelagerte Lohn- und Finanzbuchhaltung. Viele Service-Anbieter halten bereits DSGVO-konforme Musterverträge vor (siehe c't-Link).

Verarbeitungstätigkeiten: Bis auf wenige Ausnahmen ist laut DSGVO ein „Verzeichnis von Verarbeitungstätigkeiten" zu erstellen. Darin wird jeder Prozess, bei dem personenbezogene Daten erfasst und verarbeitet werden, dokumentiert. Außerdem sind Verantwortliche für diese Prozesse zu nennen. Dieses Verzeichnis ist nicht öffentlich, sondern soll der internen Qualitätskontrolle dienen und außerdem jederzeit auf

Anfrage einer Aufsichtsbehörde vorgelegt werden. Das klingt zwar aufwendig, ist es aber meist gar nicht. Der Branchenverband Bitkom etwa hält kostenfrei einen leicht verständlichen Leitfaden mit vielen Beispielen vor.

Die DSGVO gilt auch für Blogger und Vereine

Datenschutzbeauftrager: Verarbeitet ein Verein oder ein Unternehmen besonders geschützte Daten oder sind mindestens zehn Personen mit Datenbearbeitung beschäftigt, muss ein Datenschutzbeauftragter benannt werden. Er soll laut DSGVO Verantwortliche beraten, Betroffenen helfen, den Datenschutz überwachen und insbesondere als Bindeglied zwischen Betreiber und Aufsichtsbehörden dienen. Deshalb muss seine Ernennung der im Bundesland zuständigen Datenschutzbehörde gemeldet werden. Außerdem sollte er leicht zu kontaktieren sein. Dazu genügt es, seine E-Mail-Adresse in der Datenschutzerklärung zu veröffentlichen.

Einwilligungen: Die DSGVO verschärft das bislang in Deutschland geltende Kopplungsverbot bei Einwilligungen zur Datenverarbeitung. So darf etwa der Abschluss eines Vertrags nicht mehr von einer Einwilligung in andere Zwecke abhängig gemacht werden. Außerdem dürfen Webmaster nur Daten anfordern, die sie für die jeweilige Aufgabe benötigen (Datenminimierung). Bei Newsletter-Anmeldungen etwa sind die Abfrage von Postadresse oder Geburtsdatum nicht erforderlich. Pflichtfelder sollten klar zu erkennen sein. Außerdem muss der Infotext zur Einwil-

§ IT-Sicherheit

Die DSGVO macht neue Vorgaben zur IT-Sicherheit. Der „risikobasierte Ansatz" dürfte allerdings fürs Kleingewerbe und Vereine weniger relevant sein. Es geht hier darum, dass Unternehmen und Konzerne „geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten". Je nachdem, wie sensibel die Daten und Anwendungsbereiche sind, muss eine Firma sogar bereits vor der ersten Datenerhebung die Aufsichtsbehörde konsultieren. Änderungen ihrer Verarbeitungsprozesse muss sie künftig dokumentieren, das Risiko neu bewerten und ihre Schutzmaßnahmen aktualisieren.

ligung darauf hinweisen, dass sie jederzeit widerrufen werden kann.

Verschlüsselung: Personenbezogene Daten müssen transportverschlüsselt zur Website gelangen. Aus dem aus der DSGVO hervorgehenden Grundsatz der Integrität und Vertraulichkeit kann abgeleitet werden, dass eine SSL-Verschlüsselung bei Web-Formularen, Log-ins oder Shop-Bestellungen nun verpflichtend ist. Der E-Mail-Server oder -Provider muss TLS beherrschen und wann immer möglich verwenden. Auf der sicheren Seite ist, wer außerdem Dateien vor dem Versand mindestens mit Zip verschlüsselt und niemals unverschlüsselt in externe Cloud-Speicher legt.

Tracking: Denken Sie daran, mit externen Usertracking-Dienstleistern wie Google Analytics einen Vertrag zur Auftragsverarbeitung abzuschließen beziehungsweise diesen nach DSGVO-Vorgaben zu erneuern. Lassen Sie

sich bestätigen, dass Ihr Tracking-Dienst DSGVO-konform agiert. Dienen Cookies nicht nur der Erhaltung des Services, wie es etwa bei Session- oder Warenkorb-Cookies der Fall ist, benötigen Sie laut DSGVO eine „informierte Einwilligung" des Nutzers – also ein Opt-in, das sie beim ersten Website-Besuch einholen müssen. Das Tracking darf nur pseudonym und ohne Speicherung der IP-Adresse durchgeführt werden. Ein Hinweis darauf muss in die Datenschutzerklärung aufgenommen werden und eine Opt-Out-Möglichkeit muss implementiert werden.

Meldepflicht: Geschieht eine Verletzung des Schutzes personenbezogener Daten, muss dies der Verantwortliche – etwa durch seinen Datenschutzbeauftragten – unaufgefordert der zuständigen Datenschutzaufsicht melden. Ansonsten droht nach Art. 83 DSGVO ein gepfeffertes Bußgeld. Es kann sich etwa um Verlust, Veränderung oder ungewollte Veröffentlichung von Daten handeln. Falls den Inhabern der Daten ein „hohes Risiko für die persönlichen Rechte und Freiheiten" droht, müssen auch sie unverzüglich informiert werden.

Auskunftspflicht: Sorgen Sie dafür, dass Sie Auskünfte zu Nutzerdaten auf konkreten Antrag hin innerhalb eines Monats erteilen können. Der Antragsteller muss seine Identität hinreichend nachweisen. Eine Auskunft muss nicht postalisch, sondern kann auch elektronisch übermittelt werden. Außer den Daten selbst sollten auch der Zweck der Speicherung, die geplante Speicherdauer und ein Hinweis auf Löschmöglichkeit in der Antwort enthalten sein. *hob@ct.de* c't

MANAGED CLOUD

MANAGED | SCALABLE

MANAGED SERVER

DEDICATED | VIRTUAL

Information Security Management System
ISO 27001
Zertifiziert

Do IT right!

www.centron.de

centron

Ihr Rechenzentrum in

cloud services
MADE IN GERMANY

Power to the people

DSGVO für Verbraucher

Für Verbraucher ist die DSGVO ein Gewinn: Unternehmen müssen sie genauer über die Verarbeitung ihrer Daten informieren und dürfen sich dabei nicht hinter Juristenkauderwelsch verstecken. Bürger stehen zudem mehr Mittel als bisher zur Verfügung, um Daten löschen zu lassen. Im Folgenden finden Sie die wichtigsten Neuerungen für Verbraucher in Form von Stichpunkten.

Grundsätzliches

Geltungsbereich: Die DSGVO stärkt die Rechte aller Verbraucher in der EU. Jedes Unternehmen, das Angebote an EU-Bürger richtet, ist ihnen gegenüber nun auskunftspflichtig – also zum Beispiel auch US-Unternehmen wie Facebook und Google.

Privacy by default: Unternehmen müssen Programme, Apps oder sonstige Anwendungen mit datenschutzfreundlichen Voreinstellun-

gen versehen. Grundsätzlich sollen nur zwingend erforderliche personenbezogene Daten verarbeitet werden. Das umfasst die Menge der erhobenen Informationen, den Umfang ihrer Verarbeitung, die Speicherdauer sowie die Zugänglichkeit und Weitergabe.

Grundsätzlich sollen nur zwingend erforderliche personenbezogene Daten verarbeitet werden.

Datenschutzbeauftragter: Die Bestimmungen bezüglich Ansprechpartnern für den Datenschutz sind nicht einheitlich geregelt. Deutsche Unternehmen müssen wie bisher in den meisten Fällen einen Datenschutzbeauftragten benennen, an den sich Verbraucher mit ihren Anliegen wenden können. Unternehmen, die keine Niederlassung in der EU unterhalten, aber Verbrauchern in der EU Waren oder Dienstleistungen anbieten oder ihr Verhalten beobachten, müssen einen EU-Vertreter bestellen.

Aufsichtsbehörden: Für internationale Firmen ist nur noch die Datenschutz-Aufsichtsbehörde an ihrem Hauptsitz in der EU zuständig. Verbraucher können sich an ihre jeweils nächstgelegene Aufsichtsbehörde wenden, also in der Regel den Datenschutzbeauftragten des jeweiligen Bundeslandes. Der muss das Anliegen dann weiterleiten. Die Behörden müssen sich untereinander abstimmen.

Auskünfte und Anfragen

Klartext: Unternehmen müssen Kunden in „präziser, transparenter, verständlicher

und leicht zugänglicher Form in einer klaren und einfachen Sprache“ informieren – kein Juristen-Geschwurbel. Das gilt sowohl für die Datenschutzbestimmungen als auch bei Auskünften über die Daten des Kunden.

Antworten: Unternehmen müssen Anträge und Anfragen von Kunden bezüglich der über sie gespeicherten Daten grundsätzlich kostenlos innerhalb eines Monats beantworten.

§ Der c’t-Formbrief

Damit Sie gegenüber Unternehmen Ihre Auskunfts- und Löschansprüche geltend machen können, hat c’t einen Formbrief entwickelt. Sie können ihn unter **ct.de/dsgvo18** als Word- und OpenDocument-Datei für den privaten Gebrauch herunterladen. Um ihn zu testen, haben wir ihn an uns selbst ausprobiert. Auch das Ergebnis finden Sie unter **ct.de/dsgvo18**.

Informationsrechte: Unternehmen müssen Kunden ausführlich über die Verarbeitung ihrer Daten und über ihre Rechte informieren. Der Kunde hat unter anderem ein Recht zu erfahren,

- welche Daten und zu welchen Zwecken diese von ihm erhoben wurden;
- welche Empfänger seine Daten bereits erhalten haben oder künftig noch erhalten werden;
- wie lange seine Daten gespeichert werden sollen oder, falls dies unklar ist, die Kriterien für die Festlegung dieser Dauer;
- ob auf Basis seiner Daten eine automatisierte Entscheidungsfindung einschließlich „Profiling“ durchgeführt wurde, mit aussagekräftigen Informationen über die involvierte Logik.

Sofern das Unternehmen die Daten nicht bei selbst beim

Kunden erhoben hat, muss es dem Kunden alle verfügbaren Informationen über die Herkunft der Daten mitteilen.

Zugriff und Löschen

Datenkopie: Unternehmen müssen Verbrauchern auf Wunsch eine Kopie von deren personenbezogenen Daten in einem gängigen elektronischen Format zur Verfügung stellen – also zum Beispiel als PDF oder über ein Web-Frontend.

Datenübertragbarkeit: Verbraucher können von ihrem Anbieter in aller Regel verlangen, dass dieser ihre personenbezogenen Daten „in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format“ bereitstellt. Verbraucher sollen so einfach zu einem anderen Anbieter umziehen können.

Löschung: Ein Unternehmen muss persönliche Informationen löschen, sobald der Zweck weggefallen ist, für den es sie ursprünglich erhoben hat. Ein typisches Beispiel: Kundendaten, die es bei einem Kauf erfasst hat, muss es löschen, wenn die steuerrechtlichen Pflichten zur Aufbewahrung enden, aber nicht vorher.

Recht auf Vergessenwerden und Verstöße

Vergessenwerden: Das Recht auf Vergessenwerden bezieht sich auf (Spuren von) personenbezogenen Daten über eine Person, die durch Veröffentlichungen einer breiten Öffentlichkeit zugänglich sind – insbesondere im Internet. Unter bestimmten Voraussetzungen kann die Person vom Verbreiter verlangen, diese zu löschen. Der ursprüngliche Verbreiter muss dann Dritte, die die Informationen ebenfalls veröffentlichen, vom Löschverlangen unterrichten.

Datenschutzpannen: Zukünftig müssen Unternehmen Kunden die allermeisten Datenschutzpannen melden, die ihre Daten betreffen – und zwar „ohne unangemessene Verzögerung“.

Praxistest kommt erst

So nützlich die Datenschutzgrundverordnung für den Verbraucher grundsätzlich sein mag: Viele Regelungen der Verordnung sind schwammig formuliert. Andere, etwa das Recht auf Vergessenwerden, „Privacy by default“ und das Recht auf Datenübertragbarkeit sind neu. Der Praxistest steht erst noch an, er beginnt mit dem Wirksamwerden der DSGVO am 25. Mai.

Mitunter werden dann erst Aufsichtsbehörden und die Gerichte den Wirkungsbereich der Datenschutzgrundverordnung ausdefinieren müssen. Und das kann einige Jahre dauern.

jo@ct.de c't

Impressum

Redaktion
Karl-Wiechert-Allee 10,
30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.ct.de
Chefredakteur: Dr. Jürgen Rink (jr) (verantwortlich für den Textteil)
Redaktion: Jo Bager (jo@ct.de), Holger Bleich (hob@ct.de)
Art Direction: Nicole Judith Hoehne

Verlag
Heise Medien GmbH & Co. KG
Karl-Wiechert-Allee 10,
30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de
Herausgeber: Christian Heise, Ansgar Heise, Christian Persson
Geschäftsführer: Ansgar Heise, Dr. Alfons Schräder
Mitglied der Geschäftsleitung: Beate Gerold, Jörg Mühle
Verlagsleiter: Dr. Alfons Schräder
Anzeigenleiter: Michael Hanke (-167, verantwortlich für den Anzeigenteil), www.heise.de/mediadaten/ct/
Leiter Vertrieb und Marketing: André Lux (-299)

Druck: Goldschmidt GmbH, Josefstraße 35, 49809 Lingen

EU-DSGVO: MACHEN SIE DEN CHECK!

Rufen Sie die Security-Feuerwehr:

ihr-dsgvo-check.de

Eine Veranstaltung von heise Events

2. IT-Sicherheitstag Rhein-Ruhr

IT-Sicherheit in die Praxis umsetzen

Ohne IT-Sicherheit wird keine nachhaltige Digitalisierung gelingen, daher wollen wir uns am 2. IT-Sicherheitstag Rhein-Ruhr in Gelsenkirchen intensiv mit dem Thema IT-Sicherheit auseinander setzen.

Auf der Konferenz treffen Sie auf Sicherheitsexperten, die über die aktuellen, drängenden Fragen der IT-Sicherheit berichten. Sie liefern Strategien, Lösungen und konkrete Tipps für die praktische Umsetzung im Unternehmen.

Der 2. IT-Sicherheitstag Rhein-Ruhr ist eine Mischung aus Konferenz, Fachausstellung und Plattform zum Erfahrungsaustausch und Netzwerken.

Termin: 29. Mai 2018, Gelsenkirchen

THEMENSCHWERPUNKTE

- **Blockchain**
- **Sichere und vertrauenswürdige Cloud-Dienste**
- **Das Internet der Dinge: Ein neues Spielfeld für Malware**
- **Der 7. Sinn im Internet**
- **IT-Sicherheit und KI**
- **Live-Hacking: Sicherheitslücken aufspüren und schließen**

Teilnahmegebühren (inkl. MwSt.):

Frühbucherticket (bis 30. April 2018): 135,00 Euro

Standardticket: 159,00 Euro

Goldsponsoren: Capgemini, cio Solutions, netwrix, panda

Silbersponsoren: BOMGAR, DB

Organisiert von: heise Events

in Zusammenarbeit mit: if(is) internet-sicherheit.

www.heise-events.de/it-sicherheitstag-rhein-ruhr