RUHR-UNIVERSITÄT BOCHUM

RUB

# RUBinform

Datenschutz & Datensicherheit

Newsletter 02|18

**IN DIESER AUSGABE:**



**LINKS ZU DEN BEITRÄGEN:**

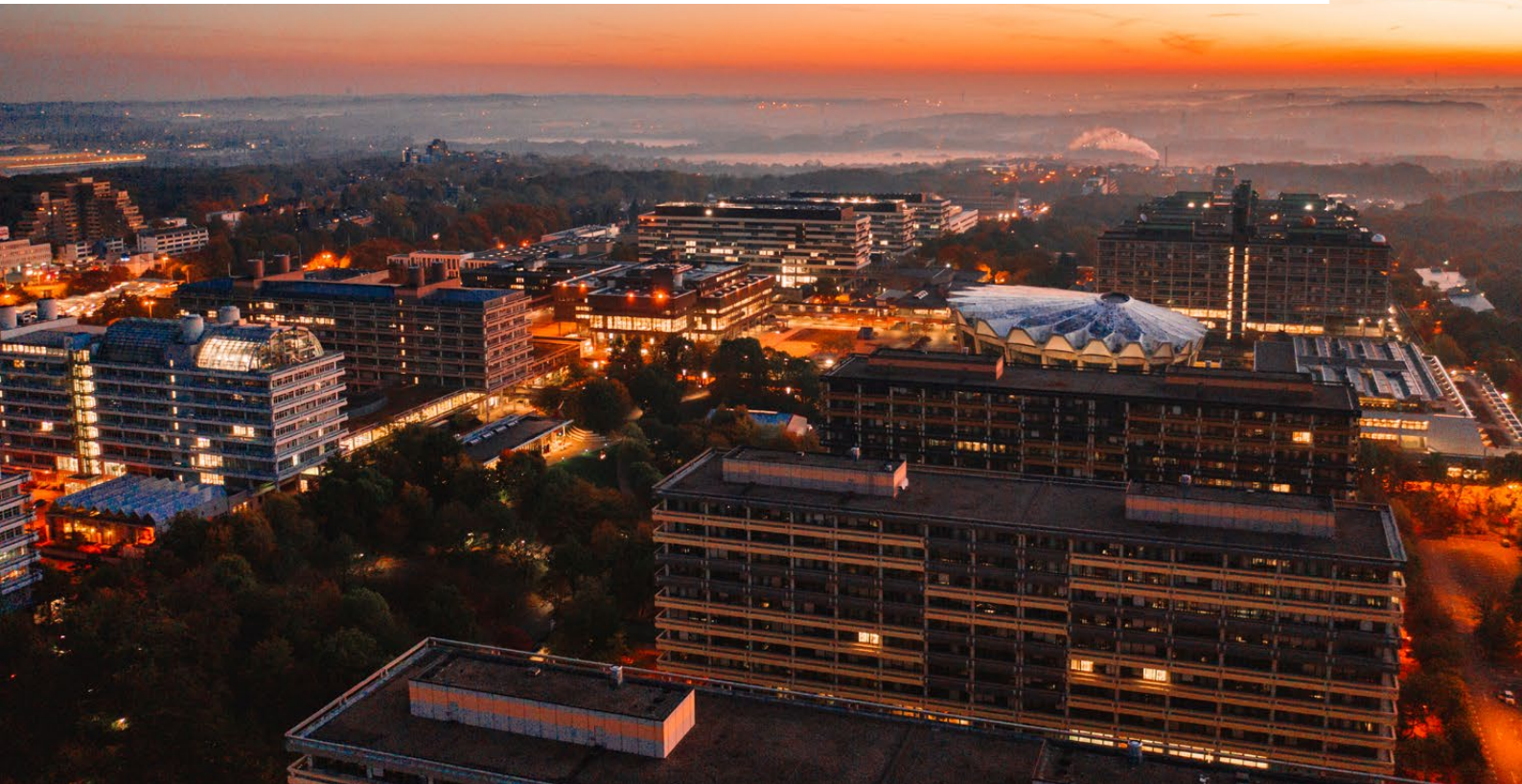
*www.rub.de/rubinform*

## ZUALLERERST

Liebe Leserinnen und Leser,
was für ein herrlicher Anblick zeigt sich auf dem Titelbild! So schön kann unsere Uni sein. Naja, wenn doch nur … Ein Jahr geht zu Ende und dieser Teilsatz provoziert viele Assoziationen. Wünsche und Klagen kommen in den Sinn: wenn man doch nur in Ruhe arbeiten könnte, wenn doch Märchen wahr würden, wenn doch nur nicht die Qual mit der DS-GVO wäre und dieser nervtötende Baulärm aufhörte. Gut – man muss wirklich ein unverbesserlicher Liebhaber sein, wenn man sie trotz aller Widrigkeiten mag, selbst wenn sie vielleicht keine Schönheit ist.

Frohe Festtage

*wünschen die Stabsstelle für Informationssicherheit und der behördliche Datenschutz*



# ECSM – EUROPEAN CYBER SECURITY MONTH

EUROPÄISCHER MONAT DER CYBER-SICHERHEIT

Seit 2012 ist es Tradition geworden, im Oktober den „Europäischen Monat der Cybersicherheit“ zu begehen.

Europaweite Aktionen zielen darauf ab, das Bewusstsein der Bürger für Informationssicherheit zu schärfen. Sie weisen auf die Gefahren hin, die bei einer allzu arglosen Nutzung des Internets entstehen können und zeigen einfache Schritte auf, die jeder zum Schutz persönlicher oder beruflicher Daten unternehmen kann. Die globale Dimension des Projekts hilft dabei, die Aufmerksamkeit und das Interesse zu steigern.

In diesem Jahr hatten sich auch die UA-Ruhr Universitäten Duisburg-Essen und die Ruhr-Universität Bochum gemeinsam mit einer Veranstaltungsreihe an dieser Aktion beteiligt. Unter anderem demonstrierte Prof. Lucas Davi (Lehrstuhl Sichere Softwaresysteme, Duisburg-Essen) in seinem gelungenen, auch für Laien verständlichen Vortrag neue Angriffstechniken, die normale Abwehrmechanismen wie Anti-Virus-Toolkits umgehen. Der Vortrag von Stephan Wallmann (Verfassungsschutz NRW) sensibilisierte dafür, dass Hochschulforschung im Visier ausländischer Nachrichtendienste steht. Die dabei zur Anwendung kommenden Methoden sind sehr ausgefeilt und langfristig angelegt: sie reichen von der Anwerbung und Ausspähung von Mitarbeiterinnen und Mitarbeitern gerade auch über soziale Netzwerke bis zu minutiös recherchierten Spear-Phishing Attacken. Die Veranstaltungsreihe umfasste 5 Vorträge. Diese wurden zum Teil aufgezeichnet. Aufzeichnungen, Folien und viele weitere Informationen sind über die Kampagnenwebseite abrufbar.

**Zugabe**

Am 12. Dezember folgt noch eine Zugabe: Der Klassiker „Hacken für Jedermann“ von und mit Tobias Schrödel (siehe Box). Die Teilnahme an dieser Live-Hacking-Show ist kostenlos, eine Anmeldung über die Kampagnenseite ist jedoch erforderlich. **BW**

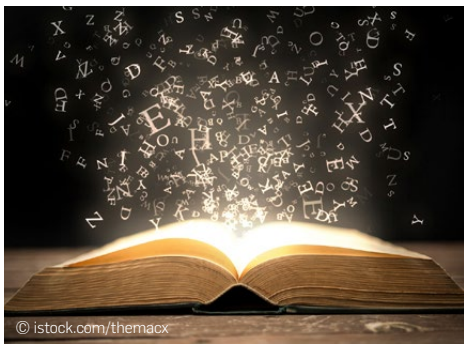
## ZUGABE

**Hacken für Jedermann – IT-Sicherheit einmal anders**

Tobias Schrödel erklärt technische Lücken und Schwachstellen in Systemen und Software für jeden verständlich und lässt dabei auch den Spaß nicht zu kurz kommen. Er ist ein weltweit gefragter Comedyhacker, Computerspezialist und Buchautor. „Hacken für Jedermann“ ist sein Klassiker: eine in über zehn Jahren immer wieder erneuerte und der aktuellen Entwicklung angepasste Live-Hacking-Show. Bei seinem ersten Auftritt an der Ruhr-Universität Bochum verblüffte und verzauberte er damit mehr als 600 begeisterte Zuschauer. Was scheinbar als Vortrag beginnt, wandelt sich binnen kürzester Zeit in eine rasante Show. Lachen und staunen Sie mit: Für Risiken und Nebenwirkungen wird keine Haftung übernommen!

*12. Dezember 2018, 15 c.t., Ruhr-Universität Bochum, HZO 30 Anmeldung erforderlich!*

# DAS MÄRCHEN VOM DATACENTER




Es war einmal eine Universität, die wollte ein Datacenter für ihre IT-Systeme bauen. Dafür glaubte sie, gute Gründe zu haben: Unterhielt sie doch eine Vielzahl von kleinen Serverräumen, deren Kühlung und Stromversorgung aufwändig installiert und teuer unterhalten werden mussten. Selbst der große alte Maschinenraum entsprach nicht mehr den Anforderungen an Verfügbarkeit und Sicherheit, die der Bedeutung ihrer IT-Anwendungen für den täglichen Betrieb gerecht würden. Also sollte ein neues Datacenter her, das alle bislang verteilten IT-Systeme beherbergen und zudem die notwendige Betriebssicherheit bieten sollte.

So geschah es, dass die Universität zu ihrem 49. Geburtstag eine kundige Firma mit der Anfertigung einer Machbarkeitsstudie beauftragte. Zum Ende des Jahres legten die fleißigen Planer eine Ausführungsskizze und eine Kostenschätzung vor. Damit ging die Universität zum Landesherrn, der den Wunsch durch seinen Schatzmeister und den Obersten Bauherrn prüfen ließ. Die Universität war ganz glücklich, als ihr Begehr bewilligt und die erforderlichen Taler bereitgestellt wurden.

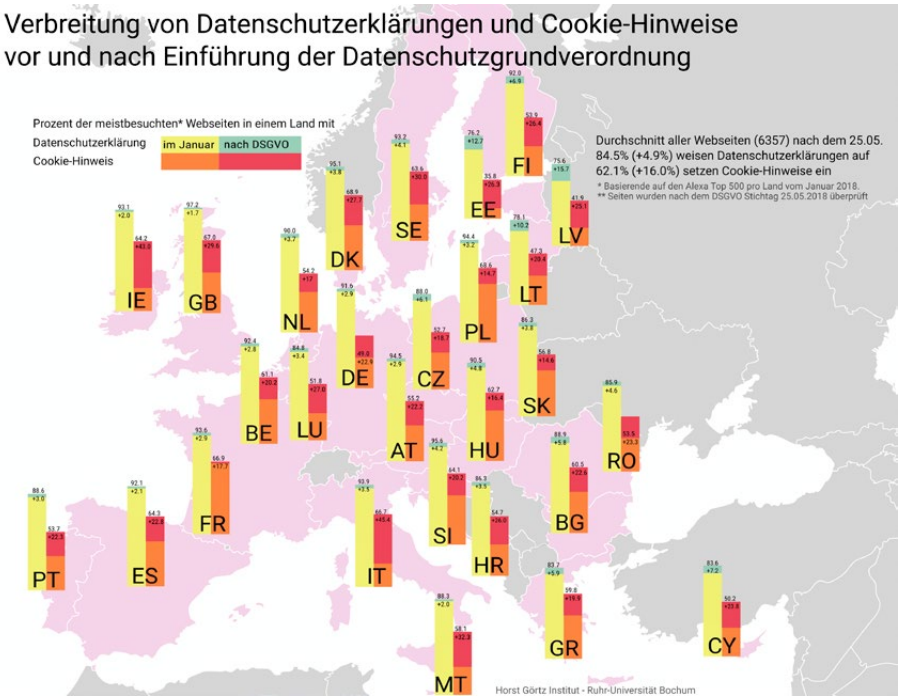
Hierüber war ein weiteres Jahr ins Land gegangen. Der Oberste Bauherr hatte das Begehren noch einmal geprüft. Darauf verlangte er von der Universität nun eine Zusicherung, dass sie unvorhergesehene Ausgaben auch über die vom Landesherrn bewilligten Taler hinaus begleichen werde. Das wollte die Universität nicht akzeptieren. Schließlich kam man überein, Umfang und Art des Begehrs gemeinsam abzustimmen und sich erst dann über den fälligen Tribut zu einigen.

Nach vielen gemeinsamen Treffen beschloss man so im 52. Jahr des Bestehens der Universität einen einvernehmlichen Plan für das Datacenter, der den Vorgaben des Landesherrn entsprach. Die Freude währte aber nur kurz, denn der Oberste Bauherr verlangte nun eine Zusicherung, dass die Universität ihm jeglichen Aufwand ersetzen werde, falls das neue Gebäude aus irgendeinem Grund nicht fertiggestellt werde. Das verstand die Universität nun gar nicht: Waren sie doch Bedienstete des gleichen Landesherrn! Warum sollte sie dem Bauherrn vergeblichen Aufwand ersetzen, auch wenn sie daran gar nicht schuld war?

Und so warten die Universität und der Oberste Bauherr bis heute auf eine Eingebung zur Lösung des Problems. Die Universität, die nicht mehr weiß, wo sie ihre IT unterbringen soll, hat derweil die Planung eines Interims aufgenommen.

AUFGESCHRIEBEN IM NOVEMBER 2018, RAINER **WOJCIESZYNSKI**

# „DIESE SEITE VERWENDET COOKIES…“




Im Zuge der Einführung der Datenschutzgrundverordnung (DS-GVO) im Mai 2018 wurde viel über die neuen Datenschutzregeln berichtet. Ob und was sich tatsächlich geändert hat, haben Forscher*innen der RUB zusammen mit der University of Michigan untersucht. Über einen Zeitraum von sechs Monaten haben sie mehr als 6500 der meistbesuchten Webseiten der 28 EU-Staaten vor und nach dem 25.5.2018 untersucht. Im Fokus stand dabei die Verfügbarkeit von Datenschutzerklärungen und Cookie-Hinweisen, aber auch, ob technische Mindeststandards wie verschlüsselte Übertragung mit HTTPS umgesetzt wurden.

Bei rund 74 % der untersuchten Seiten wurde die Datenschutzerklärung, trotz eines zweijährigen Übergangszeitraumes, erst kurz vor oder am Stichtag selbst angepasst. „Die Analyse zeigt zudem, dass in einigen Ländern ein Teil der Internetpräsenzen gar keine derartige Erklärung besaß – sie wurde erst vor Inkrafttreten der DS-GVO integriert. Letztlich können heute rund 85 % der von uns analysierten Webseiten eine Datenschutzerklärung vorweisen“, berichtet Martin Degeling vom Horst-Görtz Institut für IT-Sicherheit.

Einen Hinweis auf den Einsatz von Cookies hatten nach dem Stichtag 62 % der untersuchten Seiten – ein Anstieg von 16 Prozentpunkten im Gegensatz zum Januar 2018. Aber nicht nur die Zahl der Hinweise ist gestiegen, sondern auch die Qualität. Waren im Januar Cookie-Hinweise vorwiegend reine Informationsbanner ohne jegliche Interaktionsmöglichkeiten, bieten sie heute auch Entscheidungsmöglichkeiten für Nutzerinnen und Nutzer. Teilweise können bestimmte Funktionen wie personalisierte Werbung oder die Weitergabe von Informationen an Soziale Netzwerke deaktiviert werden. Bei einer genauen Analyse der technischen Umsetzung zeigten viele Seiten allerdings Schwächen.

Die Datenschutzgrundverordnung hat in Bezug auf Transparenz über die Datensammlungen positive Effekte. An echten, funktionierenden und auch für Nicht-Expert*innen verwendbaren Einwilligungsmechanismen mangelt es aber noch. Wie diese gestaltet werden können, wollen die Forscher*innen in einer anschließenden Studie untersuchen.

Die Forscher*innen werden ihre Ergebnisse auf der NDSS Konferenz 2019 in San Diego, USA vorstellen. Ein Vorabdruck der Studie ist online verfügbar.

DR. MARTIN **DEGELING,** CHRISTOPHER **LENTZSCH**

*Degeling, M.; Utz, C.; Lentzsch, C.; Hosseini, H.; Schaub, F. & Holz, T. We Value Your Privacy … Now Take Some Cookies: Measuring the GDPR‘s Impact on Web Privacy (https://arxiv.org/abs/1808.05096) 2018*

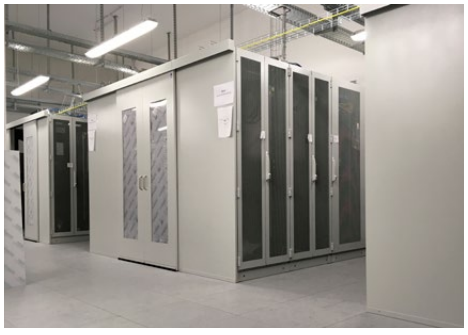
# **INTERIM** FÜR DIE IT

Zum Jahreswechsel 2018/19 müssen im Rahmen der Campussanierung die NA- und GC-Gebäude geräumt werden. Als Mitte 2017 offensichtlich wurde, dass der Datacenter-Neubau nicht rechtzeitig fertiggestellt wird, hat das Datacenter-Team die Planung eines Interims für die Unterbringung der vom Umzug betroffenen IT-Systeme aufgenommen.

Nach einer Bestandsaufnahme der Hardware und der verfügbaren Serverräume wurden zwei bestehende und ein Neubau-Serverraum in GD als geeignet für das Interim lokalisiert. In allen Räumen waren umfangreiche Infrastrukturertüchtigungen vonnöten. Zur Unterbringung der zentralen IT in einem Bestands-Serverraum mussten die Kapazität der Notstromversorgung und die Backbone-Anbindung des Datennetzes erweitert werden. Zusätzlich wurden Serverracks mit autarker Klimatisierung beschafft und vernetzt sowie der Serverraum mit einer Alarmanlage ausgestattet. Ein erster Meilenstein war erreicht, als im August 2018 der Großteil der zentralen IT an den neuen Installationsort umgezogen wurde – ohne Störungen für den IT-Betrieb! Anschließend wurde noch die Klimaüberwachung fernadministrierbar eingerichtet.

Für den Neubau-Serverraum war ein neues Nutzungskonzept erforderlich und mit der Baufirma abzustimmen: Die Verwendung als Interim bringt eine erhöhte Nutzung mit sich, so dass die Zahl der Stromzuleitungen erhöht und die Klimatisierung effizienter gestaltet werden mussten. Zudem waren Baumängel zu beseitigen. Als wesentlich erwies sich der Austausch der falsch gelieferten Klimageräte, der sich bis Ende November hinzog. Der Raum wurde mit 37 Serverracks in Kaltgangeinhausung und intelligenten PDUs ausgestattet. Die Datenvernetzung erfolgte betriebsfertig mit IP-Steckports in jedem Rack. Schließlich stand noch die Umzugsplanung mit Zuweisung der Installationsplätze für jedes betroffene IT-System an, so dass der Umzug ab Dezember starten kann.

Der zweite Bestands-Serverraum verfügt über zu wenige Stromzuleitungen, um den vorhandenen Stellplatz auszunutzen. Hierfür ist eine Ertüchtigung um zusätzliche Leitungen beauftragt. Zudem wurde ein Teil des Serverraums für den gesicherten Betrieb sensibler IT-Anwendungen abgeteilt.



Die damit geschaffenen IT-Stellplätze bieten Platz für die Unterbringung der vom Umzug 2018 betroffenen IT-Systeme. Vor der nächsten Umzugswelle bei Sanierung der NB- und GB-Gebäude bzw. auch bei Neubeschaffung von wassergekühlten IT-Hochleistungssystemen muss unbedingt das neue Datacenter verfügbar sein!

RAINER **WOJCIESZYNSKI**

# DIE RUB UND **DIE DS-GVO**


In den Medien war es kaum zu übersehen. Ob in Gremien oder an den Stammtischen – die Diskussionen kochten hoch und tun dies noch immer: seit dem 25. Mai gilt die Datenschutz-Grundverordnung (DS-GVO) – trotz zweijähriger Übergangszeit war nicht jeder gut vorbereitet. Auch wenn die DS-GVO in ihren Grundzügen stark an den deutschen Datenschutz angelehnt wurde, brachte sie zahlreiche Neuerungen mit sich. Zur Steigerung der Transparenz und Sicherheit erlegt die DS-GVO allen verarbeitenden Stellen umfangreiche Informations- und Dokumentationspflichten auf. Um diese neuen Aufgaben möglichst einheitlich und effektiv zu meistern, hat unsere Kanzlerin die Stabsstelle für Informationssicherheit mit der Durchführung eines Pilot-Projekts beauftragt.

### Pilot-Projekt

Es soll insbesondere eine sinnvolle Vorgehensweise zur Unterstützung der Einrichtungen entwickelt werden. Das Projekt wird in der Fakultät für Sportwissenschaft und dem Dezernat Personal und Recht durchgeführt. Verarbeitungen personenbezogener Daten werden erfasst und nach den Vorgaben der DS-GVO entweder als Standardverfahren dokumentiert oder sie dienen als Vorlage für spezielle Verarbeitungen in den Einrichtungen. Um geeignete Sicherheitsmaßnahmen zu definieren, werden Checklisten und Handlungsempfehlungen erarbeitet.

Neben der Dokumentation der Verarbeitungen müssen verantwortliche Stellen Betroffene über die Verarbeitung ihrer personenbezogenen Daten und ihre diesbezüglichen Rechte informieren. Dazu sind Datenschutzerklärungen auf allen Webseiten, Formularen oder Verträgen zur Verfügung zu stellen. Die für zentrale Webseiten bereitgestellte Datenschutzerklärung müssen Einrichtungen für ihre Belange anpassen – in Abhängigkeit von Art und Umfang der jeweils verarbeiteten Daten und eingesetzten Technologien.

Die Etablierung von Meldungen von Datenpannen, Abwicklung von Auskunftsersuchen, Konformitätsprüfungen bestehender Dokumente und Verfahren sowie Datenschutzfolgeabschätzungen bleiben weitere Herausforderungen.

### Meldepflicht bei Datenpannen

Datenpannen sind Unregelmäßigkeiten in der Verarbeitung personenbezogener Daten, die zu einem Risiko für Betroffene führen, z.B. der Verlust von USB-Sticks, Smart-Phones, Notebooks oder Akten, die personenbezogene Daten enthalten. Auch der falsch adressierte Versand per Briefpost oder E-Mail oder ein mit Schadsoftware infizierter Rechner gelten als Datenpannen, sobald personenbezogene Daten Anderer betroffen sind.

Die DS-GVO schreibt die Meldung von Datenschutzverletzungen binnen 72 Stunden vor. Wer vermutet oder weiß, dass personenbezogene Daten unrechtmäßig offengelegt oder verarbeitet wurden, oder ein Risiko dazu besteht, ist verpflichtet, den Vorfall zu melden. Für die Annahme und Bearbeitung von Meldungen an der RUB sind die Beauftragte für Informationssicherheit und der Datenschutzbeauftragte zuständig. Sie tragen Sorge für die fristgerechte Meldung an die Aufsichtsbehörde und veranlassen die notwendigen Maßnahmen.

Die RUB betreffende Datenpannen können per E-Mail an datenpanne@rub.de gemeldet werden. Weitere, auch anonyme oder verschlüsselte Kontaktwege sind auf unserer Webseite www.itsb.rub.de/themen/datenpanne.html beschrieben. BS

## BITS

**Warnmeldungen**

Spam-Wellen rollen fast täglich über die RUB. Aktivierte Spam-Filterung, umsichtiges Handeln und gesunder Menschenverstand bewirken in der Regel, dass Nutzer darauf nicht reinfallen. Dringende Warnungen zu akuten Sicherheitsbedrohungen, die wir von Sicherheitsteams, Behörden oder auch RUB-internen Analysetools erhalten, werden jetzt auch über das Portal Nutzungseinschränkungen weitergegeben. Über neue Meldungen können Sie sich automatisch benachrichtigen lassen.
Regelmäßig erreichen uns auch Informationen zu gekaperten Zugangsdaten unserer Nutzer, die im Internet veröffentlicht oder verkauft werden. Die Betroffenen werden in solchen Fällen von uns direkt benachrichtigt.

**Keine Abmahnwellen, aber Tricksereien**

Mit Anwendungsbeginn der Datenschutzgrundverordnung im Mai wurde eine Abmahnwelle befürchtet. Diese ist wohl zumindest bisher ausgeblieben. Stattdessen flatterte vielen Unternehmen und Organisationen aber Anfang Oktober ein Schreiben der „Datenschutzauskunft-Zentrale“ ins Haus. Das offiziell aussehende Schreiben nutzte geschickt den Zeitdruck rund um Feiertage, versteckte Aussagen im Kleingedruckten und die allgemeine Verunsicherung bezüglich der DS-GVO. So sollten Kunden ein Abonnement mit langer Laufzeit, hohen Kosten und zweifelhaftem Nutzen abschließen. Es ist leider zu erwarten, dass die Masche Nachahmer findet. Daher: bevor auf offiziell aussehende Schreiben geantwortet wird, sollte man sich immer rückversichern. Erster Ansprechpartner an der RUB ist da meist das Justitiariat. Das Aufbauen von Zeitdruck ist Teil des Handwerks, sowohl der Abmahnindustrie als auch der Abofallen.




**HERAUSGEBER** Dr. Kai-Uwe Loser (v.i.S.d.P.), KUL, Behördlicher Datenschutzbeauftragter der RUB (bDSB); Brigitte Wojcieszynski (v.i.S.d.P.), BW, Beauftragte für Informationssicherheit der RUB (ITSB); Birgit Steiner, BS, stellv. Beauftragte für Informationssicherheit der RUB (ITSB); Anschrift: Ruhr-Universität Bochum, Geschäftszimmer Stabsstelle Informationssicherheit, NAFOF 03/252, Kerstin Bussmann, 44780 Bochum, Telefon: 0234/32-24888, E-Mail: rubinform@rub.de; Infos: www.rub.de/rubinform; Titelbild: ©RUB, Kramer