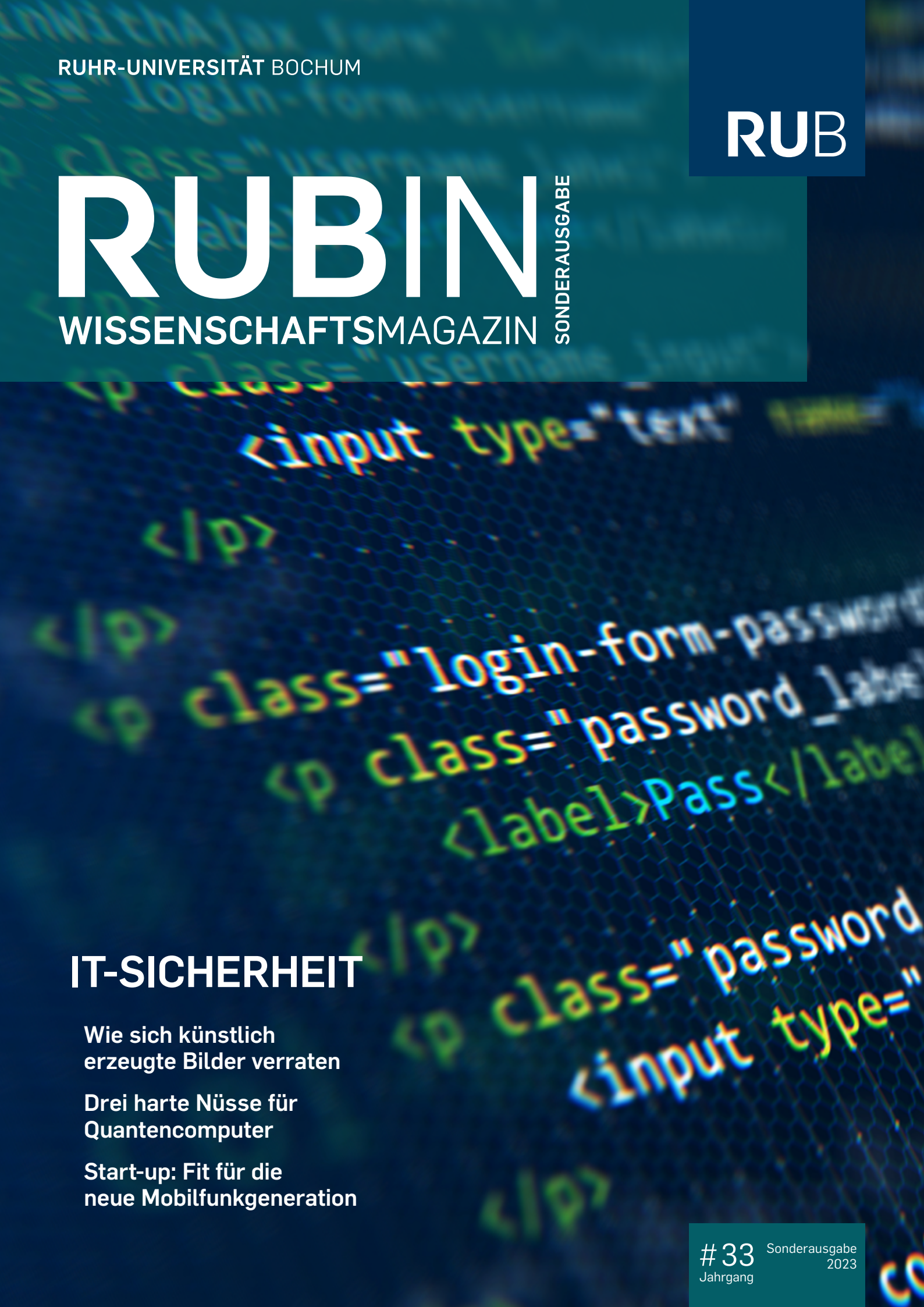
RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

SONDERAUSGABE



IT-SICHERHEIT

Wie sich künstlich erzeugte Bilder verraten

Drei harte Nüsse für Quantencomputer

Start-up: Fit für die neue Mobilfunkgeneration

#33 Jahrgang

Sonderausgabe 2023

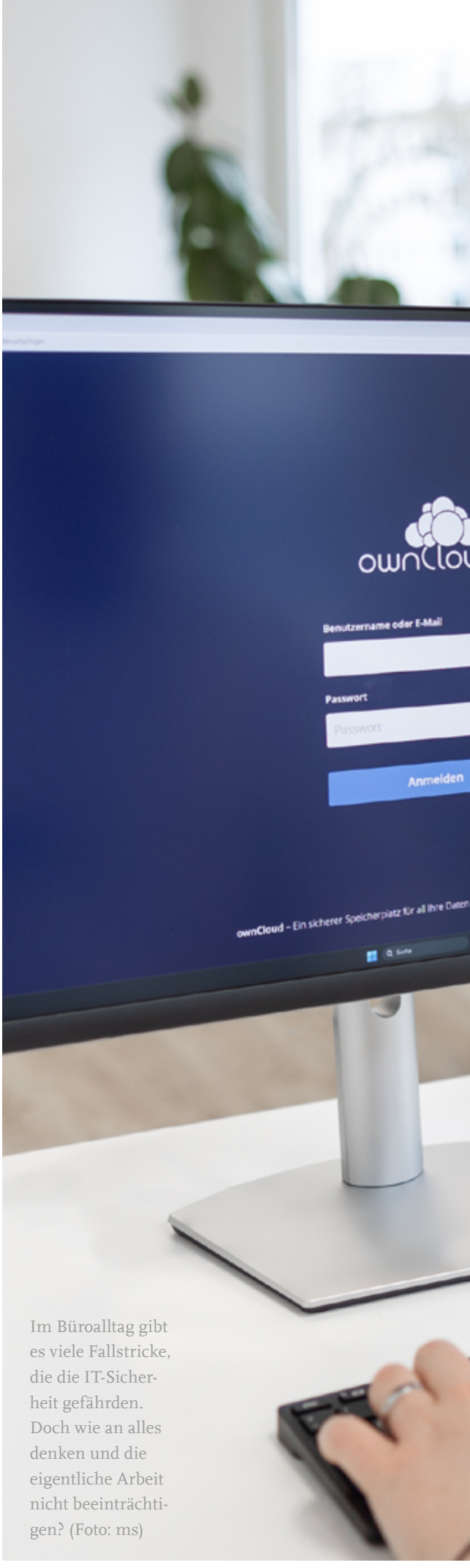
WIE MAN **IT-SICHERHEIT UND PRODUK-TIVITÄT** UNTER EINEN HUT BEKOMMT

Uta Menges und Jonas Hielscher wollen IT-Sicherheitsmaßnahmen aus der nervigen Ecke herausholen und besser in den Alltag bringen.

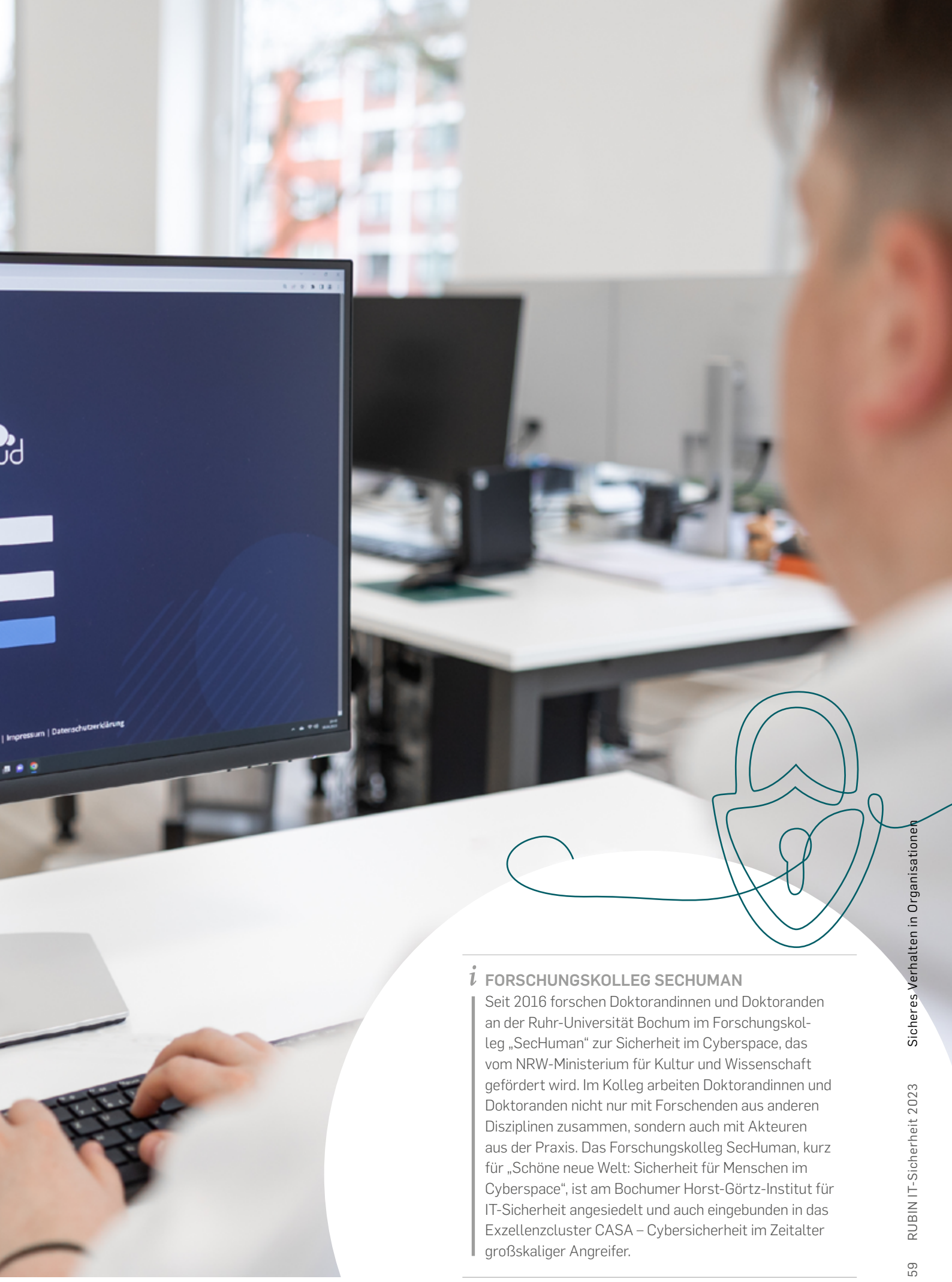
IT-Sicherheit – bei der Vokabel verdrehen viele innerlich gleich die Augen. Natürlich ist allen klar, dass das Thema wichtig ist. Die spektakulären Angriffe auf IT-Systeme von Organisationen in den vergangenen Jahren sind beängstigend, ganze Universitäten oder Stadtverwaltungen waren teils wochenlang vom Netz. Und die gelungenen Angriffe sind nur die Spitze des Eisbergs, denn versuchte Angriffe sind an der Tagesordnung. Aber was tun Unternehmen und Organisationen dafür, dass ihre IT sicher ist? Letztlich muss jede und jeder Einzelne diese Sicherheit mittragen – warum klappt das nicht gut und wie könnte es klappen?

Diese Frage treibt Uta Menges und Jonas Hielscher um. Die beiden bilden ein Tandem im Forschungskolleg SecHuman – Sicherheit für Menschen in Cyberspace. Gemeinsam arbeiten sie hier an ihrer Doktorarbeit. Dabei könnten ihre fachlichen Hintergründe kaum unterschiedlicher sein. Während Jonas Hielscher in Magdeburg Informatik studiert hat, ist Uta Menges studierte Wirtschaftspsychologin. Ihren Master hat sie in der Ehe-, Familien- und Lebensberatung absolviert und auf diesem Gebiet auch gearbeitet. Wie passt das zusammen?

„Das geht erstaunlich gut zusammen“, sagt sie. „Ich kann das dort Gelernte prima auf den Bereich der IT-Sicherheit übertragen.“ Denn im Fokus steht auf beiden Gebieten der Mensch. „Die technischen Maßnahmen für die Sicherheit eines IT-Systems können noch so gut sein – ohne die Mit- ▸



Im Büroalltag gibt es viele Fallstricke, die die IT-Sicherheit gefährden. Doch wie an alles denken und die eigentliche Arbeit nicht beeinträchtigen? (Foto: ms)



FORSCHUNGSKOLLEG SECHUMAN

Seit 2016 forschen Doktorandinnen und Doktoranden an der Ruhr-Universität Bochum im Forschungskolleg „SecHuman“ zur Sicherheit im Cyberspace, das vom NRW-Ministerium für Kultur und Wissenschaft gefördert wird. Im Kolleg arbeiten Doktorandinnen und Doktoranden nicht nur mit Forschenden aus anderen Disziplinen zusammen, sondern auch mit Akteuren aus der Praxis. Das Forschungskolleg SecHuman, kurz für „Schöne neue Welt: Sicherheit für Menschen im Cyberspace“, ist am Bochumer Horst-Görtz-Institut für IT-Sicherheit angesiedelt und auch eingebunden in das Exzellenzcluster CASA – Cybersicherheit im Zeitalter großskaliger Angreifer.

Jonas Hielscher (links) und Uta Menges wollen wissen, wie sich IT-Sicherheit so in den Arbeitsalltag integrieren lässt, dass sie nicht hinderlich ist. (Foto: CASA, Caroline Schreer)

> „DAS SCHAFFT IN EINEM NORMALEN ARBEITSTAG KEIN MENSCH."
>
> Uta Menges

arbeit der Nutzenden funktionieren sie nicht“, sagt auch Jonas Hielscher. Aber wie man Organisationen dazu bringt, ihre Mitarbeitenden bei der Umstellung zu sicherem Verhalten zu unterstützen und nicht alle Last einfach bei den Endnutzer*innen abzuladen, dazu sind die Forschungsergebnisse bislang rar. Und mit der Praxis sind Menges und Hielscher auch nicht sehr glücklich. „Viele Firmen beauftragen Anbieter zum Beispiel damit, gefakte Phishingmails an ihre Mitarbeitenden zu senden, um das Team für Angriffe zu sensibilisieren“, erzählt Jonas Hielscher. „Aber solche einmaligen und eindimensionalen Maßnahmen bringen nicht viel.“ Im Zweifel hat jemand, der drauf hereingefallen ist, das Gefühl, den Schwarzen Peter zu haben. Damit ist niemandem geholfen.

Die beiden Forschenden stellen ganz andere Fragen: Wie machbar ist IT-Sicherheit für Mitarbeitende eigentlich? Wissen die Mitarbeitenden genau, was sie zu tun haben? Lassen sich Maßnahmen wirklich umsetzen oder ist dafür im Arbeitsalltag gar keine Zeit? Stehen die IT-Sicherheitsmaßgaben in Konkurrenz mit Dingen, die zu erledigen sind? „Stichwort: Lesen Sie jede Mail ganz genau und prüfen Sie sie auf Indizien für einen Phishing-Angriff“, gibt Uta Menges ein Beispiel. „Das schafft in einem normalen Arbeitstag kein Mensch.“

Neben solchen Fragen, die unter dem Begriff „productive security“ zusammengefasst sind, fassen die beiden Promovierenden auch die Kommunikation über IT-Sicherheit ins Auge. Wie reden die Leute darüber? Die Macher sind oft Ingenieure. Sie sprechen über Technik und holen die nicht technisch versierten Kolleginnen und Kollegen damit nicht ab. Diese kommunikative Hürde führt zu Missverständnissen und trägt nicht zu einem vertrauensvollen Miteinander bei. Genau das halten die Forschenden aber für unverzichtbar. „Wenn jemand eine Phishingmail geöffnet hat und in die Falle getappt ist, darf er oder sie keine Angst haben, diesen Vorfall zu melden“, sagt Uta Menges. „Und es muss klar sein, bei wem.“ Sie fordert eine gute Fehlerkultur: Niemand darf an den Pranger gestellt werden, weil er oder sie einen Fehler gemacht hat. Es braucht klare Anweisungen. Allzu oft würden Mitarbeitende aber mit unklaren Regelungen allein gelassen. Zur Kommunikation gehört auch die Antwort eines Helpdesks. Ist sie unpersönlich, bleibt IT-Sicherheit abstrakt.

Kommunikationsprobleme stellen die beiden auch zwischen IT-Sicherheitsprofis und dem Management von Institutionen fest. „Profis wollen über Produkte reden. Für das Management ist das Risiko viel interessanter, das es einzudämmen gilt. Aber dafür, wie sicher oder unsicher sich Mitarbeitende verhalten, gibt es bisher kein Maß“, erklärt Jonas Hielscher. Er und Uta Menges wagen sich auf ein weitgehend unerforschtes Terrain. „Man müsste die Leute befragen, ihr Verhalten beobachten, ihr Feedback einholen, Vorfälle auswerten. Aber das ist alles noch nicht gemacht worden, auch weil es so kompliziert ist“, sagt er.

Auf Basis ihrer Expertise als Psychologin unterstreicht Uta Menges: Soll IT-Sicherheit in Organisationen gelingen, ist vor allem die Selbstwirksamkeitserwartung der Menschen wichtig. Mit anderen Worten: IT-Sicherheit muss zu bewältigen sein. Und sie muss wirken. „Das klingt vielleicht selbstverständlich, aber das jahrzehntealte Narrativ, dass alles ohnehin immer schlimmer wird und man sowieso nichts machen kann, steckt in vielen Köpfen“, sagt Uta Menges. „Wer das verinnerlicht hat, hat es schwer, Maßnahmen zu ergreifen, weil er nicht an sie glaubt.“

Mit verschiedenen Praxispartnern tasten sich Uta Menges und Jonas Hielscher an das Thema heran. Gemeinsam mit einem großen Industrieunternehmen aus Nordrhein-Westfalen bilden sie über ein Dutzend aktueller Auszubildener zu Botschaftern für IT-Sicherheit aus. Sie haben den Chief Information Security Officer kennengelernt und seine Handynummer bekommen. Ziel ist es, ein Netzwerk zu schaffen über die vielen Standorte des Unternehmens mit über 20.000 Mitarbeitenden hinweg. So soll IT-Sicherheit ein Gesicht bekommen. Seit November 2021 stehen die beiden in Kontakt mit einer Gruppe von 28 schweizerischen Chief Information Officers von verschiedenen Firmen. Sie gestalten hier unter anderem Workshopinhalte mit und bleiben auf dem Laufenden über Alltagsprobleme in den Unternehmen.

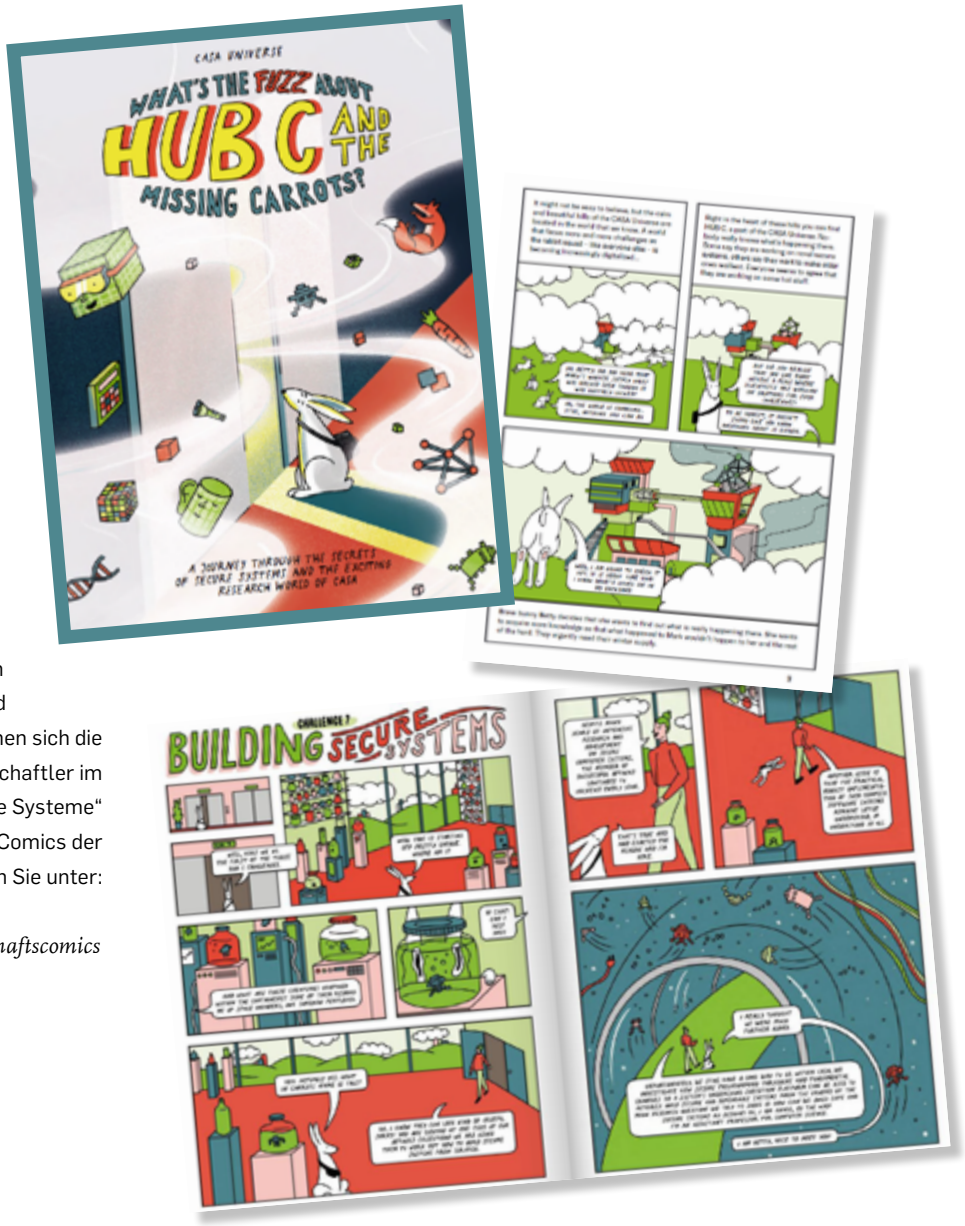
„Diese Doktorarbeit entwickelt sich erst, während wir sie erarbeiten“, sagt Jonas Hielscher. Beide sind jedoch fasziniert von ihrem Forschungsfeld. „Es ist Pionierarbeit und nicht planbar – es sind halt Menschen, die im Mittelpunkt stehen“, sagt Uta Menges. Forschungsfragen drängen sich noch jede Menge auf. Das Forschungsfeld Human Centered Security ist noch jung, erst um 2000 herum kam das Thema auf. „Aber es werden immer mehr Professuren, es ist ein wachsendes Feld“, freut sich Jonas Hielscher. „Und unsere Ergebnisse werden sicher nicht auf taube Ohren stoßen.“

md

i SCHÄDEN DURCH IT-ANGRIFFE

Wie groß der wirtschaftliche Schaden durch IT-Angriffe ist, kann niemand genau beziffern, da es in Deutschland für solche Vorfälle keine Meldepflicht gibt. Die vom Branchenverband Bitcom veröffentlichte Zahl, die sich auf rund sechs Prozent des Bruttoinlandsprodukts beläuft, ist daher auch nur eine Schätzung, die Jonas Hielscher für zu hoch hält.
Ransomware-Angriffe, bei denen IT-Systeme von außen verschlüsselt werden, um ein Lösegeld zu erpressen, treffen oft mittlere Unternehmen, deren Schutz häufig unzureichend ist.

REDAKTIONSSCHLUSS



Die Hasen im CASA Universe sind aufgeschreckt: Der scheinbar gut gesicherte Zugang zum Karottenvorrat von Hase Mark wurde gehackt und alle Wintervorräte geraubt. Die mutige Häsin Betty macht sich daraufhin auf die Suche nach Unterstützung im nahegelegenen CASA Hub C – einem geheimnisvollen Ort, der Lösungen für digitale Sicherheit bereithalten soll. So beginnt das Abenteuer von Häsin Betty, der Protagonistin des ersten Wissenschaftscomics des Exzellenzclusters CASA. Gemeinsam mit Betty lernen die Leserinnen und Leser bei ihrem Streifzug durch den Research Hub die Forschungsschwerpunkte und Herausforderungen kennen, mit denen sich die Wissenschaftlerinnen und Wissenschaftler im Forschungsbereich Hub C „Sichere Systeme" tagtäglich beschäftigen. Wie Sie alle Comics der Reihe kostenlos lesen können, erfahren Sie unter:

↗ *casa.rub.de/outreach/wissenschaftscomics*

Auflösung
DEEPFAKE-QUIZ
Folgende Gesichter sind echt:
1a, 2a, 3b, 4a, 5b, 6a

IMPRESSUM

HERAUSGEBER: Exzellenzcluster CASA und Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation der Ruhr-Universität Bochum (Hubert Hundt, v.i.S.d.P.)

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de, news.rub.de/rubin

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Lisa Bischoff (lb)

FOTOGRAFIE: Michael Schwettmann (ms), Dammstr. 6, 44892 Bochum, Tel.: 0177/3443543, info@michaelschwettmann.de, www.michaelschwettmann.de

COVER: Sashkin – stock.adobe.com

BILDNACHWEISE INHALTSVERZEICHNIS: Michael Schwettmann

GRAFIK, ILLUSTRATION, LAYOUT UND SATZ:
Agentur für Markenkommunikation, Ruhr-Universität Bochum,
www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation

DRUCK: LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, Tel.: 0231/90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

AUFLAGE: 4.700

BEZUG: Die reguläre Ausgabe von Rubin erscheint zweimal jährlich und ist erhältlich im Dezernat Hochschulkommunikation der Ruhr-Universität Bochum. Das Heft kann kostenlos abonniert werden unter news.rub.de/rubin. Das Abonnement kann per E-Mail an rubin@rub.de gekündigt werden. Die Sonderausgabe 2023 ist erhältlich beim Horst-Görtz-Institut für IT-Sicherheit. Interessierte können sich per E-Mail an hgi-presse@rub.de melden.

ISSN: 0942-6639