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

WENN DIE **HARDWARE** DIE **TÄTER** ERTAPPT

Hardware vor Manipulationen zu schützen ist bislang eine mühsame Angelegenheit – teuer und nur in kleinem Maßstab möglich. Der Einsatz von Antennen könnte das ändern.

Bezahlvorgänge, Geschäftsgeheimnisse, Dokumente, die für die nationale Sicherheit bedeutsam sind: Die großen Geheimnisse der Welt sind heute oft nicht mehr auf Papier gespeichert, sondern als Einsen und Nullen im virtuellen Raum. Wenn man sie in Gefahr wähnt, stellt man sich zumeist eine Bedrohung aus der Ferne vor – Angreiferinnen und Angreifer, die über Cyberattacken versuchen, vertrauliche Daten zu erbeuten. Aber es gibt auch noch eine andere Bedrohung, einen viel direkteren Weg, in fremde Systeme zu gelangen: nämlich indem man sich an der Hardware zu schaffen macht. Die wertvollen Informationen sind letztendlich nichts anderes als elektrische Ströme, die zwischen verschiedenen Computer-Bauteilen über Leiterbahnen wandern. Ein winziger metallischer Gegenstand, an der richtigen Stelle der Hardware platziert, kann ausreichen, um diese Datenströme abzugreifen. „Betrüger haben diese einfache Methode zum Beispiel genutzt, um Kreditkartendaten aus Kartenlesegeräten abzugreifen“, wissen Paul Staat und Johannes Tobisch. Die beiden promovieren am Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum und forschen am Bochumer Max-Planck-Institut für Sicherheit und Privatsphäre. Im Team von Prof. Dr. Christof Paar entwickeln sie Methoden, die vor Hardware-Manipulationen schützen sollen. Dabei kooperieren sie mit Prof. Dr. Christian Zenger von dem aus der Ruhr-Universität ausgegründeten Unternehmen PHYSEC, der zu seiner Zeit als Forscher die Grundlagen für diese Technik legte und seit kurzem Juniorprofessor an der Fakultät für Elektrotechnik und Informationstechnik ist.

Natürlich gibt es bereits Mechanismen, die Hardware vor Manipulationen schützen soll. „In der Regel ist das eine Art Folie mit dünnen Drähten, in die die Hardware-Komponente eingepackt ist“, erklärt Paul Staat. „Wird die Folie beschädigt, schlägt das System Alarm.“ Auf diese Weise lassen sich allerdings nur kleine Komponenten schützen, nicht das ganze System. Man kann also nicht ein ganzes Computergehäuse in die Folie einwickeln, sondern zum Beispiel nur ein besonders wichtiges Bauteil wie ein Speicherelement oder einen Prozessor. Tobisch und Staat feilen jedoch an einer Technik, die ganze Systeme auf Manipulationen überwachen soll – und obendrein nicht so teuer wäre.

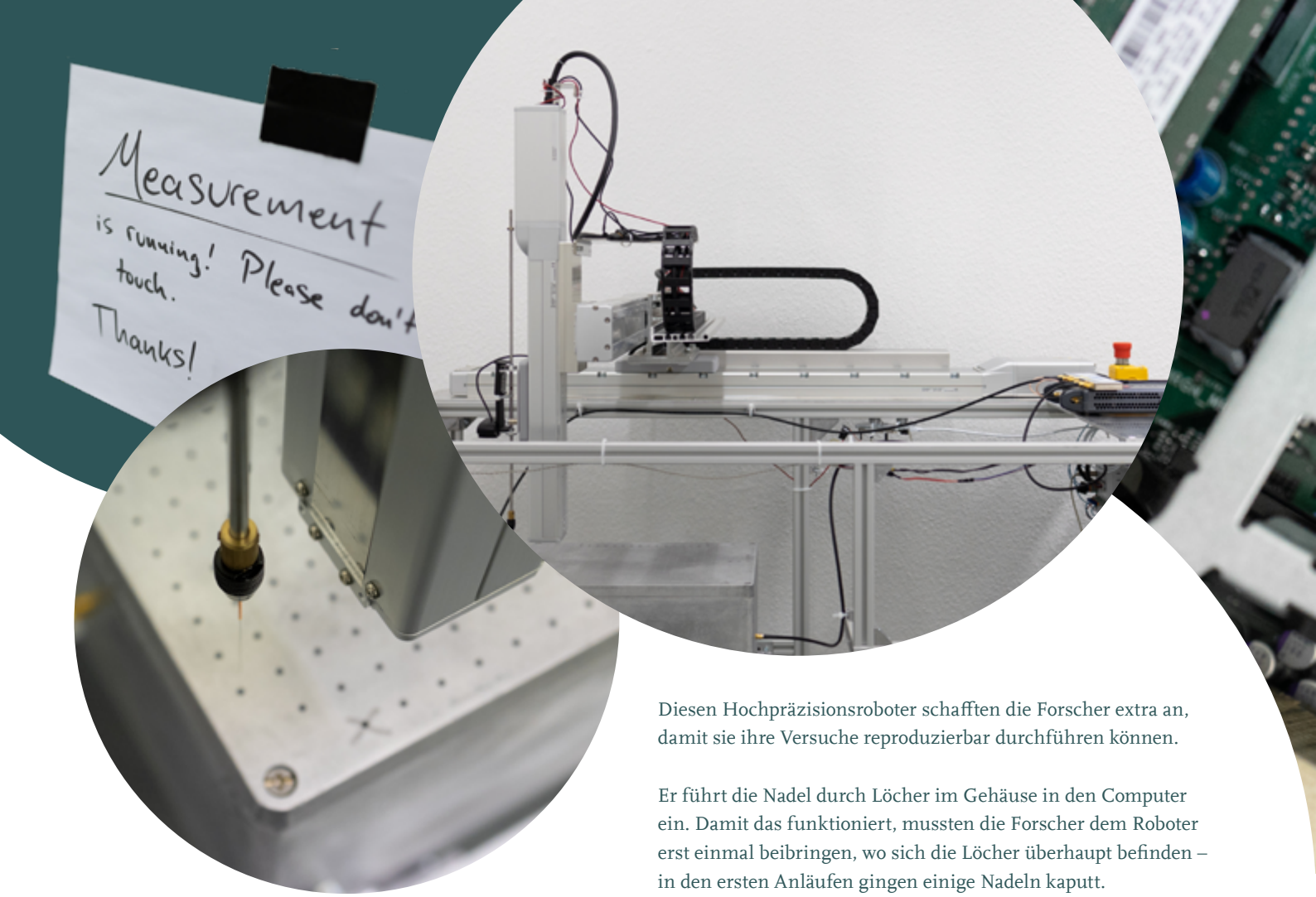
Dazu setzen sie auf Funkwellen. Sie verbauen in dem zu überwachenden System zwei Antennen: einen Sender und ei- ▸

Paul Staat (links) und Johannes Tobisch promovieren an der Ruhr-Universität und forschen am Bochumer Max-Planck-Institut für Sicherheit und Privatsphäre.

i MANIPULIERTE LESEGERÄTE

Forschende aus Cambridge haben schon 2008 gezeigt, wie leicht sich verschiedene Kartenlesegeräte manipulieren lassen – und das, obwohl die Hersteller sogar einen Manipulationsschutz eingebaut hatten. Dieser sichert aber nur einzelne Komponenten der Geräte, etwa den Prozessor. Auf den Leiterbahnen der Platine können die Daten dann aber doch abgegriffen werden: Es gelang den Wissenschaftlern, sowohl die Daten der eingeführten Karten als auch die eingetippten PINs auszulesen. Kriminelle Akteure gehen ähnlich vor und modifizieren Kartenlesegeräte sogar so, dass Daten ausgelesen und über Bluetooth übermittelt werden können. „Für solche Manipulationen gibt es einen regelrechten Markt“, weiß Paul Staat.

Mithilfe eines Hochpräzisionsroboters untersuchen Bochumer Forscher, ob sie mit ihrer Technik Hardware-Manipulationen aufspüren können.



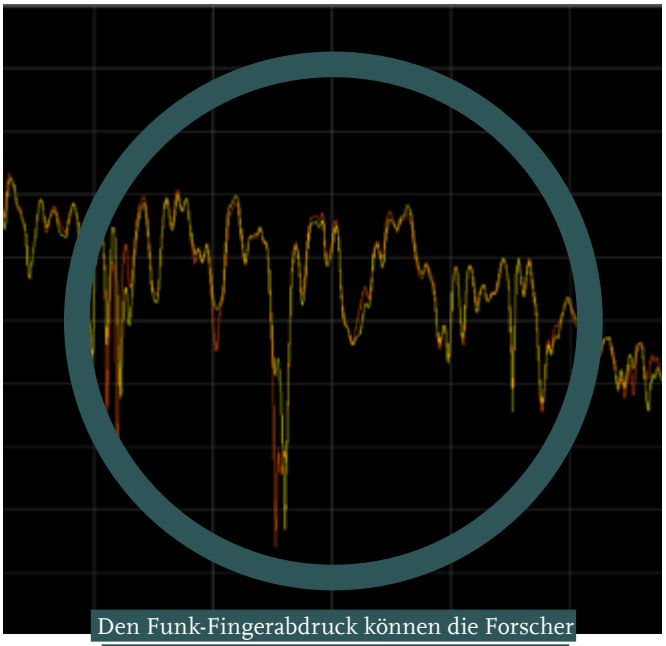
Diesen Hochpräzisionsroboter schafften die Forscher extra an, damit sie ihre Versuche reproduzierbar durchführen können.

Er führt die Nadel durch Löcher im Gehäuse in den Computer ein. Damit das funktioniert, mussten die Forscher dem Roboter erst einmal beibringen, wo sich die Löcher überhaupt befinden – in den ersten Anläufen gingen einige Nadeln kaputt.

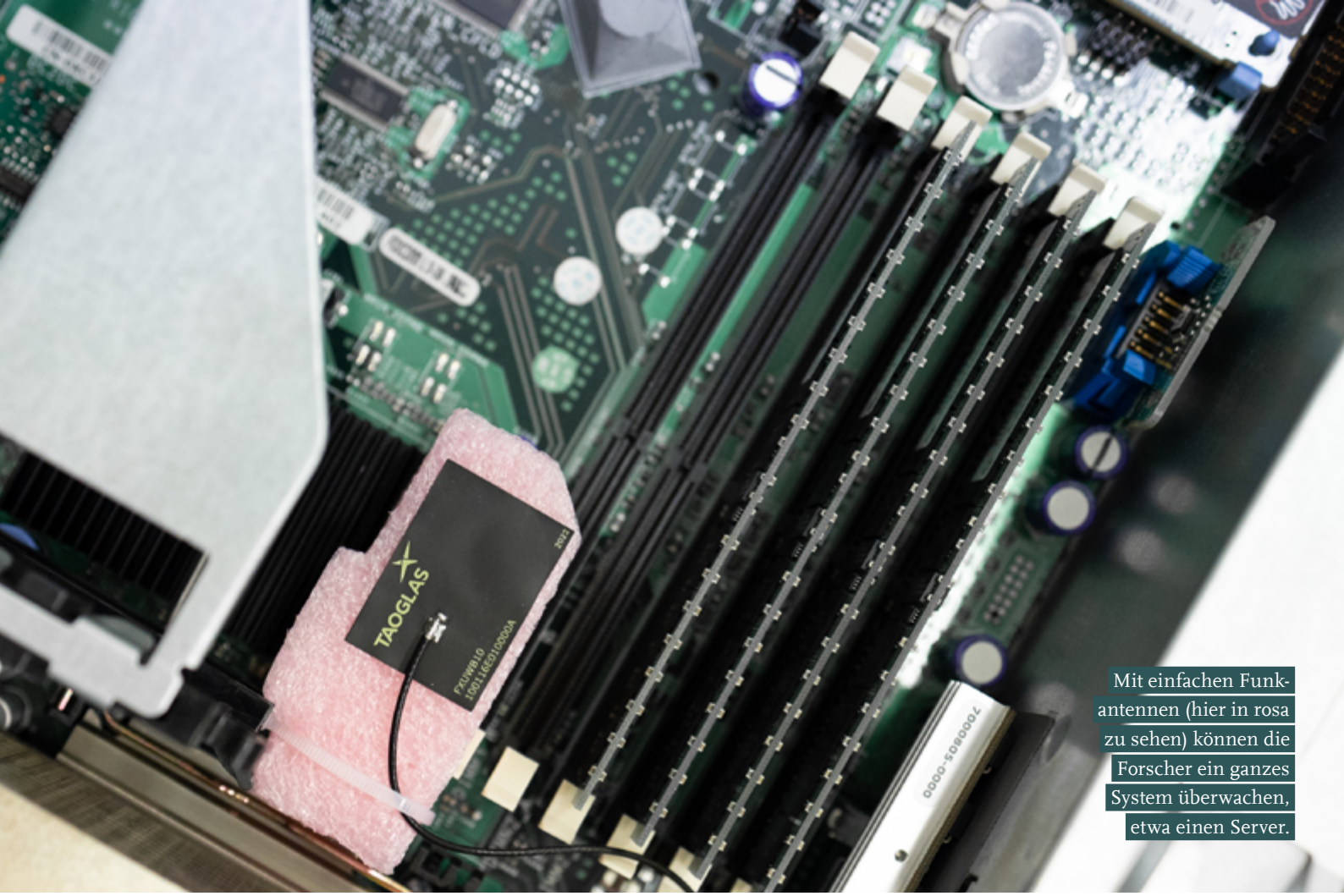
nen Empfänger. Der Sender schickt ein spezielles Funksignal in die Umgebung, das sich überall im System ausbreitet und an den Wänden und Computerkomponenten reflektiert wird. Durch all diese Reflektionen kommt beim Empfänger ein Signal an, das für das System so charakteristisch ist wie ein Fingerabdruck.

Winzige Veränderungen am System reichen aus, um den Fingerabdruck merklich zu beeinflussen, wie eine Demonstration der beiden Forscher zeigt: Ihre Funktechnik haben Paul Staat und Johannes Tobisch in ein altes Computergehäuse eingebaut. Das gemessene Funksignal machen sie auf einem Laptop als Kurve sichtbar, welche die Stärke des Signals bei verschiedenen Frequenzen in Echtzeit darstellt. Dann drehen sie aus dem überwachten Objekt eine der außen im Gehäuse sitzenden Schrauben ein kleines Stück heraus. Und schon reagiert die Frequenzkurve mit einem merklichen Ausschlag, der zuvor nicht da war.

Für ihre Forschung gehen Johannes Tobisch und Paul Staat die Untersuchungen aber systematischer an. Ihr Testobjekt ist ein herkömmlicher Computer, dessen Gehäuse sie in regelmäßigen Abständen mit Löchern versehen haben. Durch diese Löcher können sie eine feine Metallnadel in das Innere des Systems eindringen lassen und überprüfen, ob sie die Veränderung im Funksignal bemerken. Sie variieren dabei die Dicke der Nadel, die Position und die Eindringtiefe. Damit der Versuch unter kontrollierten und reproduzierbaren Bedingungen stattfindet, haben die beiden Forscher extra einen Hochpräzisionsroboter angeschafft, der die Nadel mi-



Den Funk-Fingerabdruck können die Forscher als Kurve sichtbar machen (rot). Sie zeigt die Stärke des Signals bei verschiedenen Frequenzen. Dringt die Nadel in das System ein, reagiert die Kurve mit merklichen Ausschlägen (gelb). (Bild: Paul Staat)



Mit einfachen Funkantennen (hier in rosa zu sehen) können die Forscher ein ganzes System überwachen, etwa einen Server.

krometergenau in das Gehäuse einführt. „Eine Besonderheit ist, dass wir den Versuch durchführen, während der Computer läuft“, sagt Tobisch. Das erzeugt allerhand Störungen. „Die Lüfter sind wie kleine Staubsauger und der Prozessor ist wie eine Heizung“, vergleicht Staat. Diese Schwankungen in den Umgebungsbedingungen beeinflussen das Funksignal. Solche Störungen müssen die Forscher messen und herausrechnen, um unterscheiden zu können, ob Schwankungen im Signal legitim sind oder durch Manipulationen zustande kommen.

Das Eindringen einer 0,3 Millimeter dicken Nadel können die Bochumer IT-Experten mit ihrem System ab einer Eindringtiefe von einem Zentimeter zuverlässig erkennen. Selbst bei einer Nadel von 0,1 Millimeter Dicke – etwa so dick wie ein Haar – schlägt das System noch an, allerdings nicht an allen Positionen. „Je näher sich die Nadel zur Empfangsantenne befindet, desto leichter ist sie zu detektieren“, erklärt Staat. Je dünner und weiter weg die Nadel, desto höher die Wahrscheinlichkeit, dass sie unbemerkt bleibt. Ebenso ist es mit der Eindringtiefe: Je tiefer die Nadel im System steckt, desto leichter ist sie zu erkennen. „Für die Praxis ist es also sinnvoll, sich genau zu überlegen, wo man die Antennen platziert“, resümiert Tobisch. „Sie sollten sich möglichst nah bei den besonders schützenswerten Komponenten befinden.“

Ihren Versuch ließen Johannes Tobisch und Paul Staat zehn Tage laufen und zeigten somit, dass das Messsystem über lange Zeit stabil ist. Später dehnten sie die Messdauer sogar auf einen ganzen Monat aus. Neben teurer, sehr präziser Messtechnik zum Aufzeichnen des Fingerabdrucks werteten sie das Funksignal zum Vergleich auch mit einfacher Technik aus, die für ein paar Euro zu haben ist. Das funktionierte ebenfalls, wenn auch mit einer etwas geringeren Trefferquote. „Es ist immer ein Kompromiss aus Kosten und Genauigkeit“, sagt Paul Staat.

Je nach Einsatzzweck müsste auch noch der Einfluss von Umweltfaktoren berücksichtigt werden. Denn wenn sich die Temperatur oder Luftfeuchtigkeit im Raum ändert, kann das auch den Funk-Fingerabdruck ändern. „Wir hoffen, solche Probleme in Zukunft mithilfe von Maschinellem Lernen angehen zu können“, blickt Johannes Tobisch voraus. Künstliche Intelligenz könnte selbstständig lernen, welche Veränderungen im Funksignal auf unkritische Umgebungsveränderungen zurückzuführen sind und welche auf Manipulationen – so die Idee.

„Prinzipiell steht einer breiten Anwendung der Technik nichts im Wege. Sie eignet sich sowohl für Hochsicherheitsanwendungen als auch für Alltagsprobleme“, sagt Christian Zenger, Gründer und Geschäftsführer von PHYSEC. Das IT-Unternehmen nutzt die Technik bereits, um unerlaubte Manipulationen an kritischen Infrastrukturkomponenten zu verhindern. „Weitere technische Systeme, die nicht nur vor Cyberattacken aus der Ferne, sondern auch vor Hardware-Manipulationen geschützt werden müssen, gibt es genug“, ergänzt er. „Beispielsweise Steuergeräte in Autos, Stromzähler, Medizingeräte, Satelliten und Serviceroboter.“

Text: jwe, Fotos: ms

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