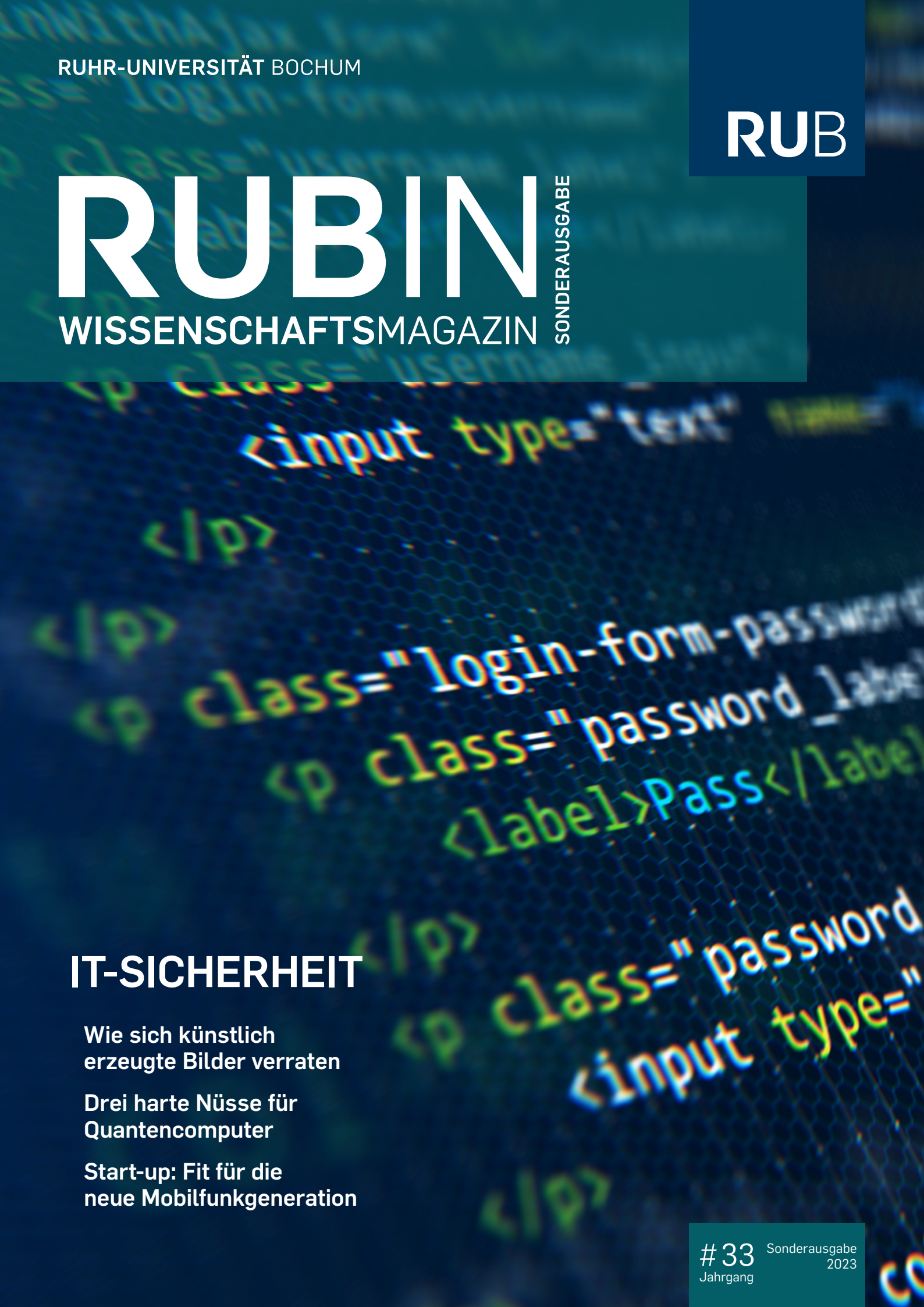
RUHR-UNIVERSITÄT BOCHUM

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

Start-up

FIT FÜR DIE NEUE **MOBILFUNK-GENERATION**

5G kann jede Menge mehr als 4G. Die Firma Radix Security sorgt dafür, dass es keine Sicherheitslücken öffnet.

Wenn man sein Smartphone zückt, um schnell nach dem richtigen Weg zu suchen oder zu schauen, wann der nächste Bus fährt, ist meist sofort die Antwort da. Die Prozesse im Hintergrund laufen so schnell, dass man kaum auf den Gedanken kommt, dass es sie gibt. Aber es sind jede Menge Schnittstellen, die gesendete Daten überwinden müssen. Das Smartphone muss sich mit dem nächsten Mobilfunkmast verbinden. So ein Mobilfunkmast ist wiederum Teil eines deutschlandweiten Netzwerks, das von den großen Telekommunikationsunternehmen eingerichtet und betrieben wird. Auf diese Weise hat man als Endnutzer (fast) immer Empfang und kann sein Telefon ganz mobil nutzen.

Um solche Verbindungen immer und überall zu ermöglichen, egal ob mit dem aktuellen iPhone oder einem LTE Banana Phone von Nokia, müssen sich alle Beteiligten auf die gleichen Standards für die Kommunikation einigen. Das gilt nicht nur für deutsche Netze, sondern auch weltweit. Das sogenannte 3rd Generation Partnership Project, kurz 3GPP, ist die Organisation, die für die Aushandlung und Veröffentlichung der entsprechenden Standards zuständig ist.

Die Spezifikationen umfassen Tausende Seiten, die Dr. David Rupprecht besser kennt, als ihm manchmal lieb wäre. Ihm und seinen Kolleginnen und Kollegen am Lehrstuhl Systemsicherheit am Horst-Görtz-Institut für IT-Sicherheit kam es dabei besonders auf die kleinen und großen Fehler im Standard an. Denn solche Spezifikationsfehler wirken sich direkt auf die Sicherheit einer Verbindung aus und betreffen damit direkt jeden einzelnen Nutzer eines Netzes.

Und das ist erst der Anfang: Selbst, wenn die Spezifikation zu 100 Prozent wasserdicht wäre, fehlt immer noch der Schritt hin zur Implementierung. Dabei werden seitenweise Anweisungen als Grundlage verwendet, um Komponenten zu implementieren. „Anders gesagt: Wer Komponenten eines Mobilfunknetzes baut, der muss Tausende Seiten Text lesen, korrekt interpretieren, und dann auch noch in fehlerfreien Code umsetzen. Und als wäre das nicht schon Herausforderung genug, kommt auch noch die enorme Komplexität von Netzen und Komponenten hinzu", so Rupprecht. Und nimmt ▸

i FÖRDERUNG

Die Gründung von Radix Security wird gefördert von den Gründungsinkubatoren Cube 5 der Ruhr-Universität und Mercator Launch der Radboud Universiteit.

Wer sein Smartphone im Alltag nutzt, hinterfragt die Prozesse nicht, die im Hintergrund laufen.

man eine 100-prozentig sichere Implementierung an – haben wir dann vollständig abgesicherte Netze? „Leider reicht auch das noch nicht aus“, erklärt David Rupprecht. „Die verschiedenen Komponenten müssen in einem komplexen Setup miteinander interagieren. Hardware von verschiedenen Herstellern trifft aufeinander, das Zusammenspiel muss also genauestens konfiguriert werden. Hier haben wir nun unsere dritte und letzte Fehlerquelle im Prozess.”

David Rupprecht und Forschende des Lehrstuhls für Symmetrische Kryptographie haben so zum Beispiel 2021 nachweisen können, dass der Mobilfunkstandard 2G sehr unsicher ist. „Wir konnten zeigen, dass es da sogar absichtlich eingebaute Schwachstellen gibt, die ein Ausspähen von Daten ermöglicht haben“, berichtet er (siehe Seite 36). Die entsprechenden Verschlüsselungsalgorithmen waren so schwach, dass das unmöglich ein Zufall sein konnte – vielmehr handelte es sich um eine Hintertür, die in den 1990er-Jahren mit Absicht beschlossen und eingebaut worden war. Obwohl der Algorithmus auch auf modernen Smartphones immer noch eingebaut ist, geht von diesen Schwachstellen wohl keine Gefahr mehr aus, schätzen die Forschenden. Denn 2G ist lange überholt und kaum mehr im Einsatz.

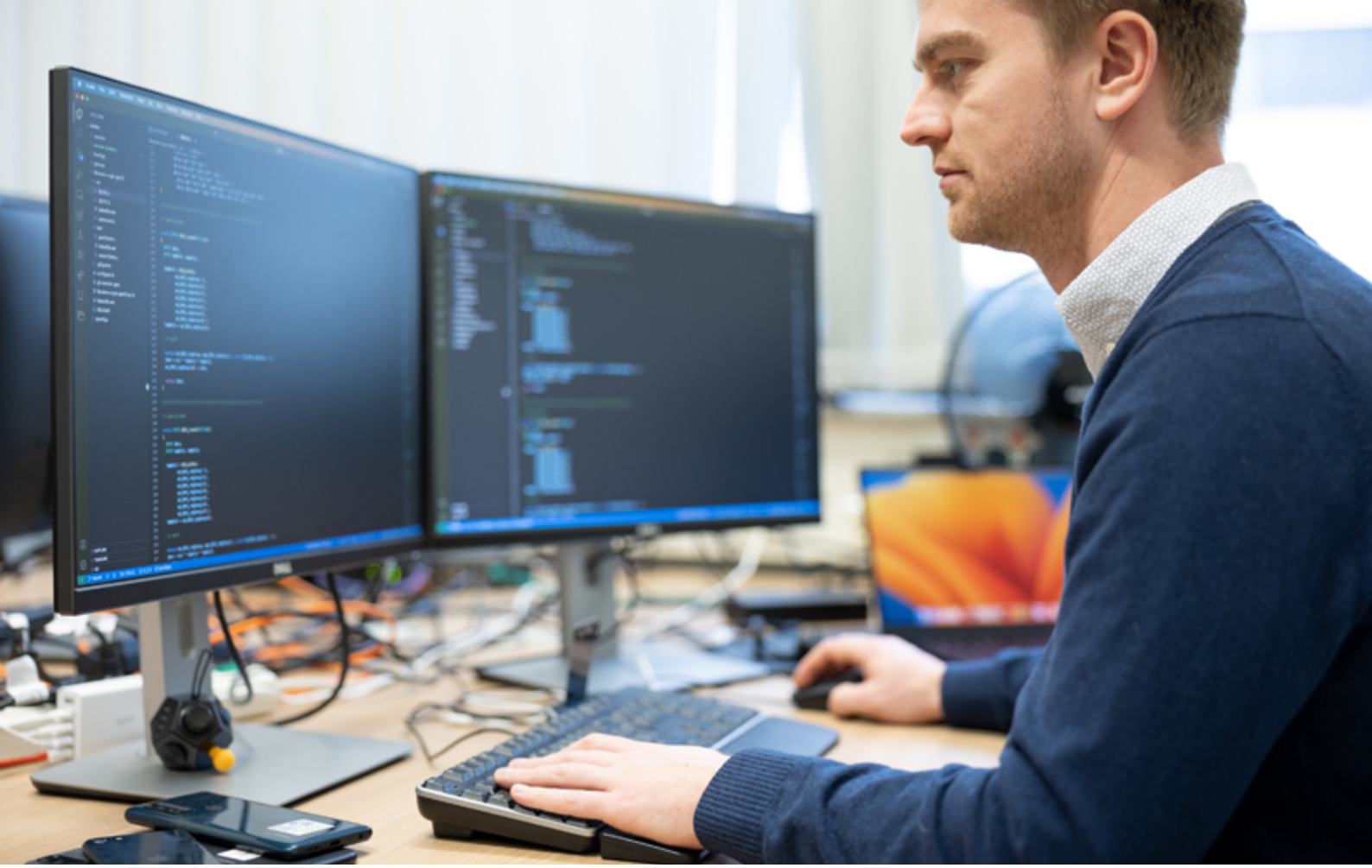
„Alle zehn Jahre gibt es eine neue Mobilfunkgeneration“, so Rupprecht. Während es bei 2G vor allem um mobile Telefonie ging, startet mit dem 3G-Standard das mobile Internet. Seit 4G steht die Nutzung des Internets in Form von Apps klar im Fokus. „Das iPhone kam auf den Markt, mobiles Internet wurde ein Massenphänomen“, so David Rupprecht über die Zeit um 2010 herum, als der Standard eingeführt wurde. Bis heute laufen die meisten Mobilverbindungen über 4G. In seiner Doktorarbeit am Exzellenzcluster CASA hat sich David Rupprecht mit Schwachstellen dieser Generation befasst.

„Währenddessen haben wir mit CASA verschiedene Schwachstellen gefunden, die eigentlich jeden Smartphone-Nutzer betreffen. Eine davon ermöglichte das Abhören von Telefongesprächen. Wenn möglich, wurden die Schwachstellen entsprechend von den Herstellern oder Betreibern geschlossen“, erklärt David Rupprecht. Letzte Sicherheit gibt es dadurch dennoch nicht, denn so ein Zugewinn an Sicherheit geht immer auf Kosten der Leistungsfähigkeit. „Das Gremium der 3GPP muss dann abwägen und andere wichtige Faktoren wie zum Beispiel Geschwindigkeit und Akkulaufzeit mit einbeziehen“, erläutert er. Zudem können sicherheitsrelevante Einstellungen, die in die Spezifikationen aufgenommen werden, mitunter noch vom Netzbetreiber an- und ausgeschaltet werden.

Dennoch hilft die Analyse von Sicherheitsmängeln der aktuellen Mobilfunkgeneration immer auch der folgenden. „Die entsprechenden Gegenmaßnahmen können gleich von vornherein mitgedacht und in die nächste Generation aufgenommen werden“, erklärt David Rupprecht. Für ihn steht mittlerweile schon die fünfte Generation (5G) im Vordergrund. „5G ist besonders interessant, weil es viele neue Anwendungsmöglichkeiten einführt, wie beispielsweise die Vernetzung von Dingen. Autos können mit Ampeln kommunizieren, Fabriken verbessern ihre internen Netze, kritische Infrastrukturen erhalten neue Vernetzungsmöglichkeiten.“ Im Fall der Fabrik-Vernetzung sind es Roboter und Industrieanlagen, die in lokalen 5G-Campusnetzen verbunden werden, und zwar erstmals in privater Regie. „Dadurch kann plötz-

> „5G IST BESONDERS INTERESSANT, WEIL ES VIELE NEUE ANWENDUNGSMÖGLICHKEITEN EINFÜHRT, WIE BEISPIELSWEISE DIE VERNETZUNG VON DINGEN.“
>
> David Rupprecht

David Rupprecht gründet die Firma Radix Security gemeinsam mit Katharina Kohls.



David Rupprecht kennt Tausende Seiten von Spezifikationen, die dafür sorgen, dass in Mobilfunknetzen alles sicher und reibungslos funktioniert.

lich jeder zum Netzbetreiber werden“, spitzt David Rupprecht zu. Die Verantwortung für die sichere Implementierung und Konfiguration der 5G-Netze liegt nun bei den privaten Betreibern. Hier setzt das Unternehmen Radix Security an, das Rupprecht gerade mit Prof. Dr. Katharina Kohls gründet.

„Wir beschäftigen uns seit Jahren mit Sicherheitsfragen in 4G- und 5G-Netzen und haben einen enormen Wissensvorsprung“, sagt Rupprecht. Die Spezifikationen sind zwar öffentlich zugänglich – aber wer kann Tausende Seiten komplexer Informationen verstehen und umsetzen? Radix Security hat es sich zur Aufgabe gemacht, 5G-Sicherheit zugänglich zu machen und Campusnetzbetreiber dabei zu unterstützen, ihre Netze sicher aufzubauen und zu betreiben. Derzeit gibt es in Deutschland rund 300 Campusnetze, auch die Ruhr-Universität hat eines für Forschungszwecke.

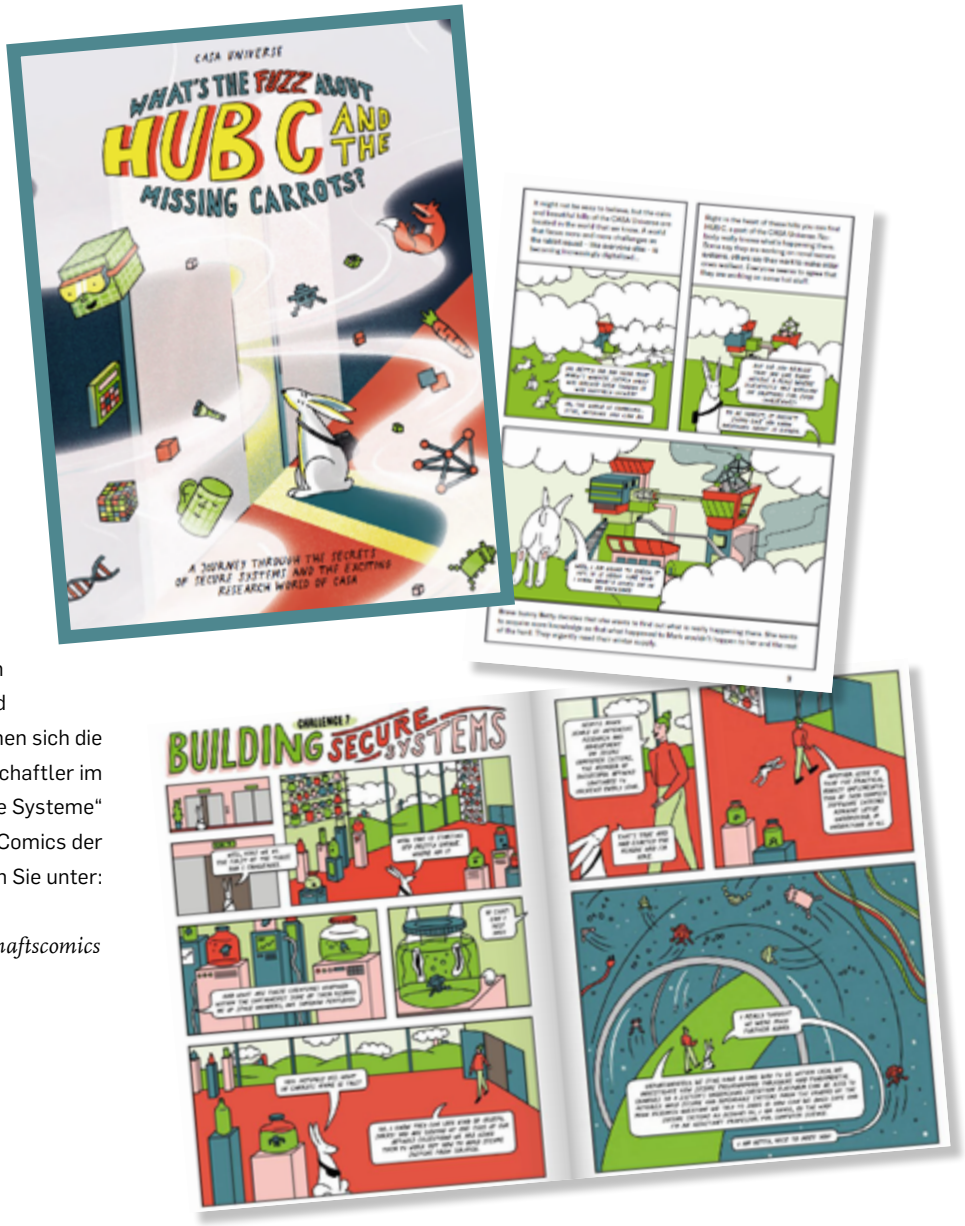
„In der jetzigen Phase, in der die Technologie der Campusnetze noch recht jung ist, stellen wir fest, dass die Sicherheit keine oder nur eine geringe Rolle spielt“, so Rupprecht. Das ist problematisch, weil es viel ressourcenintensiver ist, ein Netz im Nachhinein abzusichern, als Sicherheit von Anfang an mitzuplanen. „Nach den ersten Gesprächen merken wir, dass die Betreiber ganz unterschiedliche Vorstellungen von Sicherheit haben. Hier wird Radix Security noch viel Aufklärung und Schulungsarbeit leisten, um über die Sicherheitsrisiken und Möglichkeiten der Campusnetze aufzuklären.“

Für die Absicherung eines Campusnetzes ist das richtige Werkzeug von großer Bedeutung. Zum einen geht es darum, Angriffe zu verhindern und damit Schwachstellen in der Implementierung und Konfiguration von Netzwerkkomponenten aufzudecken. Das Radix-Security-Testwerkzeug ermöglicht es, Komponenten über den Standard hinaus auf ihre Sicherheitseigenschaften zu überprüfen. Beispielsweise wird geprüft, ob eine Komponente wichtiges Schlüsselmaterial ausgibt. Wenn dies der Fall ist, wird die gesamte Sicherheit des Netzwerks kompromittiert.

„Zusätzlich zu den Tests müssen wir ein Campusnetz in die Lage versetzen, Angriffe zu erkennen und abzuwehren“, erklärt David Rupprecht. Radix Security entwickelt zu diesem Zweck ein Angriffserkennungssystem, das auf Campusnetzbetreiber zugeschnitten ist. Die grundsätzliche Problematik liegt in der Komplexität der Netzwerke und der offenen Luftschnittstelle. Im Gegensatz zu einem verkabelten Netzwerk muss sich ein Angreifer nur in der physischen Nähe des Netzwerks befinden, um es anzugreifen. „Bei all unseren Entwicklungen und Ideen hilft die Nähe zur Universität“, so Rupprecht. „Die Universität gibt uns einen Vorteil gegenüber unseren Mitbewerbern. Durch die Forschungsinfrastruktur, wie durch das Exzellenzcluster CASA, können unsere Kunden von Cutting-Edge-Forschung profitieren und sich so gegen die neuesten Angriffe schützen.“

Text: md, 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