RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

SCIENCEMAGAZINE

SPECIAL ISSUE

IT SECURITY

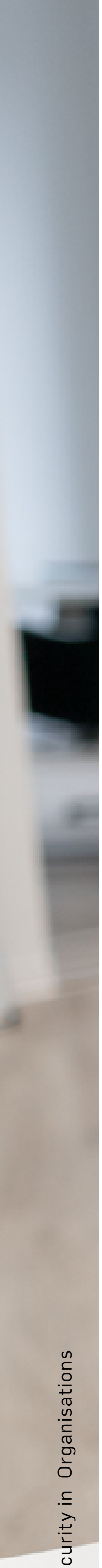
Three tough nuts for quantum computers to crack

This is how artificially generated images reveal their true colours

Start-up: Ready for the new generation of mobile communications

#33 Volume

Special Issue 2023



Organisations

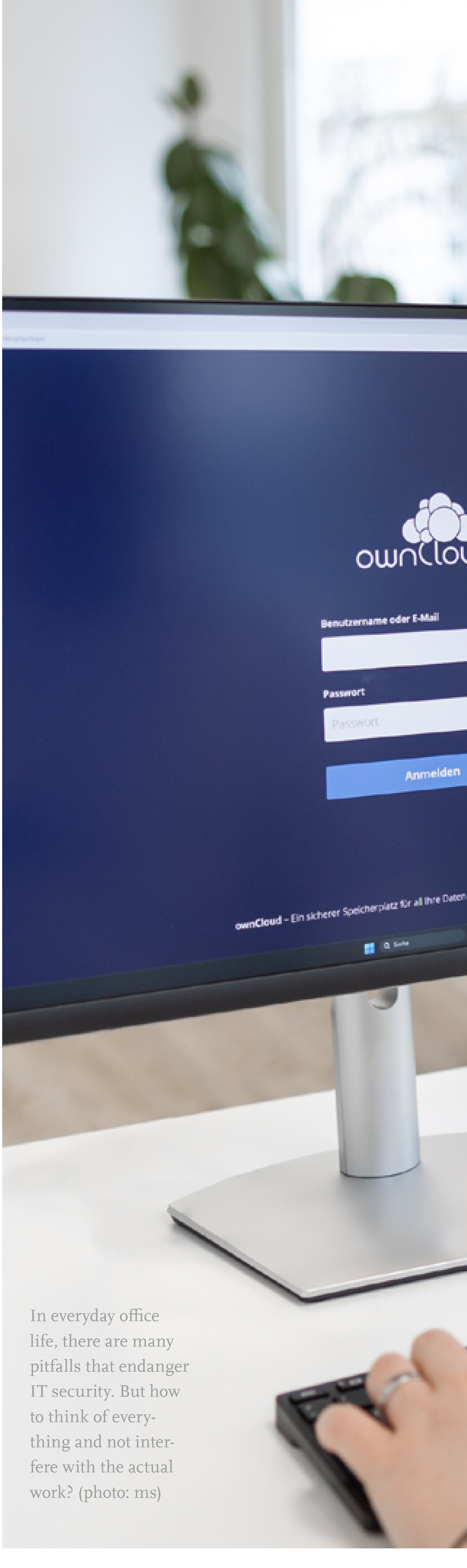
HOW TO RECONCILE IT **SECURITY AND PRODUCTIVITY**

Uta Menges and Jonas Hielscher want to lift the label of being a nuisance from IT security measures and incorporate them more effectively into everyday life.

IT security – many people roll their eyes at the mere sound of the word. Everybody realises, of course, that it is a matter of great importance. The spectacular attacks on IT systems of organisations in recent years are frightening; entire universities and city administrations were sometimes offline for weeks. And the successful attacks are only the tip of the iceberg, because attempted attacks are a daily occurrence. But what are companies and organisations doing to ensure that their IT is secure? Ultimately, each and every individual has to contribute to this security. Why doesn't it actually work all that well and how could it be made to work?

This is the question explored by Uta Menges and Jonas Hielscher. The two form a tandem in the Graduate School SecHuman – Security for People in Cyberspace. Even though they're working together on their PhD thesis, their professional backgrounds couldn't be more different. While Jonas Hielscher studied computer science in Magdeburg, Uta Menges studied business psychology. She completed her Master's degree in the field of marriage, family and life coaching and has also worked in this area. How do they all go together?

"They go surprisingly well together," she says. "I can transfer what I've learned to the field of IT security." This is because the focus in both fields is on humans. "No matter how good the technological measures for the security of an IT system are, they won't work without the cooperation of the users," adds Jonas Hielscher. But research results have been ▸



In everyday office life, there are many pitfalls that endanger IT security. But how to think of everything and not interfere with the actual work? (photo: ms)

SECHUMAN GRADUATE SCHOOL

Since 2016, PhD students at Ruhr University Bochum have been researching security in cyberspace at the "SecHuman" Graduate School, which is funded by the NRW Ministry of Culture and Science. At the school, PhD students work not only with researchers from other disciplines, but also with actors from the industry. The SecHuman Graduate School, short for "Brave New World: Security for People in Cyberspace", is located at the Horst Görtz Institute for IT Security in Bochum and is also integrated into the Cluster of Excellence CASA – Cybersecurity in the Age of Large-Scale Adversaries.

Jonas Hielscher (left) and Uta Menges want to know how IT security can be integrated into everyday working life so that it is not a hindrance. (photo: CASA, Caroline Schreer)

> ”NO ONE CAN DO THAT ON A NORMAL WORKING DAY“
>
> Uta Menges

scarce on how to get organisations to support their employees in the transition to secure behaviour and not simply dump the burden on the end users. And Menges and Hielscher are not very happy with the way it's handled in practice either.

"Many companies commission providers, for example, to send fake phishing emails to their employees in order to sensitise the team to potential attacks," elaborates Jonas Hielscher. "But such one-off and one-dimensional measures don't effect much." In case of doubt, someone who has fallen for it has the feeling of being in the hot seat. That doesn't help anyone.

The two researchers ask completely different questions: How feasible is IT security for employees? Do employees know exactly what they have to do? Can measures really be implemented or is there no time for it in the daily work routine? Do the IT security measures compete with other tasks that need to be done? "For example: read every email very carefully and check it for indications of a phishing attack," illustrates Uta Menges. "No one can do that in a normal working day."

In addition to such questions, which are grouped under the umbrella term "productive security", the two PhD researchers also focus on communication about IT security. How do people talk about it? The implementers are often engineers. They talk about technology without taking their colleagues who are not technologically savvy on board. This communicative hurdle leads to misunderstandings and doesn't do anything to foster a cooperation based on mutual trust. But this is precisely what the researchers consider indispensable. "If someone has opened a phishing email and fallen into the trap, they mustn't be afraid to report the incident," says Uta Menges. "And it must be clear to whom." She calls for a healthy error culture: no one should be pilloried because they've made a mistake. Clear instructions are essential. All too often, however, employees are left alone with vague rules. Communication also includes the response of the help desk. If it's impersonal, IT security remains abstract.

i DAMAGE CAUSED BY IT ATTACKS

No one can put an exact figure on how much economic damage is caused by IT attacks, as there is no obligation to report such incidents in Germany. The figure published by the industry association Bitcom, which amounts to around six per cent of the gross domestic product, is therefore only an estimate, and Jonas Hielscher believes it is too high.
Ransomware attacks, in which IT systems are encrypted by external parties in order to extort a ransom, frequently hit medium-sized companies, whose protection is often inadequate.

Both researchers have also identified communication barriers between IT security professionals and the managers of institutions. "Professionals want to talk about products. Management is much more interested in the risk that needs to be contained. But there's no measure of how secure or insecure the behaviour of employees is," Jonas Hielscher explains. He and Uta Menges are venturing into largely unexplored territory. "You'd have to interview people, observe their behaviour, get their feedback, evaluate incidents. But none of that has been done yet, partly because it's so complicated," he says.

Based on her expertise as a psychologist, Uta Menges points out: if IT security is to succeed in organisations, self-efficacy is the most important aspect. In other words: IT security must be manageable. And it must be effective. "This may sound self-evident, but the decades-old narrative that everything's getting worse and nothing can be done anyway is stuck in many people's heads," says Uta Menges. "Those who have internalised it have a hard time taking action because they don't believe in it."

Uta Menges and Jonas Hielscher are tackling the issue with a number of partners from the industry. Together with a large enterprise in North Rhine-Westphalia, they are coaching more than a dozen trainees to become ambassadors for IT security. They've met the Chief Information Security Officer and got his mobile phone number. The goal is to create a network across the company's many subsidiaries with over 20,000 employees. This is how IT security is to be given a face. Since November 2021, the two researchers have been communicating with a group of 28 Swiss Chief Information Officers from various companies. Among other things, they help design workshops and stay up to date on everyday problems in the companies.

"This PhD thesis is only just evolving as we work on it," says Jonas Hielscher. Still, both are fascinated by their field of research. "It's pioneering work and can't be planned – after all, it's humans who are the focus," says Uta Menges. Plenty of research questions are still open. The research field of human-centred security is still young, the concept only emerged around 2000. "But there's an ever increasing number of professorships, it's a growing field," as Jonas Hielscher is pleased to say. "And our results will certainly not fall on deaf ears."

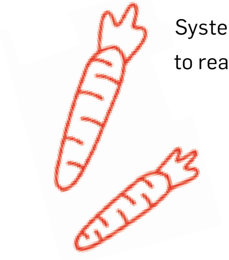
md

EDITOR'S DEADLINE

CASA UNIVERSE
WHAT'S THE FUZZ ABOUT
HUB C AND THE
MISSING CARROTS?
A JOURNEY THROUGH THE SECRETS OF SECURE SYSTEMS AND THE EXCITING RESEARCH WORLD OF CASA

The rabbits in the CASA Universe are startled: the seemingly well-secured access to Rabbit Mark's carrot stash has been hacked and all winter supplies have been stolen. The brave bunny Betty then starts looking for support at the nearby CASA Hub C – a mysterious place that is supposed to hold solutions for digital security. Thus begins the adventure of Betty the bunny, the protagonist of the first science comic from the Cluster of Excellence CASA. Along with Betty, the readers explore the Research Hub and learn about the research priorities and challenges that the scientists in the Research Hub C "Secure Systems" deal with on a daily basis. Find out how to read this and more CASA comics at no cost at:

↗ *casa.rub.de/en/outreach/science-comics*



Answers
DEEP FAKE-QUIZ
The following faces are real:
1a, 2a, 3b, 4a, 5b, 6a

??

LEGAL NOTICE

PUBLISHER: Cluster of Excellence CASA at the Horst Görtz Institute for IT Security at Ruhr University Bochum in collaboration with the Corporate Communications Department at Ruhr University Bochum (Hubert Hundt, v.i.S.d.P.)

EDITORIAL ADDRESS: Corporate Communications Department, Editorial Office Rubin, Ruhr-Universität Bochum, 44780 Bochum, Germany, phone: +49 234 32 25228, rubin@rub.de, news.rub.de/rubin

EDITORIAL BOARD: Dr. Julia Weiler (jwe, editor-in-chief); Meike Drießen (md); Lisa Bischoff (lb)

PHOTOGRAPHER: Michael Schwettmann (ms), Dammstr. 6, 44892 Bochum, Tel.: +49 177 3443543, info@michaelschwettmann.de, www.michaelschwettmann.de

COVER: Sashkin – stock.adobe.com

PHOTOGRAPHS FOR TABLE OF CONTENTS: Michael Schwettmann

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

PRINTED BY: LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, Germany, Tel.: +49 231 90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

EDITION: 800

DISTRIBUTION: Rubin is published twice a year in German language; the regular issues are available from the Corporate Communications Department at Ruhr-Universität Bochum. The magazine can be subscribed to free of charge at news.rub.de/rubin/abo. The subscription can be cancelled by email to rubin@rub.de. The special issue 2021 is available from the Horst Görtz Institute for IT Security. In case of interest, please contact hgi-presse@rub.de.

ISSN: 0942-6639

Reprinting with reference to source and submission of proof copies