CASA UNIVERSE

DURCH DEN DSCHUNGEL DER NUTZBAREN SICHERHEIT MIT HUB ID

EINE REISE ZU DEN RÄTSELN DER NUTZBAREN SICHERHEIT UND DER AUFREGENDEN FORSCHUNGSWELT VON CASA

DURCH DEN DSCHUNGEL DER NUTZBAREN SICHERHEIT MIT IHUB ID

EINE REISE ZU DEN RÄTSELN DER NUTZBAREN SICHERHEIT UND DER AUFREGENDEN FORSCHUNGSWELT VON CASA

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

CASA

Cybersicherheit im Zeitalter großskaliger Angreifer

Herausragende Wissenschaftler*innen erforschen und entwickeln im Rahmen des Exzellenzclusters „CASA – Cyber Security in the Age of Large-Scale Adversaries“ starke und nachhaltige Gegenmaßnahmen gegen mächtige Cyber-Angreifer, mit besonderem Fokus auf nationalstaatliche Angriffe. Die Forschung von CASA zeichnet sich durch einen starken interdisziplinären Ansatz aus, der nicht nur technische Fragen, sondern auch das Zusammenspiel von menschlichem Verhalten und IT-Sicherheit untersucht. Dieser einzigartige, ganzheitliche Ansatz bildet die Grundlage für exzellente IT-Sicherheitsforschung.

CASA umfasst vier Forschungsbereiche (Research Hubs):

HUB A „Kryptographie der Zukunft“: Forschung zur zukünftigen Kryptographie mit beweisbarer Sicherheit und Entwicklung von Ansätzen, die auch gegen Quantencomputer sicher sind.

HUB B „Eingebettete Sicherheit“: Untersuchung der Sicherheit eingebetteter Systeme auf der Hardware-Ebene sowie der Interaktion von Sicherheitssystemen mit ihrer physischen Umgebung.

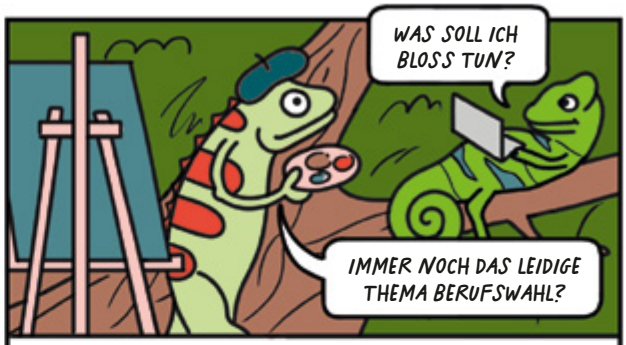
HUB C „Sichere Systeme“: Entwicklung von sicheren und effizienten Systemen auf der Software-Ebene, auch mit Hilfe von Methoden aus dem Bereich des maschinellen Lernens.

HUB D „Benutzerfreundlichkeit“: Konzentration auf benutzerfreundliche Sicherheit und Privatsphäre sowie die Erforschung der Schnittstelle zwischen Mensch und Technik.

Jeder HUB befasst sich mit spezifischen Forschungsherausforderungen (Challenges), die sorgfältig ausgewählt wurden, um Sicherheitsfragen anzugehen, die für den Schutz vor komplexen Angriffen von entscheidender Bedeutung sind.

Die Challenges des HUB D sind:
Challenge 10: Entwickler*innen und nutzbare Sicherheit
Challenge 11: Anwender*innen und nutzbare Sicherheit

Ein ganz gewöhnlicher Tag im dampfend warmen Dschungel des CASA-Universums.

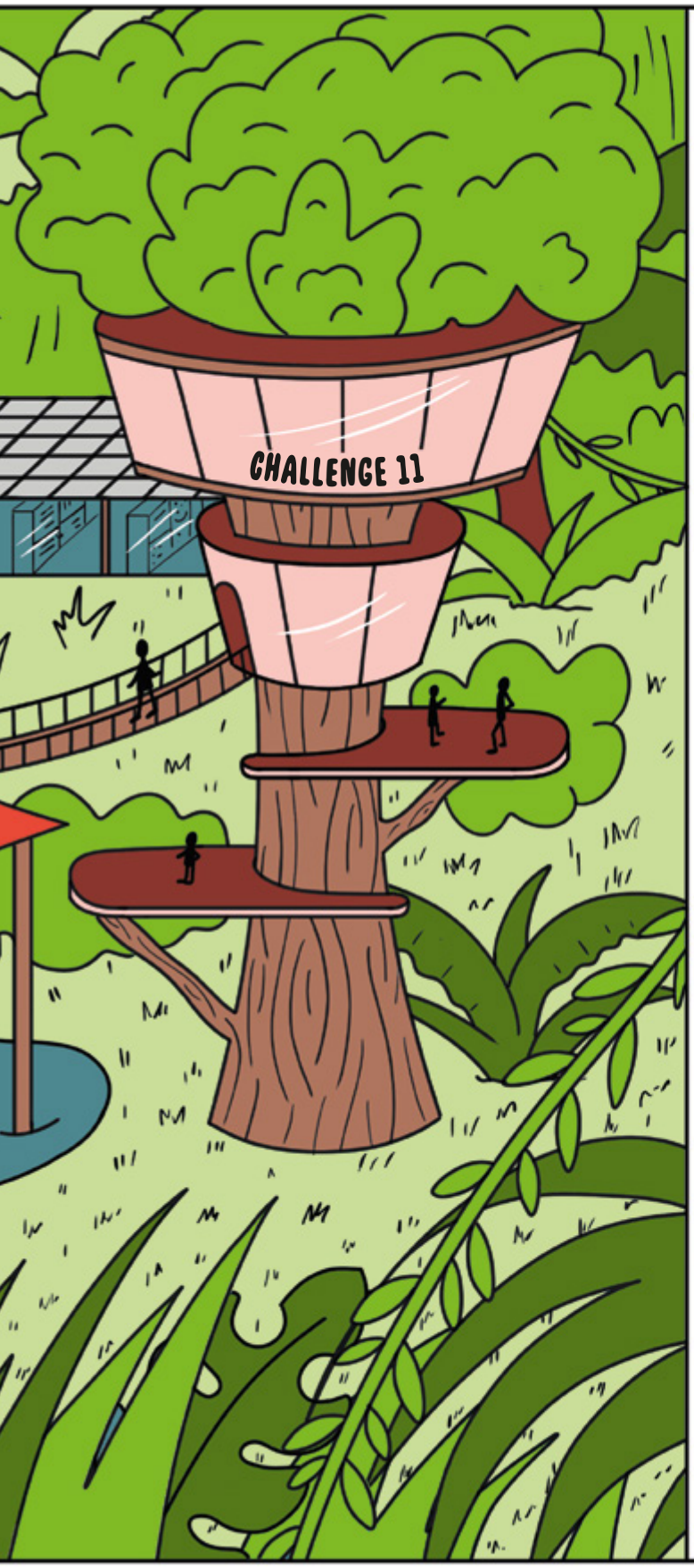


Pablo malt leidenschaftlich, während seine Schwester Maggie wie üblich am Laptop sitzt.

Seit ihrem Schulabschluss kann sich Maggie nicht entscheiden, was sie als Nächstes machen soll: sie arbeitet gerne mit Menschen, aber sie liebt auch Zahlen und programmiert gerne. Eine Mischung wäre ideal.

Hat ihr Bruder recht? Sie schwankt zwischen dem Schutz von Nutzenden und der Erfüllung von Anforderungen an Sicherheit und Datenschutz. Im Dschungel der Informationen hofft sie auf Antworten.


WILLKOMMEN IN HUB D
CHALLENGE 10



Inhalt

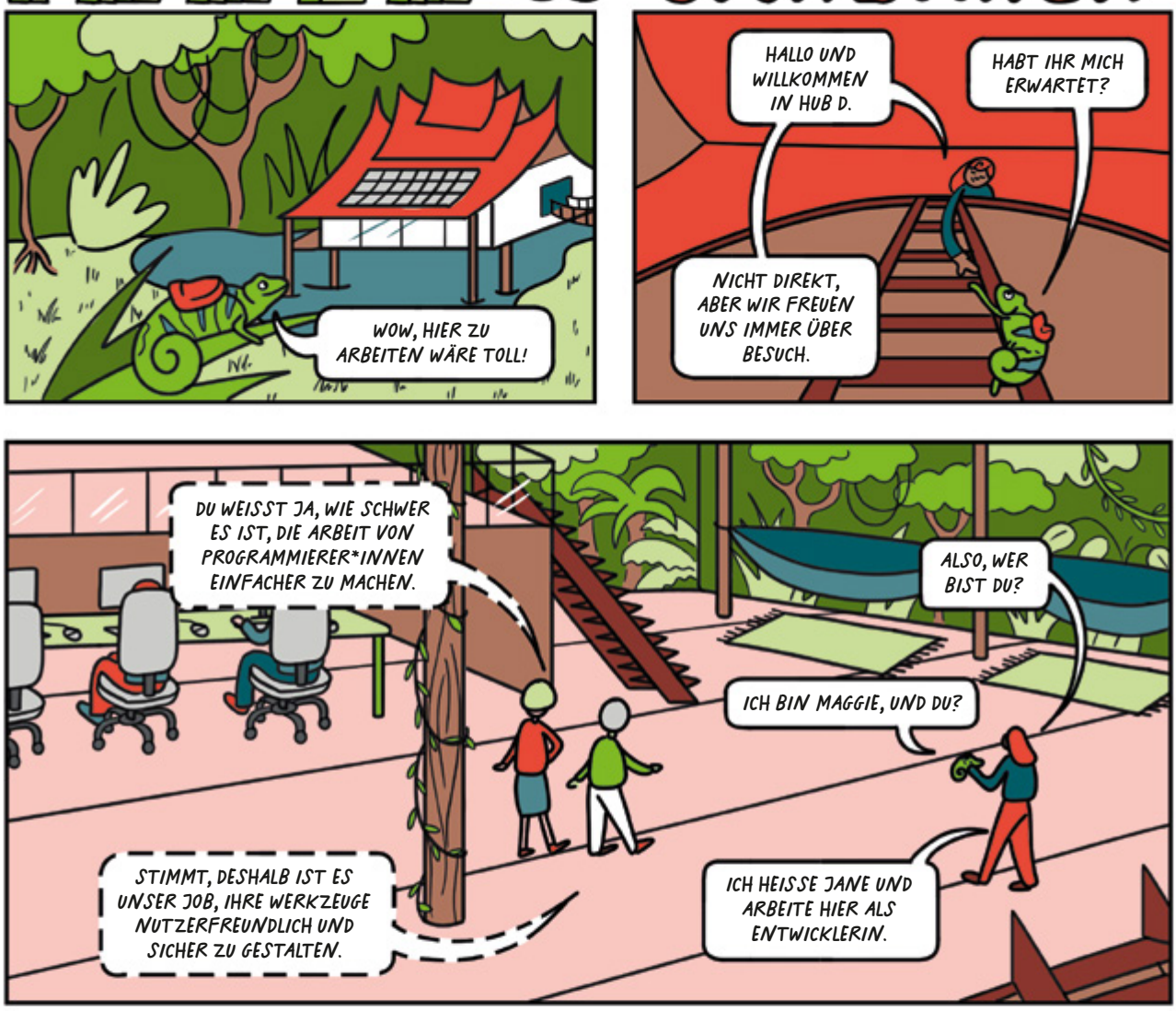
CASA BACKGROUND

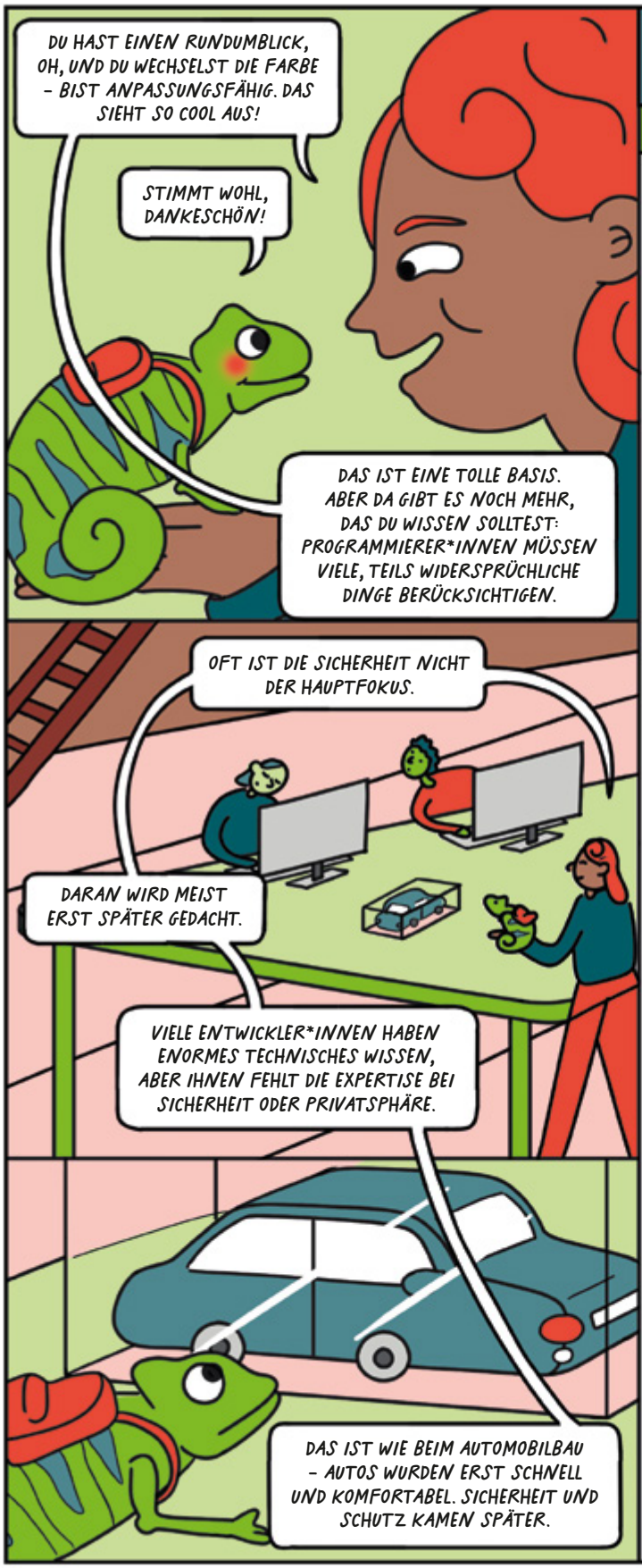
CASA steht für „Cyber Security in the Age of Large-Scale Adversaries“ und wird als Exzellenzcluster (EXC) im Rahmen der Exzellenzstrategie der DFG in Deutschland gefördert. Ziel ist es, nachhaltige Sicherheit gegen komplexe, groß angelegte Angriffe zu ermöglichen. Dazu erforscht ein interdisziplinäres Team nicht nur technische, sondern auch soziale Faktoren und Zusammenhänge. Das Exzellenzcluster ist an der Ruhr-Universität Bochum angesiedelt.

casa.rub.de

CHALLENGE 10

ENTWICKLER*INNEN UND NUTZBARE SICHERHEIT





CASA WIKI

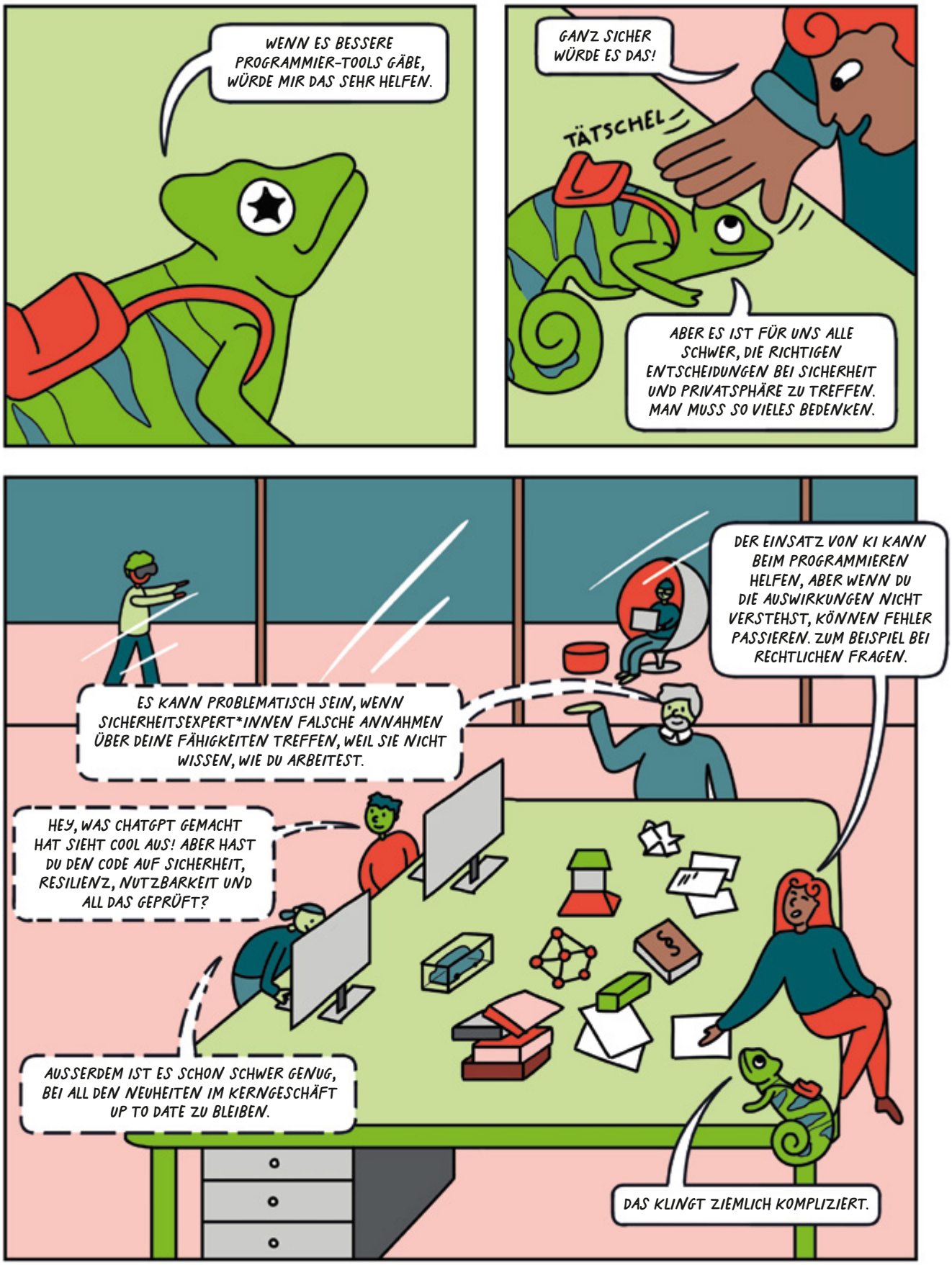
Mit einer **Programmierschnittstelle (API)** kann man eine Sammlung von Funktionen erstellen, die andere in ihren Programmen verwenden können. Sie können zum Beispiel auf Informationen wie das aktuelle Wetter über eine API zugreifen, um sie in ihr Programm zu integrieren.

Die **Datenschutzgrundverordnung (DSGVO)** ist das Datenschutzgesetz der Europäischen Union. Es wurde zum Schutz der Daten europäischer Bürger*innen entwickelt. Unternehmen, die Software für den europäischen Markt entwickeln, müssen sich an diese Gesetze halten oder riskieren erhebliche Geldstrafen.

KI-Tools sind Programme wie ChatGPT, die künstliche Intelligenz nutzen und Softwareentwickler*innen bei der Programmierung unterstützen können, indem sie beispielsweise Code generieren oder Fragen beantworten. Es ist jedoch noch nicht klar, wie diese Tools die Sicherheit der geschriebenen Software beeinflussen.

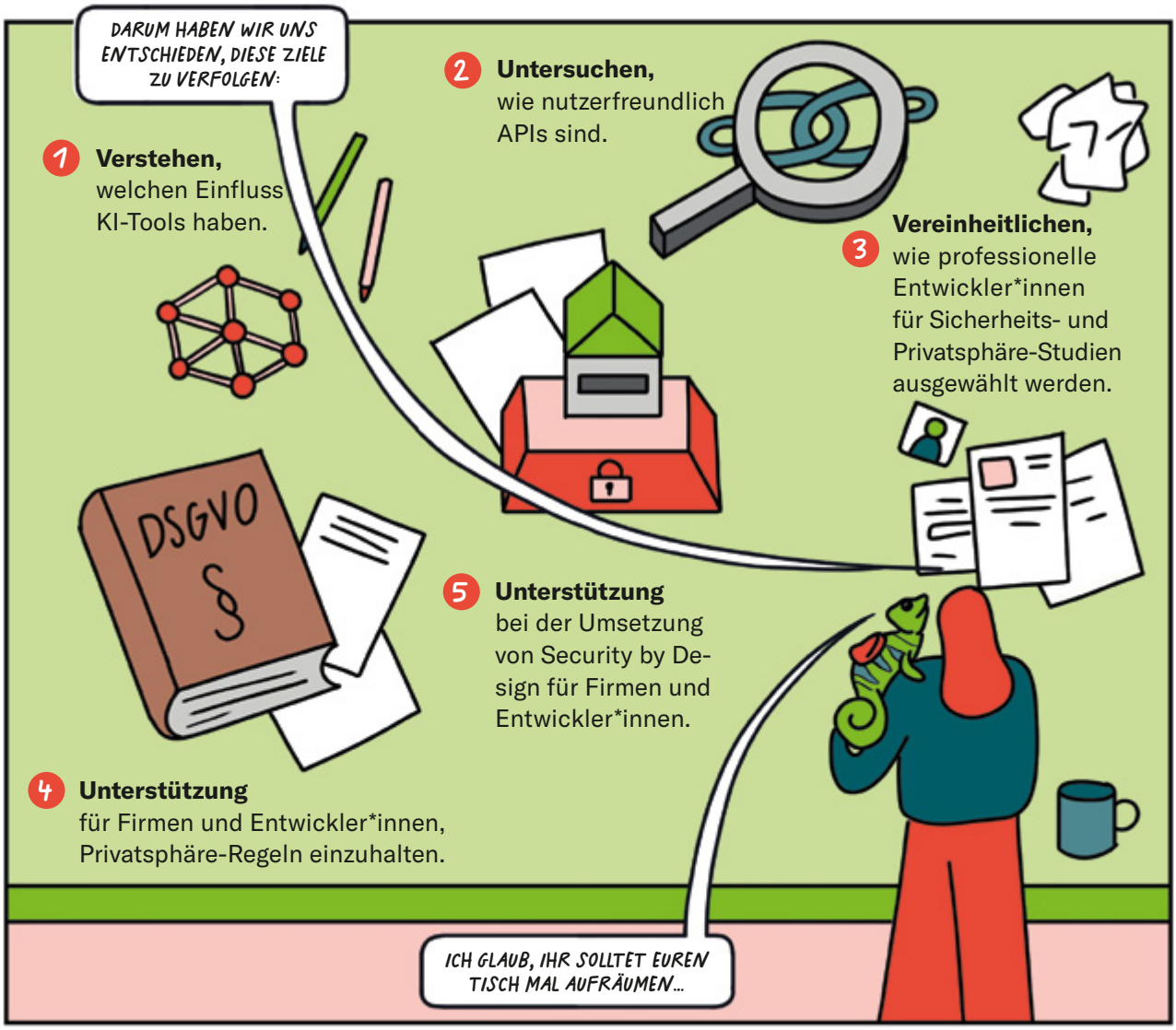
S&P ist die Abkürzung für ‚Sicherheit und Privatsphäre'.

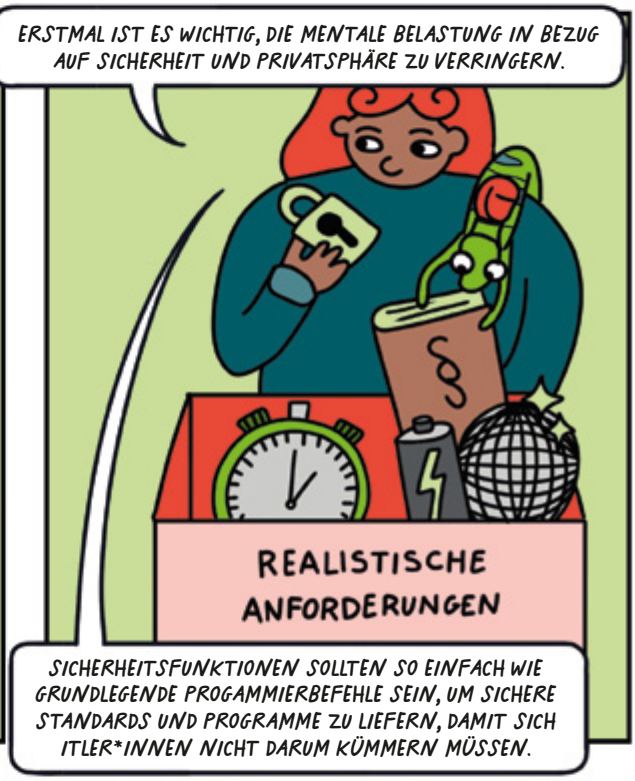
Security Champions sind Mitarbeiter*innen, die über vertiefte Kenntnisse im Bereich der Informationssicherheit verfügen und eine direkte Verbindung zum Sicherheitsteam haben.


WENN ES BESSERE PROGRAMMIER-TOOLS GÄBE, WÜRDE MIR DAS SEHR HELFEN.
GANZ SICHER WÜRDE ES DAS!
TÄTSCHEL
ABER ES IST FÜR UNS ALLE SCHWER, DIE RICHTIGEN ENTSCHEIDUNGEN BEI SICHERHEIT UND PRIVATSPHÄRE ZU TREFFEN. MAN MUSS SO VIELES BEDENKEN.
DER EINSATZ VON KI KANN BEIM PROGRAMMIEREN HELFEN, ABER WENN DU DIE AUSWIRKUNGEN NICHT VERSTEHST, KÖNNEN FEHLER PASSIEREN. ZUM BEISPIEL BEI RECHTLICHEN FRAGEN.
ES KANN PROBLEMATISCH SEIN, WENN SICHERHEITSEXPERT*INNEN FALSCHE ANNAHMEN ÜBER DEINE FÄHIGKEITEN TREFFEN, WEIL SIE NICHT WISSEN, WIE DU ARBEITEST.
HEY, WAS CHATGPT GEMACHT HAT SIEHT COOL AUS! ABER HAST DU DEN CODE AUF SICHERHEIT, RESILIENZ, NUTZBARKEIT UND ALL DAS GEPRÜFT?
AUSSERDEM IST ES SCHON SCHWER GENUG, BEI ALL DEN NEUHEITEN IM KERNGESCHÄFT UP TO DATE ZU BLEIBEN.
DAS KLINGT ZIEMLICH KOMPLIZIERT.

REAL LIFE STORY

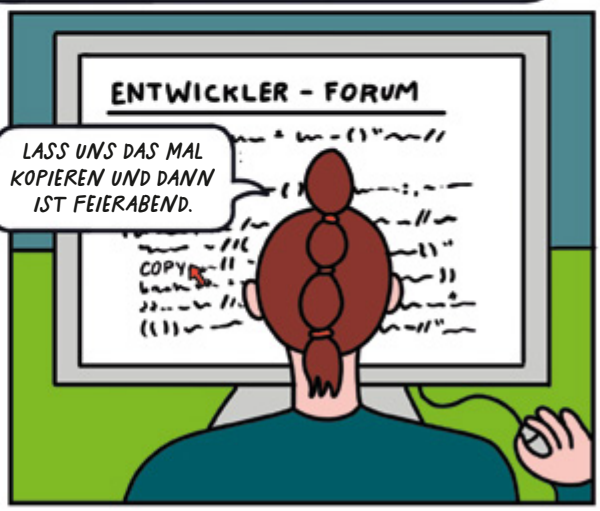
Eine Studie zeigte, dass Informatikstudierende und professionelle freiberufliche Entwickler*innen Probleme mit der sicheren Speicherung von Passwörtern haben. Es zeigte sich unter anderem, dass Sicherheit für die Entwickler*innen nur eine untergeordnete Aufgabe ist. Zwar bieten viele Frameworks eine sichere Speicherung an, aber das muss explizit ausgewählt werden. Sie helfen den Anwender*innen nicht von vornherein und provozieren schwache Sicherheitseinstellungen.

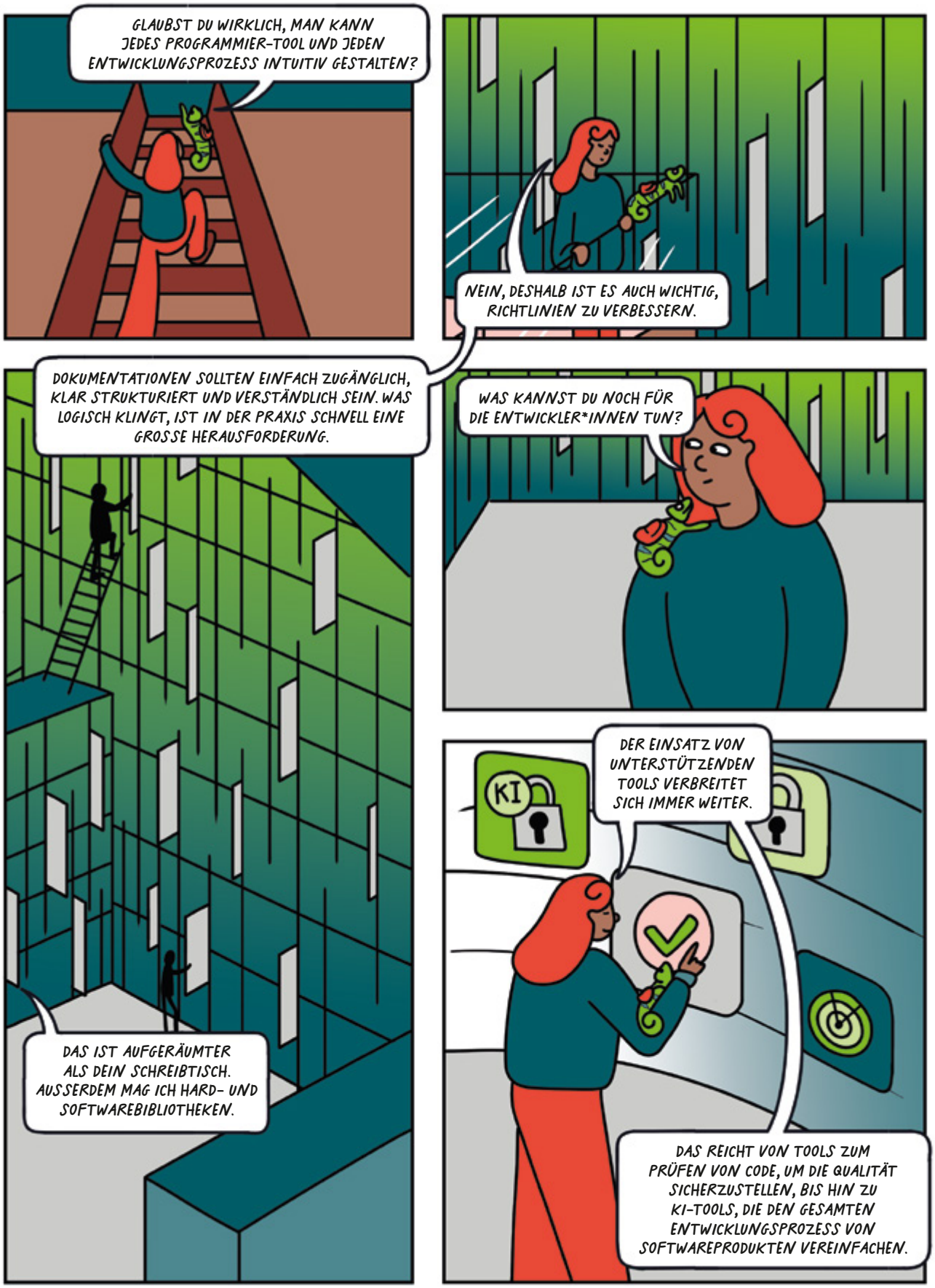




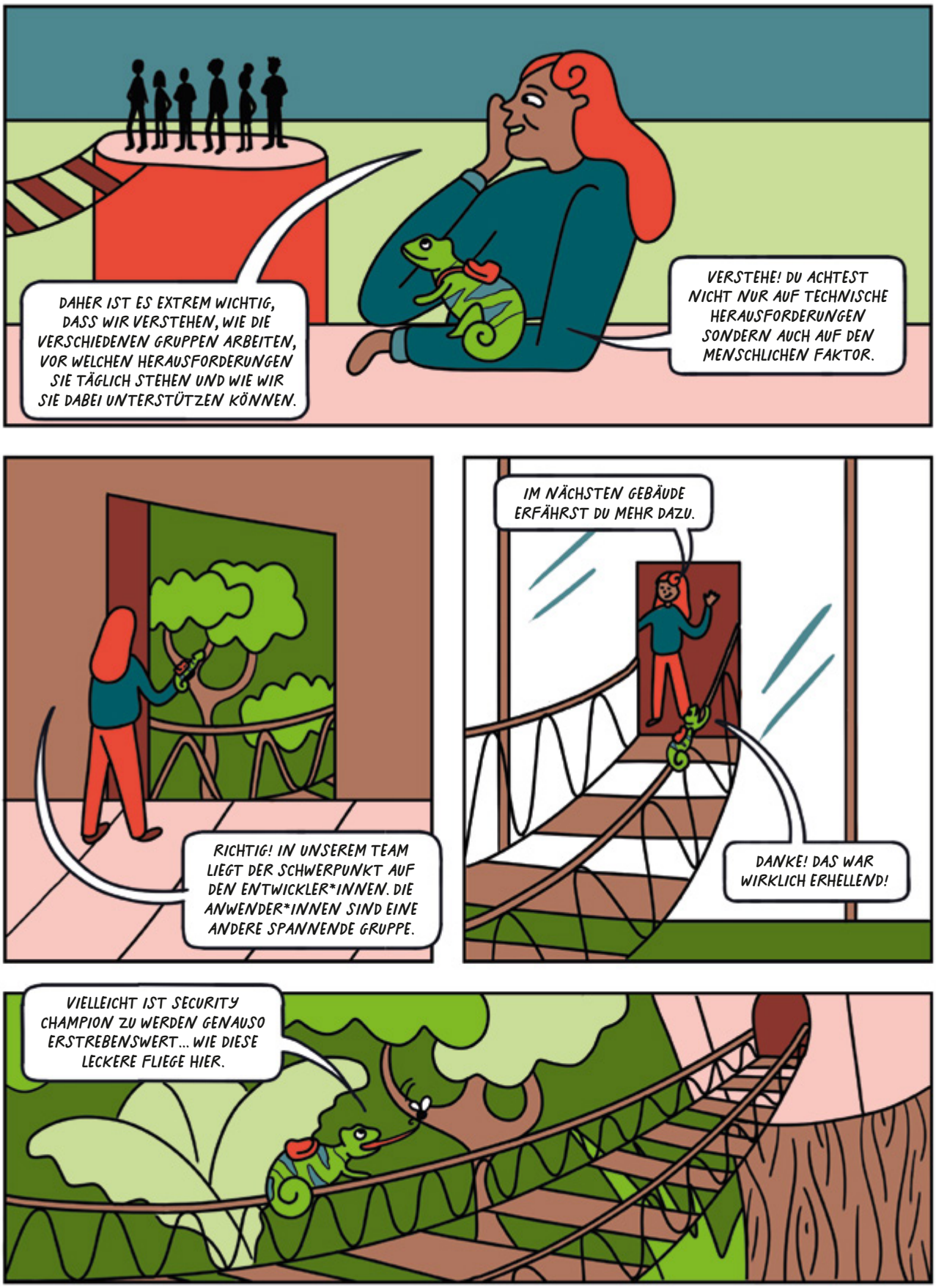
FUN FACT

Selbst auf Webseiten, die sich an Entwickler*innen richten, sind Sicherheit und Datenschutz manchmal nur von untergeordneter Bedeutung. So werden beispielsweise in einem Artikel über Verschlüsselung auf der Webseite „Android for Developers“ veraltete Standards als Beispielcode verwendet. Obwohl im restlichen Text auch sichere Lösungen vorgestellt werden, überehmen einige Programmierer*innen den Beispielcode aus Bequemlichkeit.



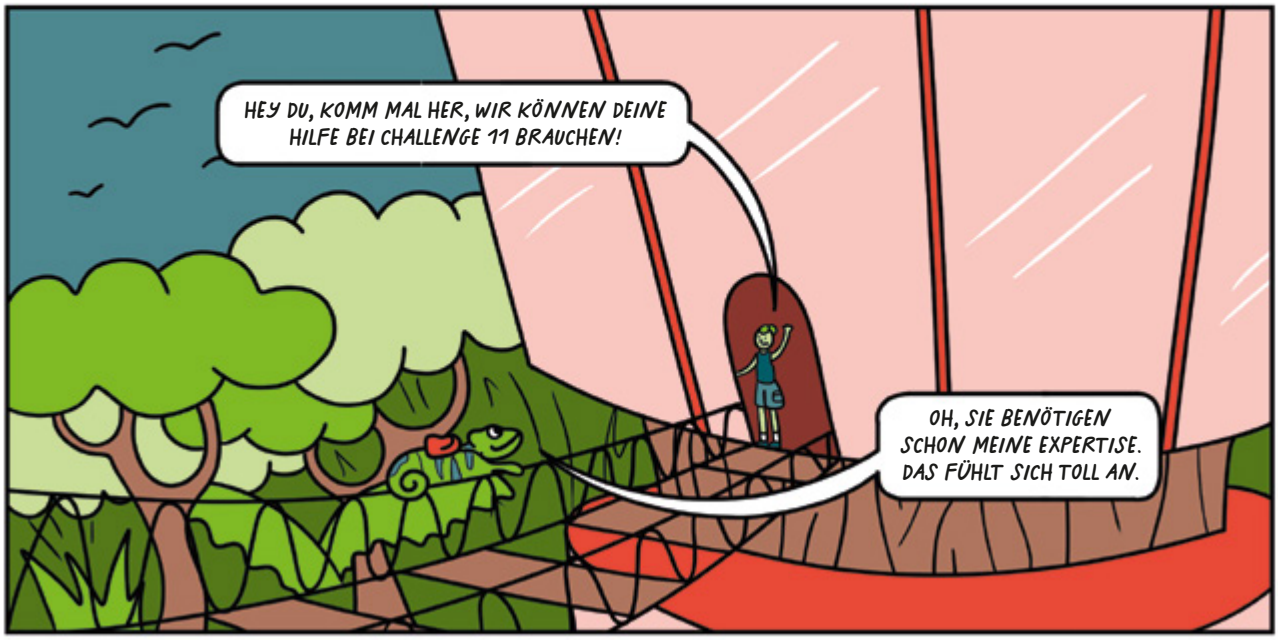

GLAUBST DU WIRKLICH, MAN KANN JEDES PROGRAMMIER-TOOL UND JEDEN ENTWICKLUNGSPROZESS INTUITIV GESTALTEN?
NEIN, DESHALB IST ES AUCH WICHTIG, RICHTLINIEN ZU VERBESSERN.
DOKUMENTATIONEN SOLLTEN EINFACH ZUGÄNGLICH, KLAR STRUKTURIERT UND VERSTÄNDLICH SEIN. WAS LOGISCH KLINGT, IST IN DER PRAXIS SCHNELL EINE GROSSE HERAUSFORDERUNG.
WAS KANNST DU NOCH FÜR DIE ENTWICKLER*INNEN TUN?
DAS IST AUFGERÄUMTER ALS DEIN SCHREIBTISCH. AUSSERDEM MAG ICH HARD- UND SOFTWAREBIBLIOTHEKEN.
KI
DER EINSATZ VON UNTERSTÜTZENDEN TOOLS VERBREITET SICH IMMER WEITER.
DAS REICHT VON TOOLS ZUM PRÜFEN VON CODE, UM DIE QUALITÄT SICHERZUSTELLEN, BIS HIN ZU KI-TOOLS, DIE DEN GESAMTEN ENTWICKLUNGSPROZESS VON SOFTWAREPRODUKTEN VEREINFACHEN.


KI
TROTZDEM IST ES WICHTIG, DASS DAS ERGEBNIS VON DEN ENTWICKLER*INNEN, DIE DIESE WERKZEUGE VERWENDEN, VERSTANDEN UND BEWERTET WIRD.
UM SICHERHEITSMASSNAHMEN IM PROZESS ZU VERANKERN, IST ES SINNVOLL, DEN NUTZER*INNEN DAS WISSEN DARÜBER NÄHER ZU BRINGEN UND MITARBEITENDE ZU SOGENANNTEN SECURITY CHAMPIONS ZU MACHEN.
INTERESSIERTE MITARBEITENDE KÖNNTEN GESCHULT UND SO ZU ANSPRECHPARTNER*INNEN FÜR ALLTÄGLICHE SICHERHEITS- UND DATENSCHUTZFRAGEN WERDEN.
ZERTIFIKAT
GENAU! DADURCH KANN DIE HEMMSCHWELLE, UM HILFE ZU BITTEN, GESENKT UND DIE SICHERHEIT IN DEN ALLTAG DER ENTWICKLERTEAMS INTEGRIERT WERDEN.
ALS FORSCHENDE HABEN WIR UNS DAS ZIEL GESETZT, IT-FACHLEUTEN BEI DER BEWÄLTIGUNG VON HERAUSFORDERUNGEN IN DER CYBERSICHERHEIT ZU HELFEN.

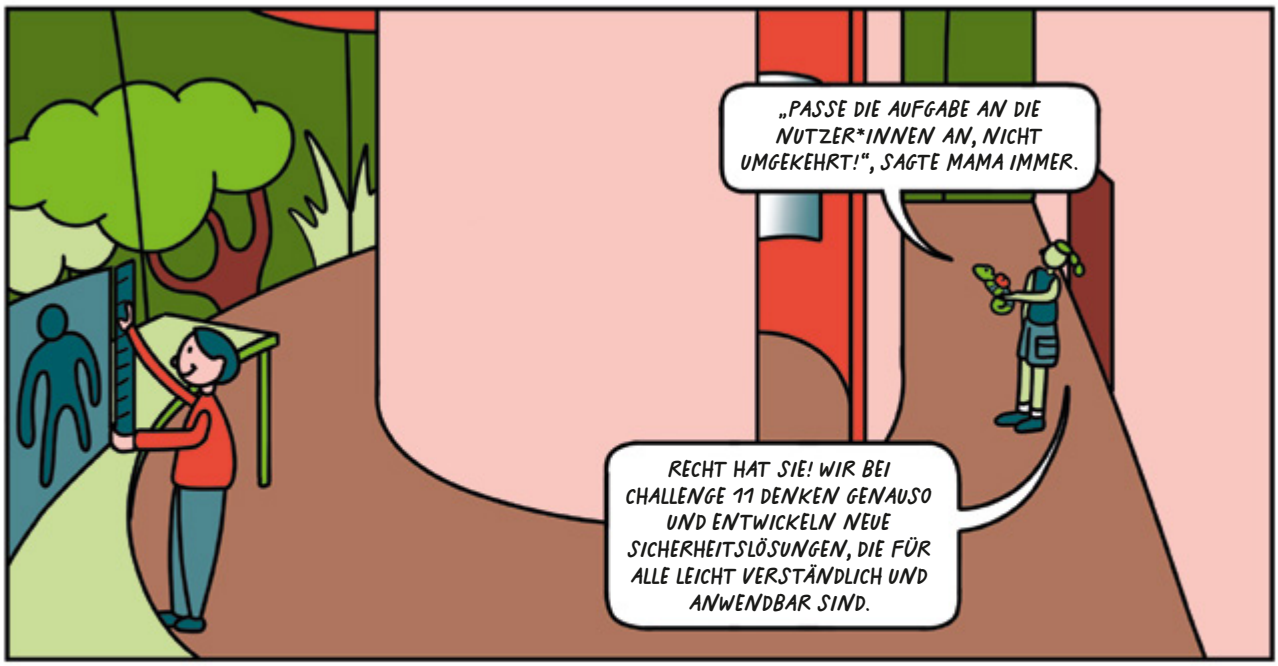

DAHER IST ES EXTREM WICHTIG, DASS WIR VERSTEHEN, WIE DIE VERSCHIEDENEN GRUPPEN ARBEITEN, VOR WELCHEN HERAUSFORDERUNGEN SIE TÄGLICH STEHEN UND WIE WIR SIE DABEI UNTERSTÜTZEN KÖNNEN.
VERSTEHE! DU ACHTEST NICHT NUR AUF TECHNISCHE HERAUSFORDERUNGEN SONDERN AUCH AUF DEN MENSCHLICHEN FAKTOR.
RICHTIG! IN UNSEREM TEAM LIEGT DER SCHWERPUNKT AUF DEN ENTWICKLER*INNEN. DIE ANWENDER*INNEN SIND EINE ANDERE SPANNENDE GRUPPE.
IM NÄCHSTEN GEBÄUDE ERFÄHRST DU MEHR DAZU.
DANKE! DAS WAR WIRKLICH ERHELLEND!
VIELLEICHT IST SECURITY CHAMPION ZU WERDEN GENAUSO ERSTREBENSWERT... WIE DIESE LECKERE FLIEGE HIER.

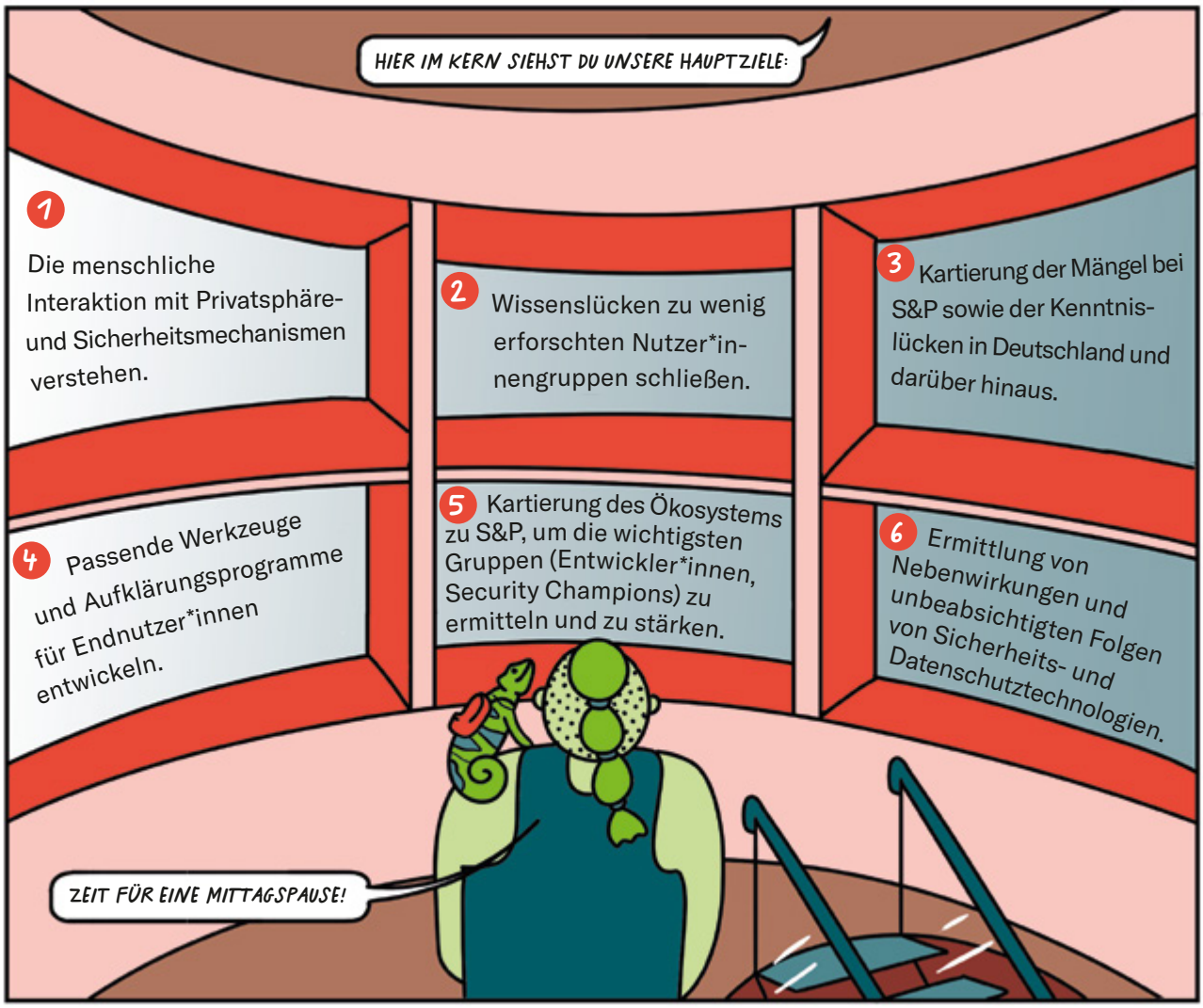
CHALLENGE 11

ANWENDER*INNEN & NUTZBARE SICHERHEIT




HEY LEUTE, BEGRÜSST MAL MAGGIE, SIE WIRD UNS AUSHELFEN.
http:
ALSO, ERKENNST DU HIER AUF DER WEBSEITE IRGENDEIN PROBLEM?
HMM, DIE URL BEGINNT MIT „HTTP:“ UND NICHT MIT „HTTPS:“, DAS BEDEUTET, DASS DIE VERBINDUNG NICHT SICHER UND INTEGER IST.
PRIMA AUFGEPASST! GUT GEMACHT!
ICH FINDE GUT, DASS IHR SOFTWARE TESTET UND NICHT DIE NUTZER*INNEN.
DANKE! LEIDER HÄLT SICH DAS NEGATIVE BILD VON DEN NUTZER*INNEN ALS SCHWACHSTELLE IMMER NOCH HARTNÄCKIG.
SIE FÜHLEN SICH DANN UNZULÄNGLICH UND ALS RISIKOFAKTOR.
30 JAHRE FORSCHUNG HABEN GEZEIGT, DASS VERHALTENSÄNDERUNGEN VIEL KOMPLEXER SIND ALS DIE TECHNOLOGIE ANZUPASSEN. DAS KÖNNTE DEN MENSCHEN HELFEN, DEN SICHEREN WEG ZU WÄHLEN.
MIR GEFÄLLT DER NEUE UMHANG AUCH SO!


„PASSE DIE AUFGABE AN DIE NUTZER*INNEN AN, NICHT UMGEKEHRT!“, SAGTE MAMA IMMER.
RECHT HAT SIE! WIR BEI CHALLENGE 11 DENKEN GENAUSO UND ENTWICKELN NEUE SICHERHEITSLÖSUNGEN, DIE FÜR ALLE LEICHT VERSTÄNDLICH UND ANWENDBAR SIND.


HIER IM KERN SIEHST DU UNSERE HAUPTZIELE:
1 Die menschliche Interaktion mit Privatsphäre- und Sicherheitsmechanismen verstehen.
2 Wissenslücken zu wenig erforschten Nutzer*innengruppen schließen.
3 Kartierung der Mängel bei S&P sowie der Kenntnislücken in Deutschland und darüber hinaus.
4 Passende Werkzeuge und Aufklärungsprogramme für Endnutzer*innen entwickeln.
5 Kartierung des Ökosystems zu S&P, um die wichtigsten Gruppen (Entwickler*innen, Security Champions) zu ermitteln und zu stärken.
6 Ermittlung von Nebenwirkungen und unbeabsichtigten Folgen von Sicherheits- und Datenschutztechnologien.
ZEIT FÜR EINE MITTAGSPAUSE!

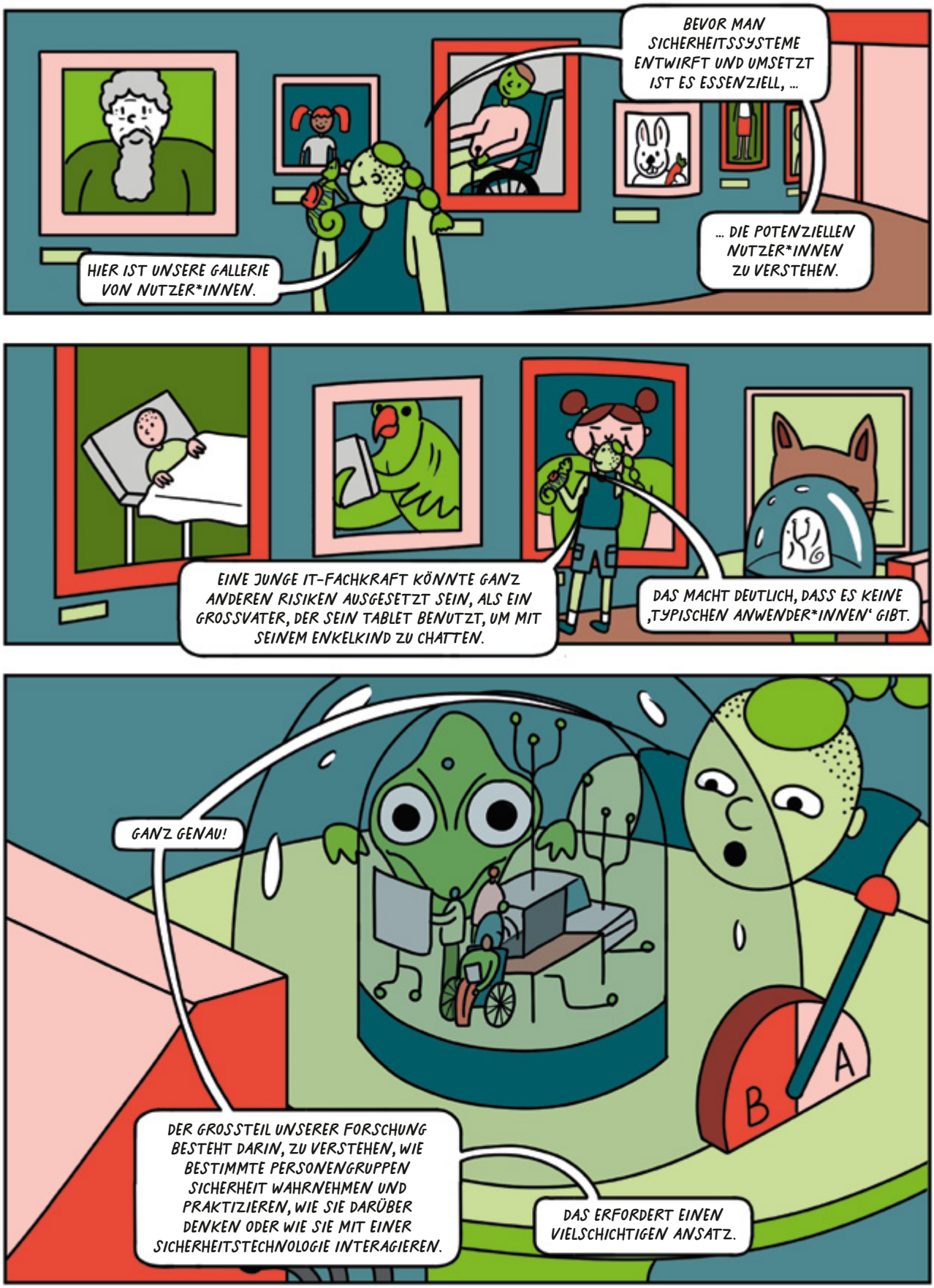
CASA WIKI

Co-Design ist ein partizipativer, mitgestaltender und offener Designprozess, der die Nutzer*innen als Expert*innen und Vermittler*innen einbezieht. Er zielt darauf ab, Ideen zu entwickeln, die die Bedürfnisse der Anwender*innen verbessern, Lösungen zu validieren und bessere Beziehungen zu schaffen.

Creative Engagements sind Methoden zur Einbeziehung von Nutzer*innen und Interessenvertreter*innen in die Erforschung, Gestaltung und Bewertung von Sicherheits- und Datenschutzmechanismen unter Verwendung kreativer Methoden und Werkzeuge (z.B. Lego, Zeichnen, Performance, Collagen). Sie helfen dabei, die Bedürfnisse der Anwender*innen zu verstehen, innovative Ideen zu entwickeln und die Menschen in den Prozess einzubeziehen.

HCI (Human-Computer Interaction) ist die Forschung im Bereich der Gestaltung und Nutzung von Computertechnologie. Sie interessiert sich dafür, wie Menschen mit Computern interagieren und entwickelt neue Technologien (z. B. Computermaus, Touchscreens).

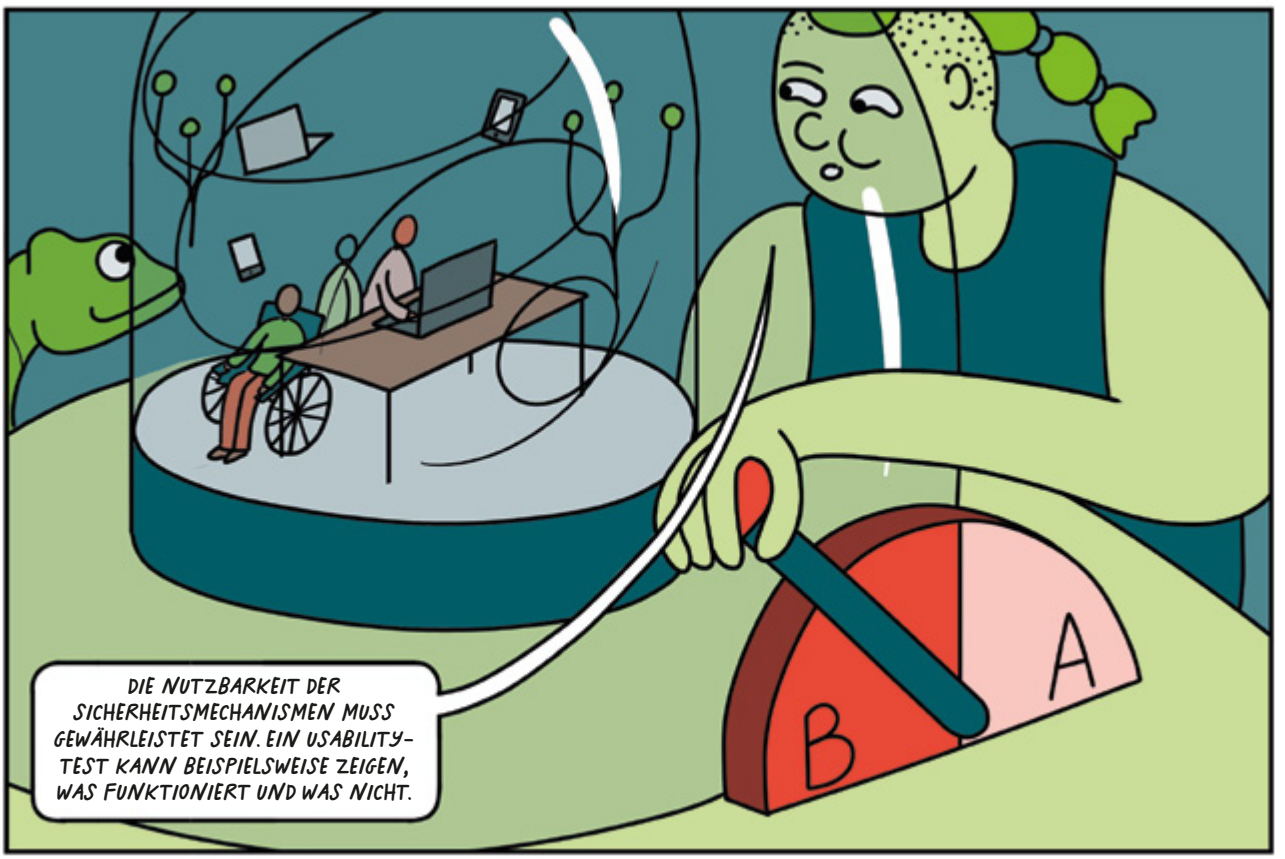
Eine **User Journey** beschreibt eine Methode, die Aufschluss darüber gibt, welche Erfahrungen eine Person bei der Interaktion mit Technik macht. Sie kommt typischerweise bei der Entwicklung von Software zum Einsatz.

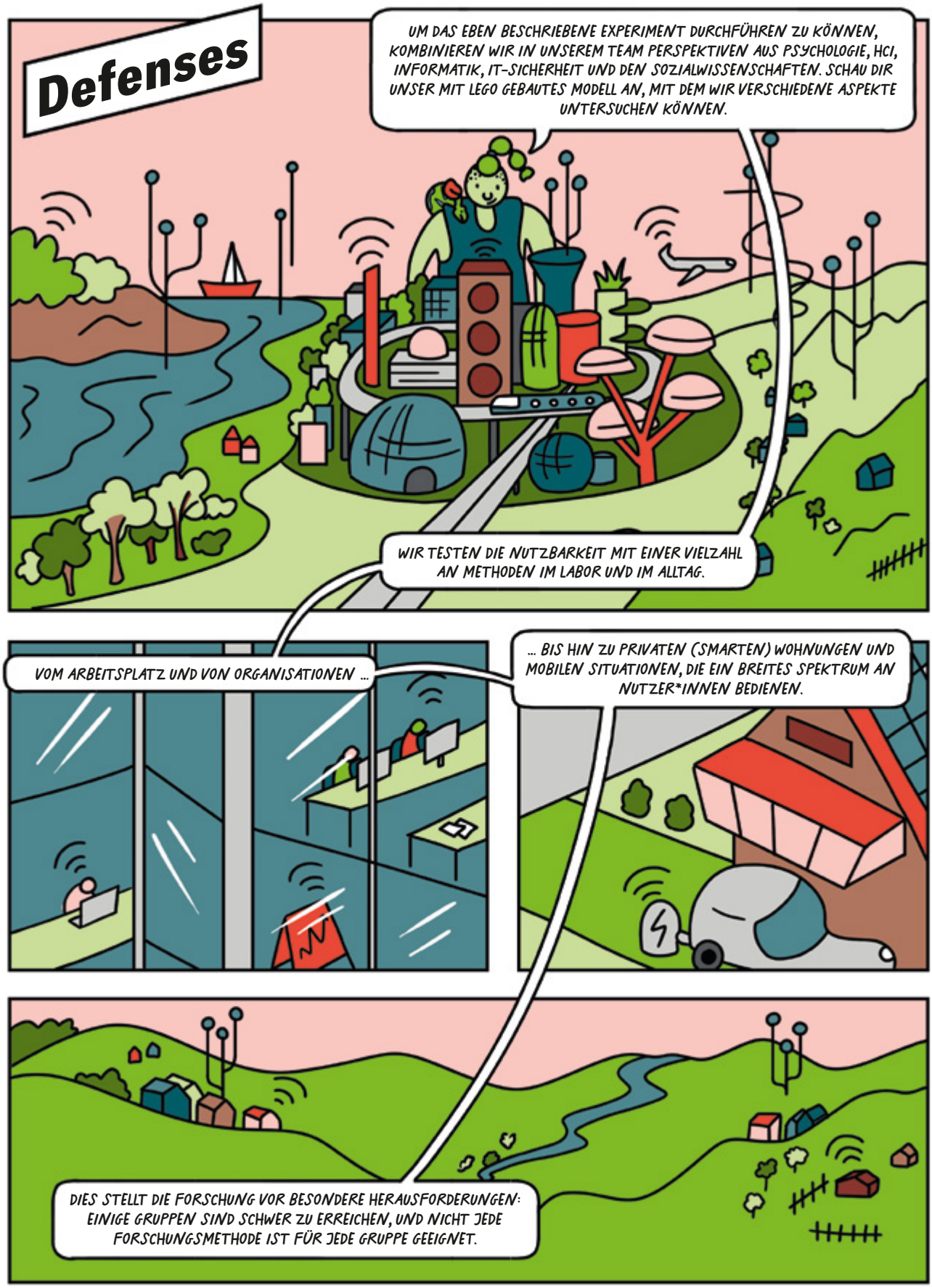

BEVOR MAN SICHERHEITSSYSTEME ENTWIRFT UND UMSETZT IST ES ESSENZIELL, ...
... DIE POTENZIELLEN NUTZER*INNEN ZU VERSTEHEN.
HIER IST UNSERE GALLERIE VON NUTZER*INNEN.
EINE JUNGE IT-FACHKRAFT KÖNNTE GANZ ANDEREN RISIKEN AUSGESETZT SEIN, ALS EIN GROSSVATER, DER SEIN TABLET BENUTZT, UM MIT SEINEM ENKELKIND ZU CHATTEN.
DAS MACHT DEUTLICH, DASS ES KEINE ‚TYPISCHEN ANWENDER*INNEN' GIBT.
GANZ GENAU!
DER GROSSTEIL UNSERER FORSCHUNG BESTEHT DARIN, ZU VERSTEHEN, WIE BESTIMMTE PERSONENGRUPPEN SICHERHEIT WAHRNEHMEN UND PRAKTIZIEREN, WIE SIE DARÜBER DENKEN ODER WIE SIE MIT EINER SICHERHEITSTECHNOLOGIE INTERAGIEREN.
DAS ERFORDERT EINEN VIELSCHICHTIGEN ANSATZ.
B
A

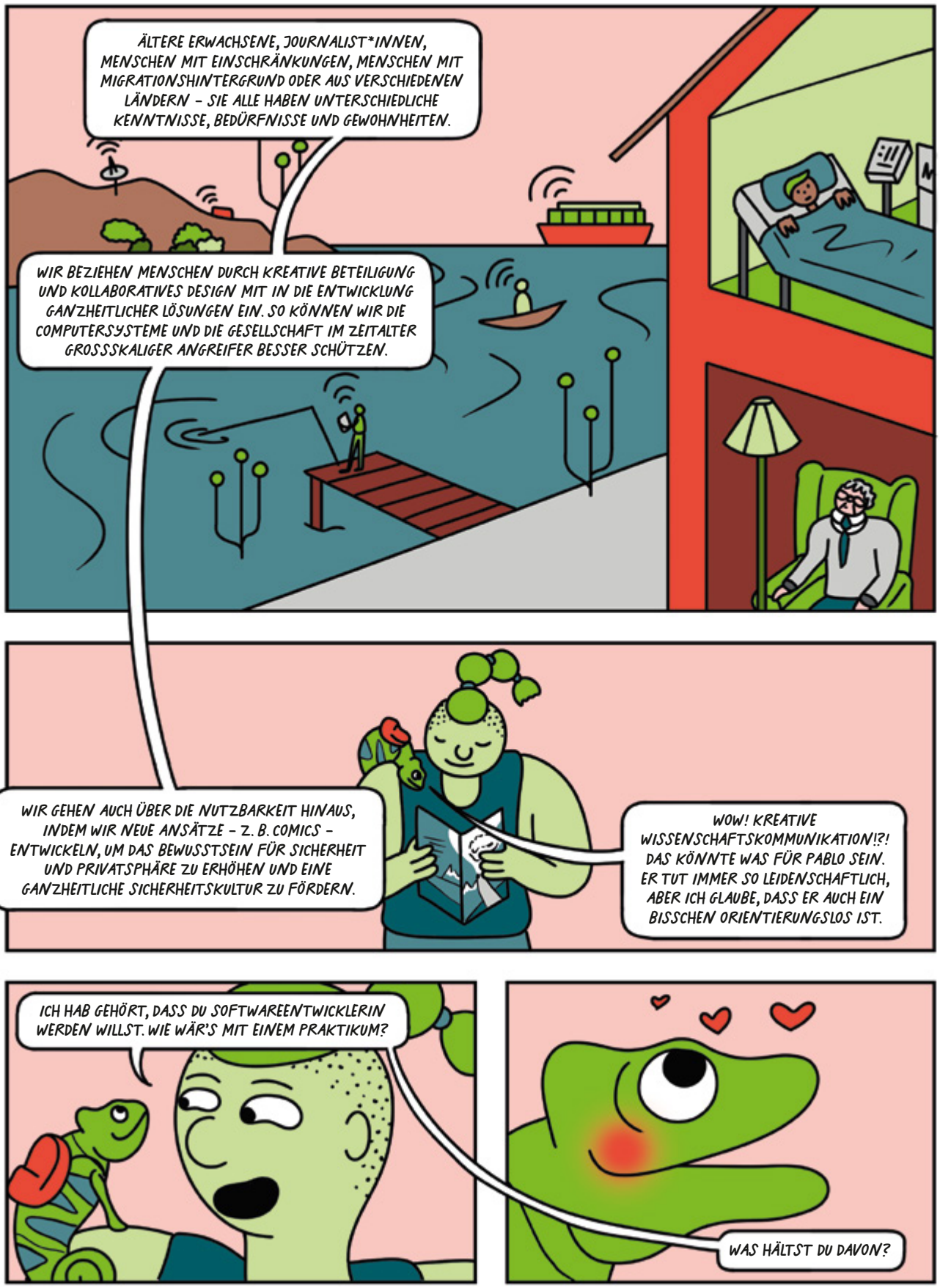
REAL LIFE STORY

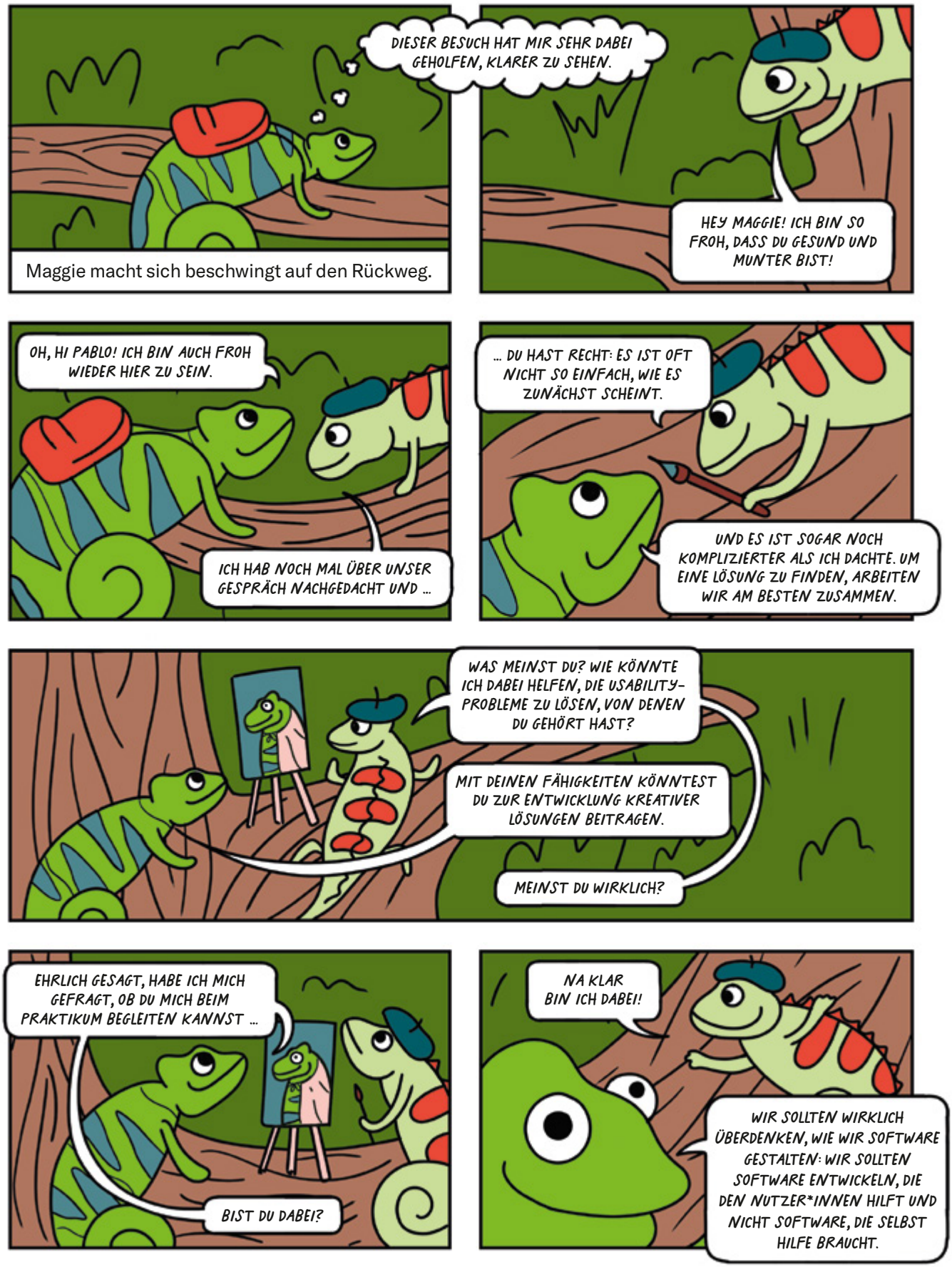
Makros sind kleiner ausführbarer Code, der in Microsoft Office-Dateien eingebettet ist. Sie können genutzt werden, um Computer mit Viren zu infizieren. Sie sind standardmäßig deaktiviert, aber beim Öffnen eines Dokuments mit Makros erhalten die Nutzenden eine Warnmeldung – und die Möglichkeit, sie mit einem Klick zu aktivieren.

Eine Studie ergab, dass fast ⅔ der Teilnehmer*innen ein potenziell gefährliches Makro aktivierten, weil es nur ein einziger Mausklick war. Auf Nachfrage hatten die Teilnehmenden oft keine Ahnung, wie Makros funktionieren und dass sie eine Sicherheitsbedrohung darstellen können.




Defenses
UM DAS EBEN BESCHRIEBENE EXPERIMENT DURCHFÜHREN ZU KÖNNEN, KOMBINIEREN WIR IN UNSEREM TEAM PERSPEKTIVEN AUS PSYCHOLOGIE, HCI, INFORMATIK, IT-SICHERHEIT UND DEN SOZIALWISSENSCHAFTEN. SCHAU DIR UNSER MIT LEGO GEBAUTES MODELL AN, MIT DEM WIR VERSCHIEDENE ASPEKTE UNTERSUCHEN KÖNNEN.
WIR TESTEN DIE NUTZBARKEIT MIT EINER VIELZAHL AN METHODEN IM LABOR UND IM ALLTAG.
VOM ARBEITSPLATZ UND VON ORGANISATIONEN ...
... BIS HIN ZU PRIVATEN (SMARTEN) WOHNUNGEN UND MOBILEN SITUATIONEN, DIE EIN BREITES SPEKTRUM AN NUTZER*INNEN BEDIENEN.
DIES STELLT DIE FORSCHUNG VOR BESONDERE HERAUSFORDERUNGEN: EINIGE GRUPPEN SIND SCHWER ZU ERREICHEN, UND NICHT JEDE FORSCHUNGSMETHODE IST FÜR JEDE GRUPPE GEEIGNET.


ÄLTERE ERWACHSENE, JOURNALIST*INNEN, MENSCHEN MIT EINSCHRÄNKUNGEN, MENSCHEN MIT MIGRATIONSHINTERGRUND ODER AUS VERSCHIEDENEN LÄNDERN – SIE ALLE HABEN UNTERSCHIEDLICHE KENNTNISSE, BEDÜRFNISSE UND GEWOHNHEITEN.
WIR BEZIEHEN MENSCHEN DURCH KREATIVE BETEILIGUNG UND KOLLABORATIVES DESIGN MIT IN DIE ENTWICKLUNG GANZHEITLICHER LÖSUNGEN EIN. SO KÖNNEN WIR DIE COMPUTERSYSTEME UND DIE GESELLSCHAFT IM ZEITALTER GROSSSKALIGER ANGREIFER BESSER SCHÜTZEN.
WIR GEHEN AUCH ÜBER DIE NUTZBARKEIT HINAUS, INDEM WIR NEUE ANSÄTZE – Z. B. COMICS – ENTWICKELN, UM DAS BEWUSSTSEIN FÜR SICHERHEIT UND PRIVATSPHÄRE ZU ERHÖHEN UND EINE GANZHEITLICHE SICHERHEITSKULTUR ZU FÖRDERN.
WOW! KREATIVE WISSENSCHAFTSKOMMUNIKATION!?! DAS KÖNNTE WAS FÜR PABLO SEIN. ER TUT IMMER SO LEIDENSCHAFTLICH, ABER ICH GLAUBE, DASS ER AUCH EIN BISSCHEN ORIENTIERUNGSLOS IST.
ICH HAB GEHÖRT, DASS DU SOFTWAREENTWICKLERIN WERDEN WILLST. WIE WÄR'S MIT EINEM PRAKTIKUM?
WAS HÄLTST DU DAVON?


DIESER BESUCH HAT MIR SEHR DABEI GEHOLFEN, KLARER ZU SEHEN.
Maggie macht sich beschwingt auf den Rückweg.
HEY MAGGIE! ICH BIN SO FROH, DASS DU GESUND UND MUNTER BIST!
OH, HI PABLO! ICH BIN AUCH FROH WIEDER HIER ZU SEIN.
ICH HAB NOCH MAL ÜBER UNSER GESPRÄCH NACHGEDACHT UND ...
... DU HAST RECHT: ES IST OFT NICHT SO EINFACH, WIE ES ZUNÄCHST SCHEINT.
UND ES IST SOGAR NOCH KOMPLIZIERTER ALS ICH DACHTE. UM EINE LÖSUNG ZU FINDEN, ARBEITEN WIR AM BESTEN ZUSAMMEN.
WAS MEINST DU? WIE KÖNNTE ICH DABEI HELFEN, DIE USABILITY-PROBLEME ZU LÖSEN, VON DENEN DU GEHÖRT HAST?
MIT DEINEN FÄHIGKEITEN KÖNNTEST DU ZUR ENTWICKLUNG KREATIVER LÖSUNGEN BEITRAGEN.
MEINST DU WIRKLICH?
EHRLICH GESAGT, HABE ICH MICH GEFRAGT, OB DU MICH BEIM PRAKTIKUM BEGLEITEN KANNST ...
BIST DU DABEI?
NA KLAR BIN ICH DABEI!
WIR SOLLTEN WIRKLICH ÜBERDENKEN, WIE WIR SOFTWARE GESTALTEN: WIR SOLLTEN SOFTWARE ENTWICKELN, DIE DEN NUTZER*INNEN HILFT UND NICHT SOFTWARE, DIE SELBST HILFE BRAUCHT.

ÜBER CASA

CASA: Cyber Security in the Age of Large-Scale Adversaries wurde 2019 gegründet und ist das einzige Exzellenzcluster im Bereich IT-Sicherheit in Deutschland. Von der Deutschen Forschungsgemeinschaft (DFG) wird CASA mit 30 Millionen Euro über sieben Jahre hinweg gefördert, um ausgezeichnete Forschungsbedingungen zu garantieren. Bei CASA arbeitet eine Kerngruppe führender Forscher*innen mit einem klaren Fokus auf Sicherheit und Datenschutz eng mit ausgewählten Spitzenforscher*innen aus hochrelevanten Nachbardisziplinen zusammen. Dabei deckt das Team sämtliche Disziplinen ab, die erforderlich sind, um die anspruchsvollen Forschungsprobleme im Bereich der modernen IT-Sicherheit zu bewältigen, darunter Informatik, Mathematik, Elektrotechnik und Psychologie.

CASA ist am Horst-Görtz-Institut für IT-Sicherheit (hgi.rub.de) angesiedelt, einem wegweisenden Forschungsinstitut in Deutschland. Außerdem arbeitet CASA eng mit dem Max-Planck-Institut für Sicherheit und Privatsphäre in Bochum (mpi-sp.org) und zahlreichen weiteren Instituten und Universitäten zusammen.

Was ist ein „Exzellenzcluster“?
Mit der Förderlinie „Exzellenzcluster“ werden international wettbewerbsfähige Forschungszentren an Universitäten oder Universitätsverbünden in Deutschland projektbezogen für einen Zeitraum von sieben Jahren gefördert. Innerhalb dieser Cluster arbeiten Wissenschaftler*innen aus verschiedenen Disziplinen und Institutionen gemeinsam an einem Forschungsprojekt. Die Förderung ermöglicht es ihnen, sich intensiv auf ihr Forschungsziel zu konzentrieren, wissenschaftlichen Nachwuchs auszubilden und internationale Spitzenforscher*innen zu gewinnen.

casa.rub.de

TECHNISCHER BACKGROUND

Die in diesem Comic vorgestellten Konzepte und Methoden wurden von den am Exzellenzcluster CASA mitwirkenden Forscher*innen entwickelt. Die Originalveröffentlichungen sind online verfügbar und geben detaillierte Einblicke in ihre Forschung. Zusätzlich veröffentlichen wir zu vielen Publikationen den Quellcode und weitere Forschungsergebnisse. Bei Fragen stehen wir gerne zur Verfügung: info@casa.rub.de

PUBLIKATIONEN

Lisa Geierhaas, Anna-Marie Ortloff, Matthew Smith, Alena Naiakshina: **Let’s Hash: Helping Developers with Password Security,** Symposium on Usable Privacy and Security (SOUPS), 2022.

Stefan Albert Horstmann, Samuel Domiks, Marco Gutfleisch, Mindy Tran, Yasemin Acar, Veelasha Moonsamy, Alena Naiakshina: **Those things are written by lawyers, and programmers are reading that. Mapping the Communication Gap Between Software Developers and Privacy Experts,** Privacy Enhancing Technologies Symposium (PETS), 2024.

Jan H. Klemmer, Marco Gutfleisch, Christian Stransky, Yasemin Acar, M. Angela Sasse, Sascha Fahl: **“Make Them Change it Every Week”: A Qualitative Exploration of Online Developer Advice on Usable and Secure Authentication,** The ACM Conference on Computer and Communications Security (CCS), 2023.

Marco Gutfleisch, Jan H. Klemmer, Niklas Busch, Yasemin Acar, M. Angela Sasse, Sascha Fahl: **How Does Usable Security (Not) End Up in Software Products? Results From a Qualitative Interview Study,** IEEE Symposium on Security and Privacy (S&P), 2022.

Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, M. Angela Sasse, Yasemin Acar, Markus Dürmuth: **A World Full of Privacy and Security (Mis)conceptions? Findings of a Representative Survey in 12 Countries,** Conference on Human Factors in Computing Systems (CHI), 2023.

Ahmet Erinola, Annalina Buckmann, Jennifer Friedauer, Aslı Yardım, M. Angela Sasse: **“As Usual, I Needed Assistance of a Seeing Person”: Experiences and Challenges of People with Disabilities and Authentication Methods,** IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2023.

Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, M. Angela Sasse: **Digital Security - A Question of Perspective. A Large-Scale Telephone Survey with Four At-Risk User Groups,** IEEE Symposium on Security and Privacy (S&P), 2023.

Mark Turner, Martin Schmitz, Morgan Masichi Bierey, Mohamed Khamis, Karola Marky: **Tangible 2FA – An In-the-Wild Investigation of User-Defined Tangibles for Two-Factor Authentication,** Symposium on Usable Privacy and Security (SOUPS), 2023.

CASA HUB D

1. Auflage 2025

Redaktion
Mirjam Stricker (CASA / Ruhr-Universität Bochum)
Annika Gödde (CASA / Ruhr-Universität Bochum)
Niels Jansen (Ellery Studio)
Alena Naiakshina (CASA / Ruhr-Universität Bochum)
Stefan Horstmann (CASA / Ruhr-Universität Bochum)
Felix Reichmann (CASA / Ruhr-Universität Bochum)
Aslı Yardım (CASA / Ruhr-Universität Bochum)
M. Angela Sasse (CASA / Ruhr-Universität Bochum)
Annalina Buckmann (CASA / Ruhr-Universität Bochum)
Konstantin Fischer (CASA / Ruhr-Universität Bochum)
Marco Gutfleisch (CASA / Ruhr-Universität Bochum)
Franziska Herbert (CASA / Ruhr-Universität Bochum)
Marvin Kowalewski (CASA / Ruhr-Universität Bochum)
Karola Marky (CASA / Ruhr-Universität Bochum)
Priyasha Chatterjee (CASA / Ruhr-Universität Bochum)
Yixin Zou (CASA / Max-Planck-Institut für Sicherheit und Privatsphäre)

Ellery Studio
Illustration: Lucía Cordero, Hannah Schrage
Design: Yasemin Çakır
Projektmanagement: Niels Jansen

Umschlaggestaltung
Hannah Schrage

Druck
Schmidt, Ley + Wiegandt GmbH + Co. KG,
Lünen, www.slw-medien.de

Herausgeber
CASA: Cyber Security in the Age
of Large-Scale Adversaries
Universitätsstraße 150
44780 Bochum

hgi-presse@rub.de
casa.rub.de

Scanne den QR-Code, um zur digitalen Version dieses Comics und zu den Comics (Englisch/Deutsch) der anderen Research HUBs zu gelangen:

Auf Englisch sind folgende Comics erschienen:

- The Secrets of HUB A and the Traces of the Cookies
- A Deep Dive Into HUB B and the Swirl of Embedded Security
- What's the Fuzz About HUB C and the Missing Carrots?
- HUB D and the Rumble in the Jungle of Usability

CASA
Cyber Security in the Age of Large-Scale Adversaries

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

RUHR UNIVERSITÄT BOCHUM
RUB

ellery studio

WIE KÖNNEN IT-SPEZIALIST*INNEN UND SICHERHEITSEXPERT*INNEN IHRE FÄHIGKEITEN AM BESTEN KOMBINIEREN? WELCHE WERKZEUGE KÖNNEN HELFEN, DEM ZIEL VON SICHERHEIT UND PRIVATSPHÄRE BY DESIGN NÄHER ZU KOMMEN? UND WIE SIEHT ES MIT DER NUTZERFREUNDLICHKEIT FÜR DIE VERSCHIEDENEN GRUPPEN VON ANWENDER*INNEN AUS?

BEGLEITE CHAMÄLEON MAGGIE AUF IHRER SUCHE NACH EINEM ERFÜLLENDEN BERUF. WIRD SIE IM INFORMATIONSDSCHUNGEL DEN ORT DER ERLEUCHTUNG ENTDECKEN?

FINDE ES HERAUS!