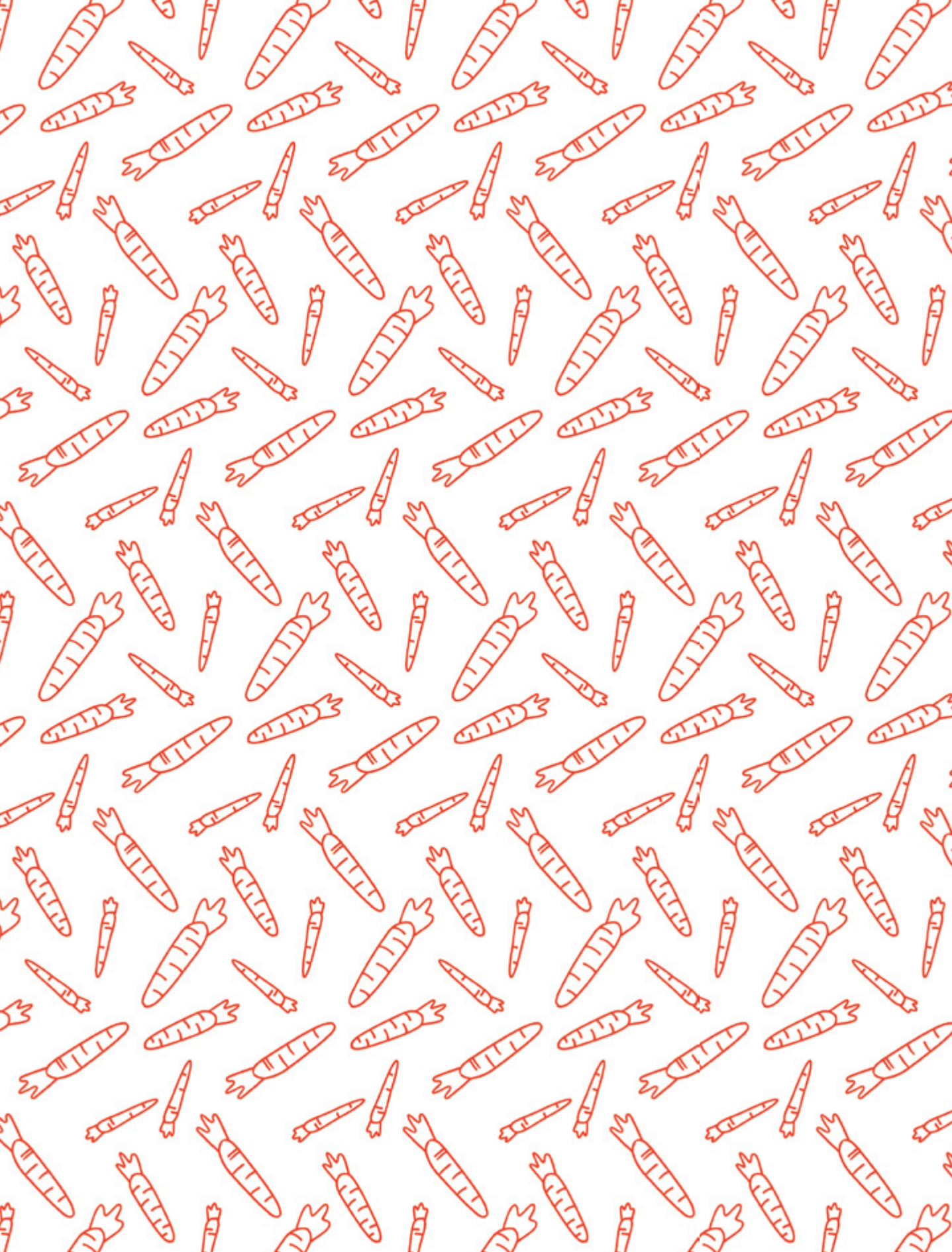
CASA UNIVERSE

WIRBEL UM HUBC UND DIE VERSCHWUNDENEN KAROTTEN

EINE REISE DURCH DIE GEHEIMNISSE SICHERER SYSTEME UND DIE AUFREGENDE FORSCHUNGSWELT VON CASA



WIRBEL UM HUBC UND DIE VERSCHWUNDENEN KAROTTEN

EINE REISE DURCH DIE GEHEIMNISSE
SICHERER SYSTEME UND DIE AUFREGENDE
FORSCHUNGSWELT VON CASA

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

CASA

Cyber Security in the Age of Large-Scale Adversaries

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 national-staatliche 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“: Stärkung der Sicherheit eingebetteter Systeme auf der Hardware-Ebene durch die Untersuchung 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.

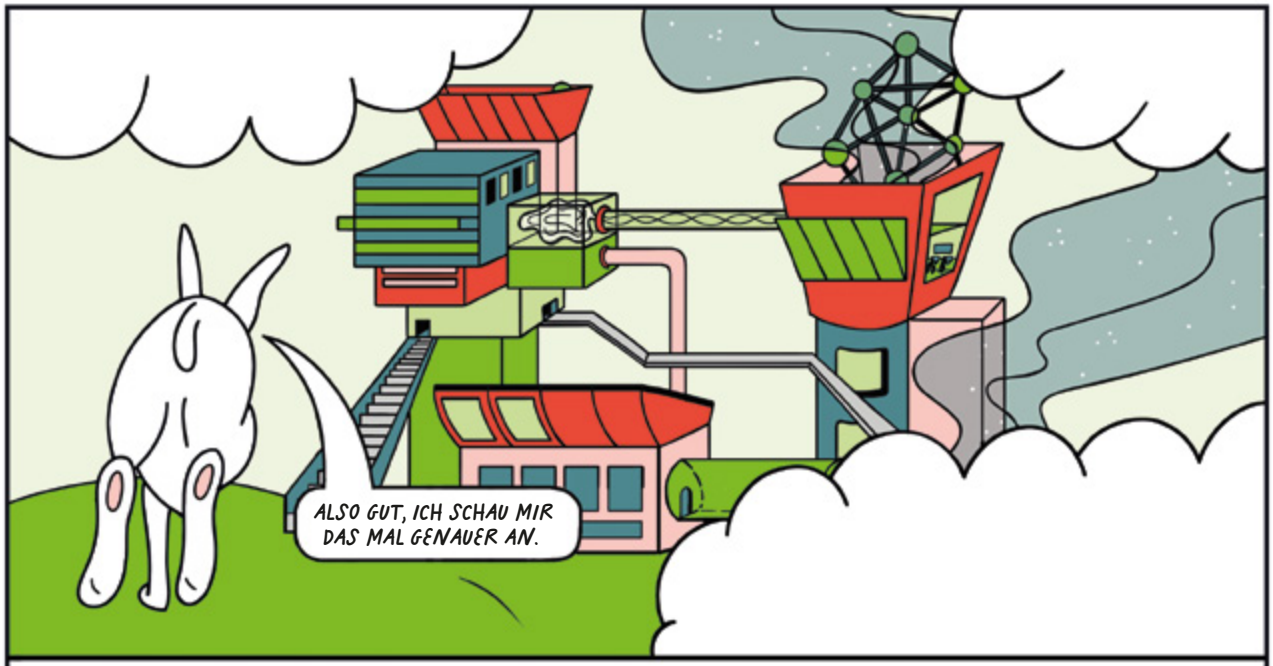
HUB D „Usability“: Konzentration auf benutzerfreundliche Sicherheit und Privatsphäre sowie die Erforschung der Schnittstelle zwischen Mensch und Technik.

Jedes 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.

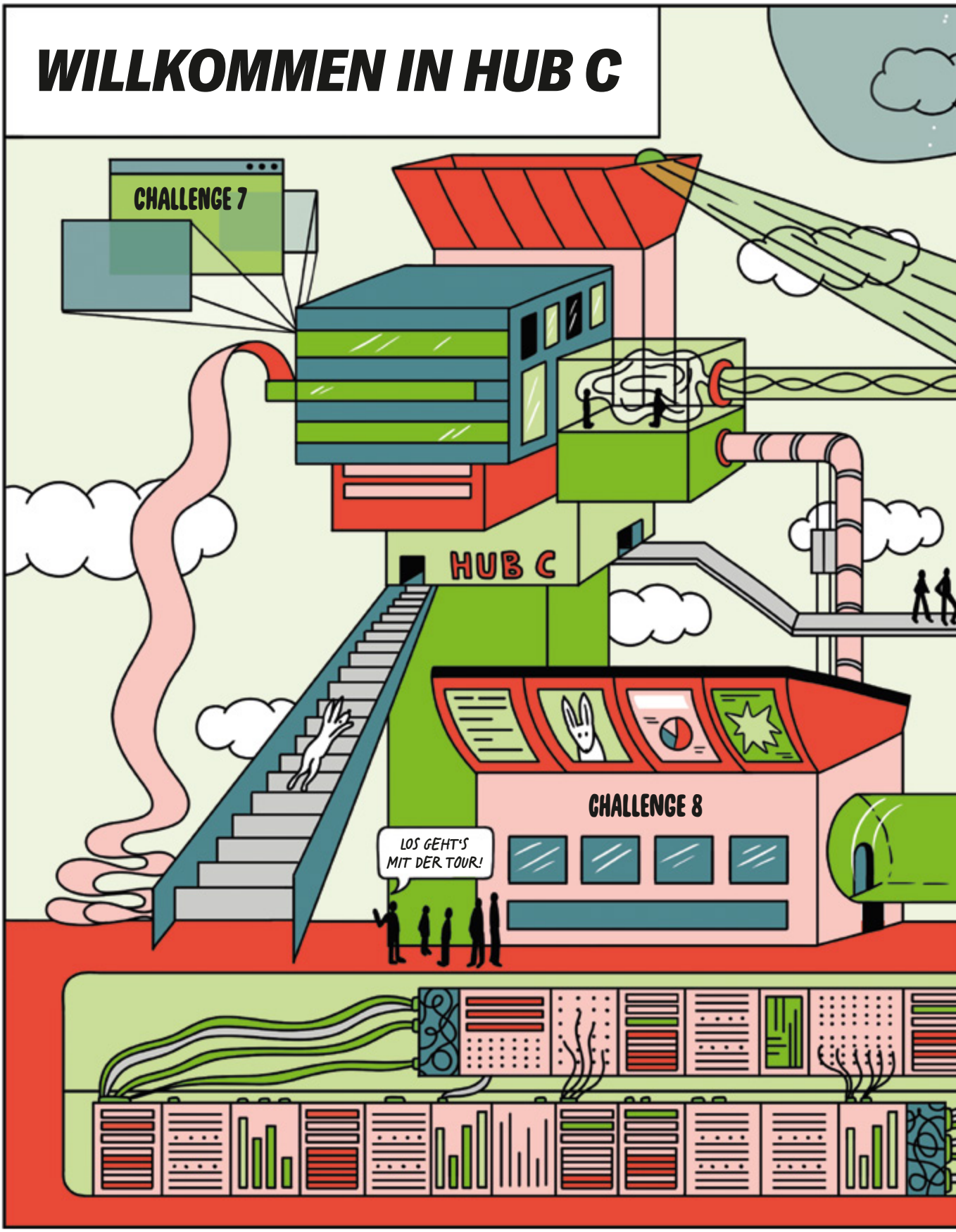
Die Challenges des HUB C sind:
Challenge 7: Konstruktion sicherer Systeme
Challenge 8: Sicherheit mit nicht-vertrauenswürdigen Komponenten
Challenge 9: Intelligente Sicherheitssysteme

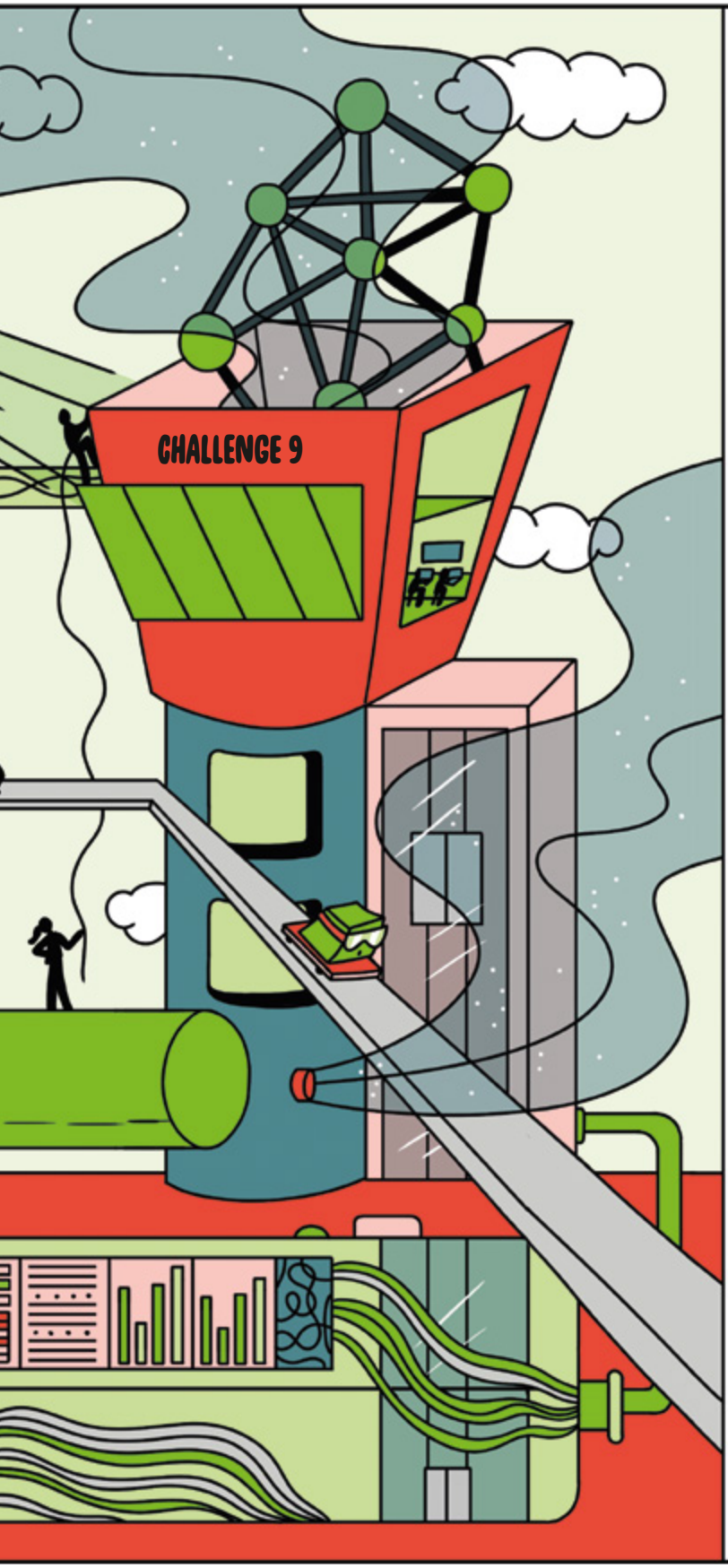
An einem geheimen Ort in unserer Welt verstecken sich die malerischen Hügel des CASA-Universums. In einer Welt, in der sich selbst die Hasenbande digitalen Herausforderungen stellen muss.

Am Fuße der Hügel liegt HUB C. Niemand weiß so genau, was dort vor sich geht. Manche sagen, sie tüfteln dort an neuen Sicherheitssystemen, andere behaupten, sie machen alte Systeme robuster. Aber alle sind sich einig: sie arbeiten an ganz heißem Sch...



Die tapfere Häsin Betty beschließt herauszufinden, was dort wirklich los ist. Damit ihr und dem Rest der Bande nicht dasselbe passiert wie Mark. Sie brauchen ihre Wintervorräte dringend...


WILLKOMMEN IN HUB C
CHALLENGE 7
HUB C
CHALLENGE 8
LOS GEHT'S MIT DER TOUR!



INHALT

CHALLENGE 7

Konstruktion sicherer Systeme
Wie können wir sichere und zuverlässige Systeme entwickeln? Von Grund auf und vertrauenswürdiger als jemals zuvor.

CHALLENGE 8

Sicherheit mit nicht-vertrauenswürdigen Komponenten
Wie können wir Systeme zuverlässig und robust machen und erhalten, auch wenn ältere Hard- und Software verwendet wird?

CHALLENGE 9

Intelligente Sicherheitssysteme
Sicherheit ist ein Prozess, kein Zustand. Wie können wir potentiellen Angriffen zuvorkommen und widerstandsfähig sein, auch wenn Unvorhergesehenes passiert?

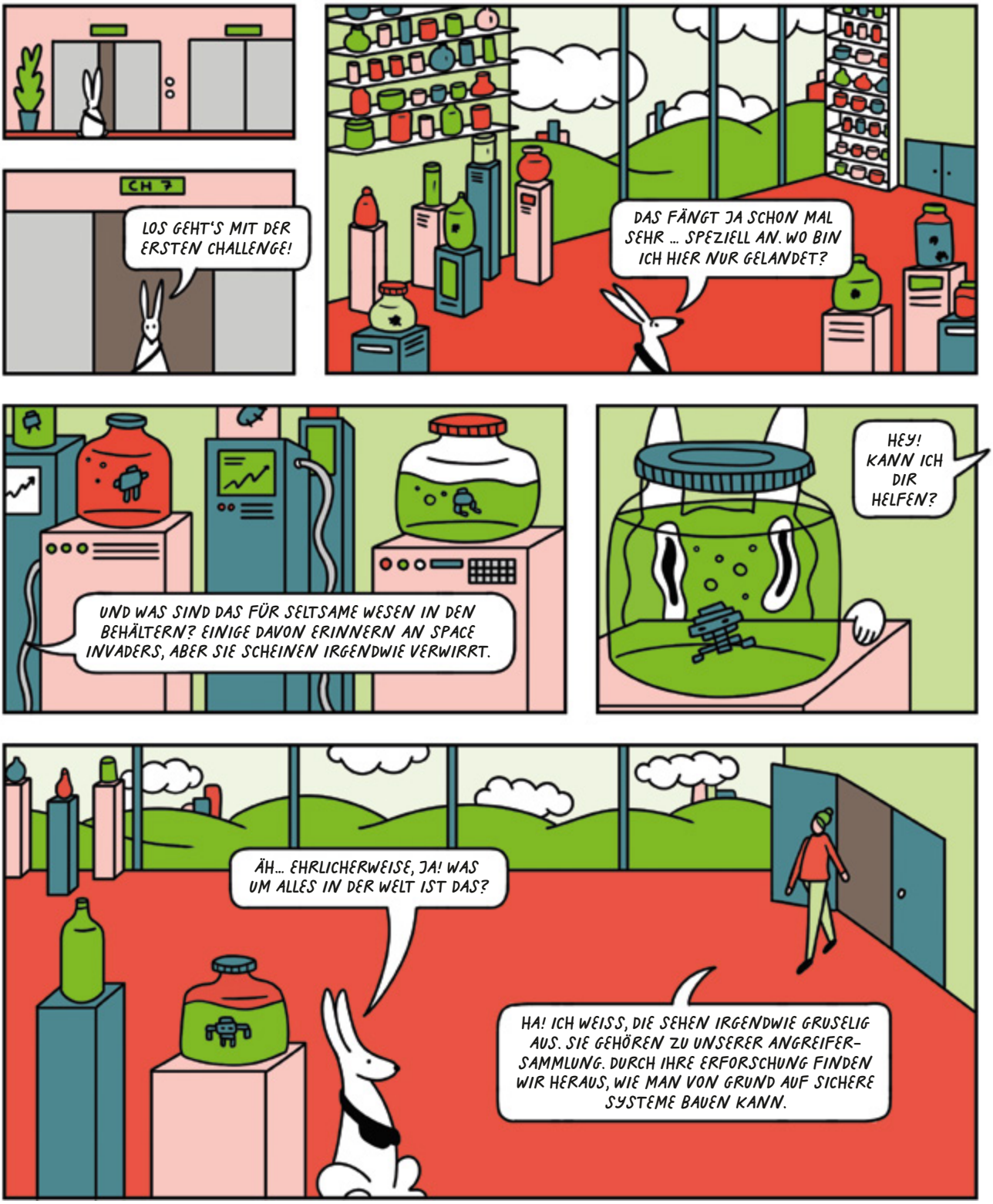
CASA BACKGROUND

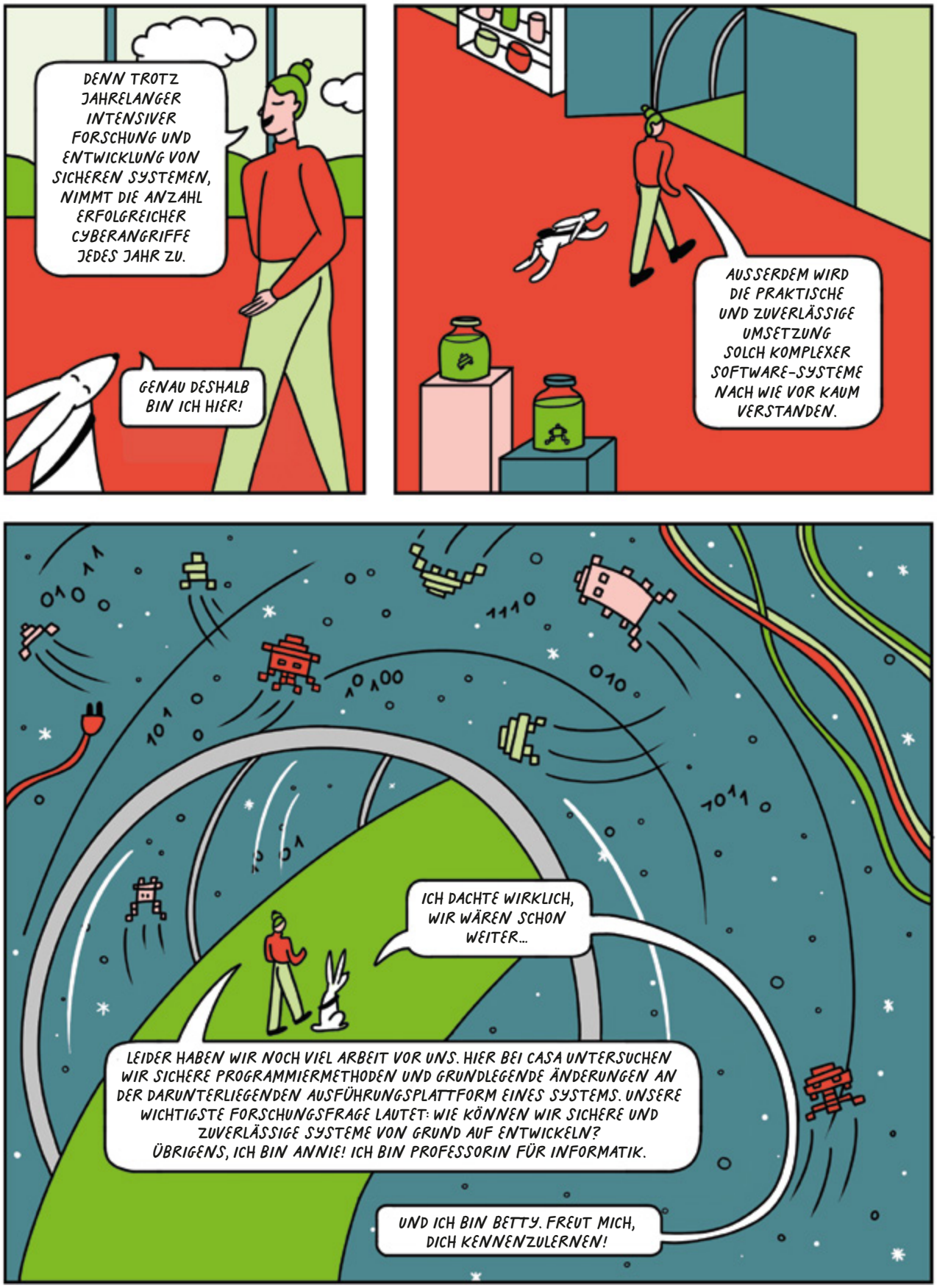
CASA steht für „Cyber Security in the Age of Large-Scale Adversaries“ und wird als Exzellenzcluster im Rahmen der Exzellenzstrategie der DFG gefördert. Ziel ist es, nachhaltige Sicherheitslösungen gegen komplexe, groß angelegte Angriffe zu entwickeln. Dazu erforscht ein interdisziplinäres Team nicht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

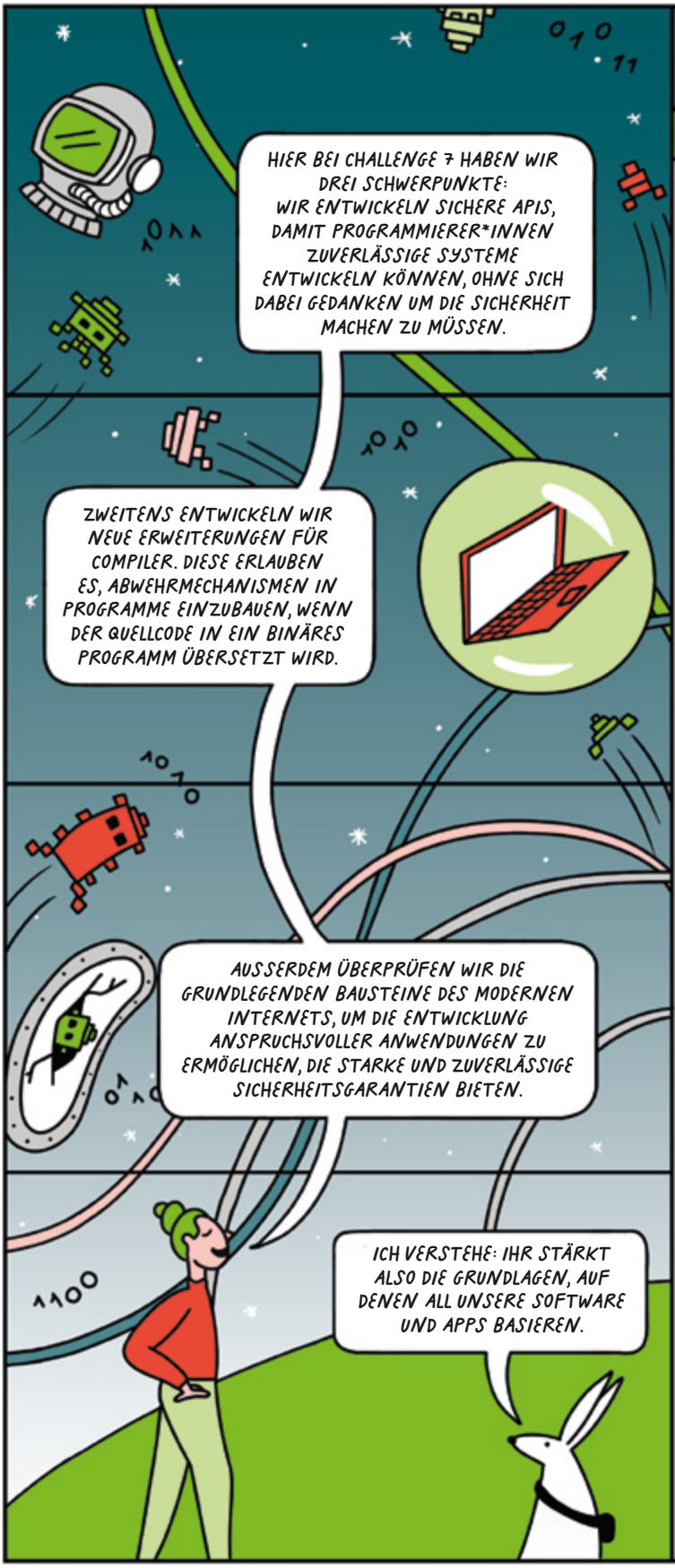
casa.rub.de

CHALLENGE 7

KONSTRUKTION SICHERER SYSTEME




DENN TROTZ JAHRELANGER INTENSIVER FORSCHUNG UND ENTWICKLUNG VON SICHEREN SYSTEMEN, NIMMT DIE ANZAHL ERFOLGREICHER CYBERANGRIFFE JEDES JAHR ZU.
GENAU DESHALB BIN ICH HIER!
AUSSERDEM WIRD DIE PRAKTISCHE UND ZUVERLÄSSIGE UMSETZUNG SOLCH KOMPLEXER SOFTWARE-SYSTEME NACH WIE VOR KAUM VERSTANDEN.
ICH DACHTE WIRKLICH, WIR WÄREN SCHON WEITER...
LEIDER HABEN WIR NOCH VIEL ARBEIT VOR UNS. HIER BEI CASA UNTERSUCHEN WIR SICHERE PROGRAMMIERMETHODEN UND GRUNDLEGENDE ÄNDERUNGEN AN DER DARUNTERLIEGENDEN AUSFÜHRUNGSPLATTFORM EINES SYSTEMS. UNSERE WICHTIGSTE FORSCHUNGSFRAGE LAUTET: WIE KÖNNEN WIR SICHERE UND ZUVERLÄSSIGE SYSTEME VON GRUND AUF ENTWICKELN?
ÜBRIGENS, ICH BIN ANNIE! ICH BIN PROFESSORIN FÜR INFORMATIK.
UND ICH BIN BETTY. FREUT MICH, DICH KENNENZULERNEN!



CASA WIKI

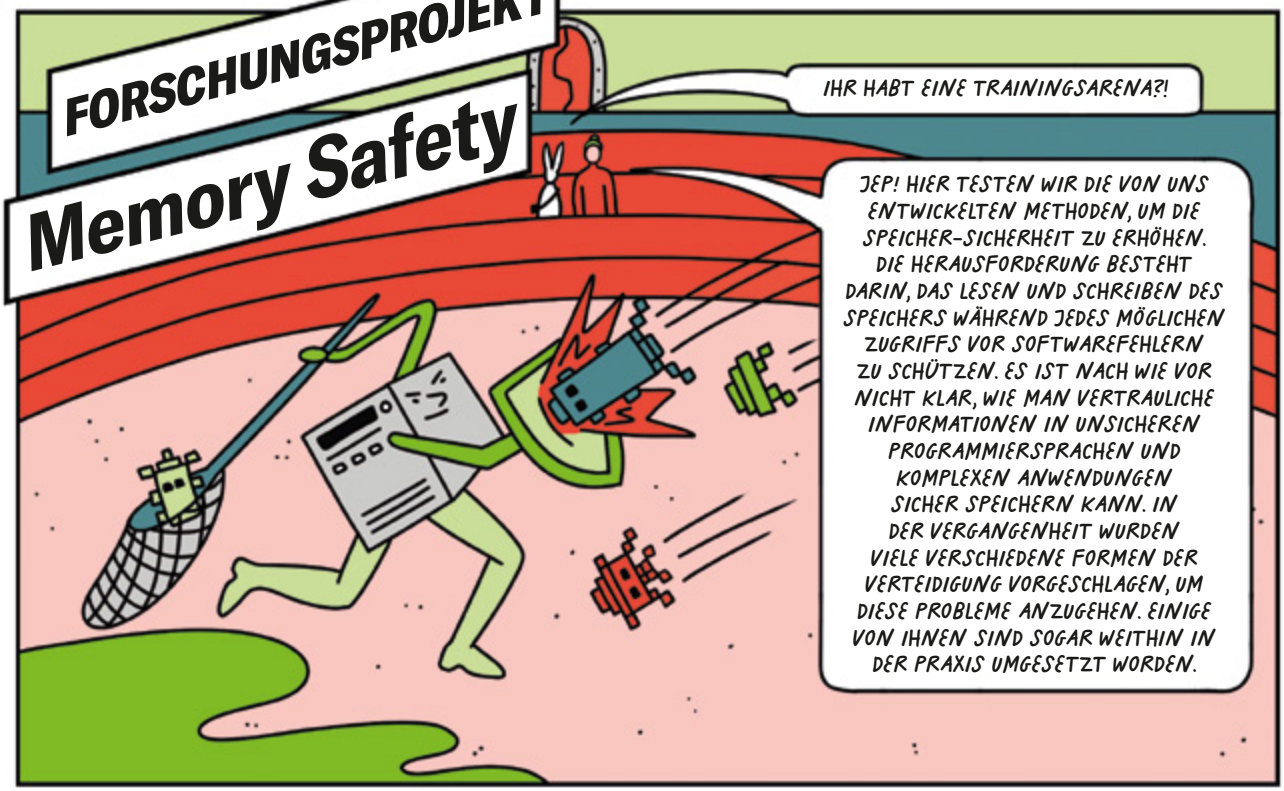
Ein **Application Programming Interface (API)** ist eine Schnittstelle, die es zwei Programmen ermöglicht, standardisiert miteinander zu kommunizieren. Die Übertragung von Daten und Befehlen erfolgt in einer definierten Syntax.

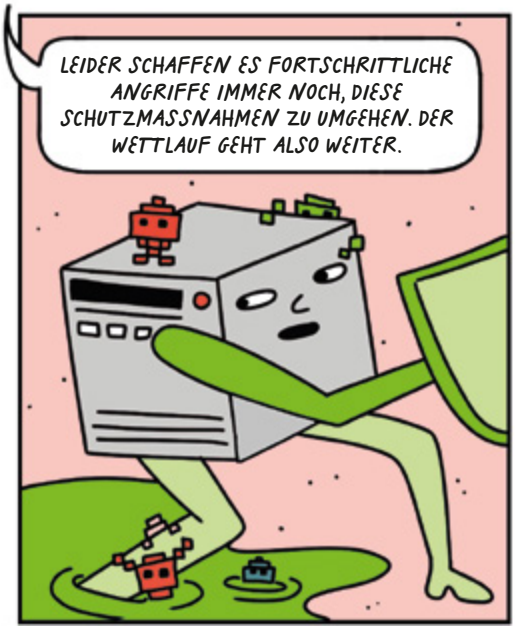
Ein von einem Computer ausgeführtes Programm besteht nur aus zwei verschiedenen Zeichen – der 0 und der 1 – und wird daher als Binärprogramm bezeichnet. Ein **Compiler** ist ein Programm, das den Quellcode, der in einer höheren Programmiersprache geschrieben ist (z.B. C/C++), in die maschinenlesbare Binärsprache übersetzt. Das Ergebnis ist „ausführbarer Code“, den der Computer dann interpretieren und umsetzen kann.

Eine **Central Processing Unit** (CPU), oft auch Prozessor genannt, ist die zentrale Einheit in einem Computer. Der Prozessor koordiniert sämtliche Prozesse und führt arithmetische und logische Operationen zur Verarbeitung von Daten aus internen oder externen Quellen aus, zum Beispiel aus dem Hauptspeicher. Es gibt unterschiedliche CPU-Architekturen von Intel, AMD oder ARM.

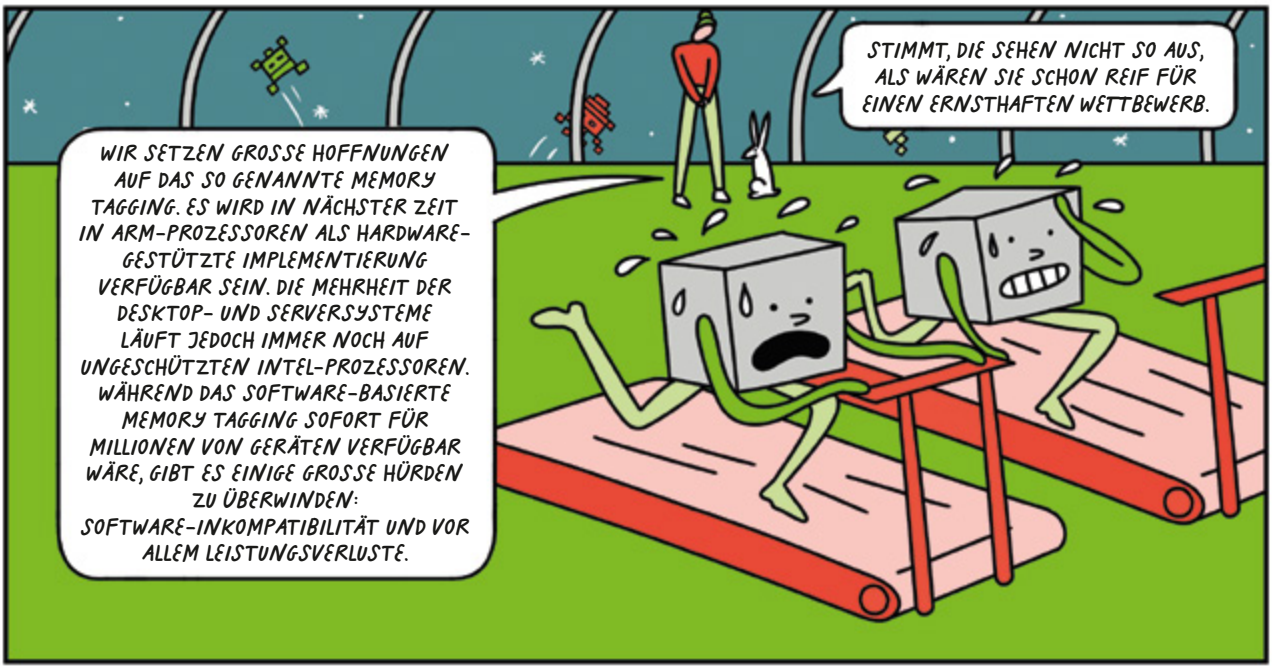
In der Praxis gibt es viele erfolgreiche Angriffe auf verschiedenste Ziele, wie zum Beispiel den Deutschen Bundestag, Unternehmen oder politische Aktivist*innen. Ein aktuelles Beispiel ist die **Spionagesoftware Pegasus,** die durch das Ausnutzen einer Sicherheitslücke heimlich auf Smartphones installiert werden kann. So kann man bei einem kompromittierten Telefon unter anderem Textnachrichten lesen, Anrufe verfolgen und private Informationen stehlen.


DIESE TÜR SIEHT SEEEHR SICHER AUS!
DAS IST DAS MINDESTE, WAS WIR TUN KÖNNEN, UM UNSERE INFORMATIONEN ZU SCHÜTZEN.

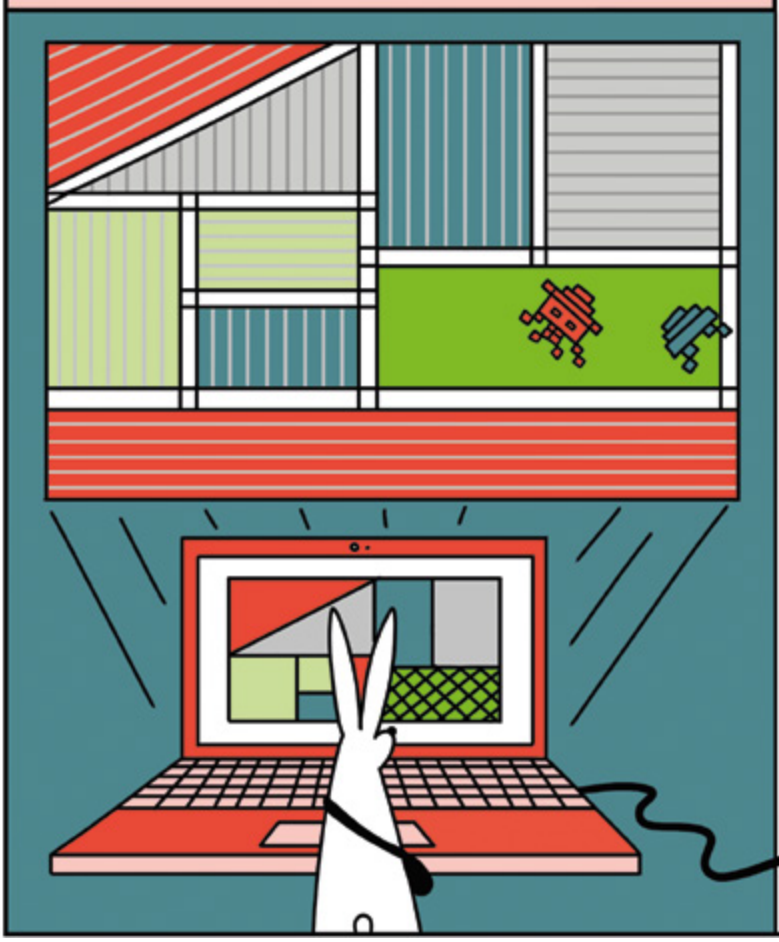

FORSCHUNGSPROJEKT
Memory Safety
IHR HABT EINE TRAININGSARENA?!
JEP! HIER TESTEN WIR DIE VON UNS ENTWICKELTEN METHODEN, UM DIE SPEICHER-SICHERHEIT ZU ERHÖHEN. DIE HERAUSFORDERUNG BESTEHT DARIN, DAS LESEN UND SCHREIBEN DES SPEICHERS WÄHREND JEDES MÖGLICHEN ZUGRIFFS VOR SOFTWAREFEHLERN ZU SCHÜTZEN. ES IST NACH WIE VOR NICHT KLAR, WIE MAN VERTRAULICHE INFORMATIONEN IN UNSICHEREN PROGRAMMIERSPRACHEN UND KOMPLEXEN ANWENDUNGEN SICHER SPEICHERN KANN. IN DER VERGANGENHEIT WURDEN VIELE VERSCHIEDENE FORMEN DER VERTEIDIGUNG VORGESCHLAGEN, UM DIESE PROBLEME ANZUGEHEN. EINIGE VON IHNEN SIND SOGAR WEITHIN IN DER PRAXIS UMGESETZT WORDEN.


LEIDER SCHAFFEN ES FORTSCHRITTLICHE ANGRIFFE IMMER NOCH, DIESE SCHUTZMASSNAHMEN ZU UMGEHEN. DER WETTLAUF GEHT ALSO WEITER.


BEI CASA UNTERSUCHEN WIR, WIE ZUKÜNFTIGE SOFTWARE-SYSTEME AUFGEBAUT SEIN MÜSSEN, UM SELBST DEN RAFFINIERTESTEN ANGRIFFEN STANDZUHALTEN.
OOOH! DIE SIND ABER NIEDLICH!

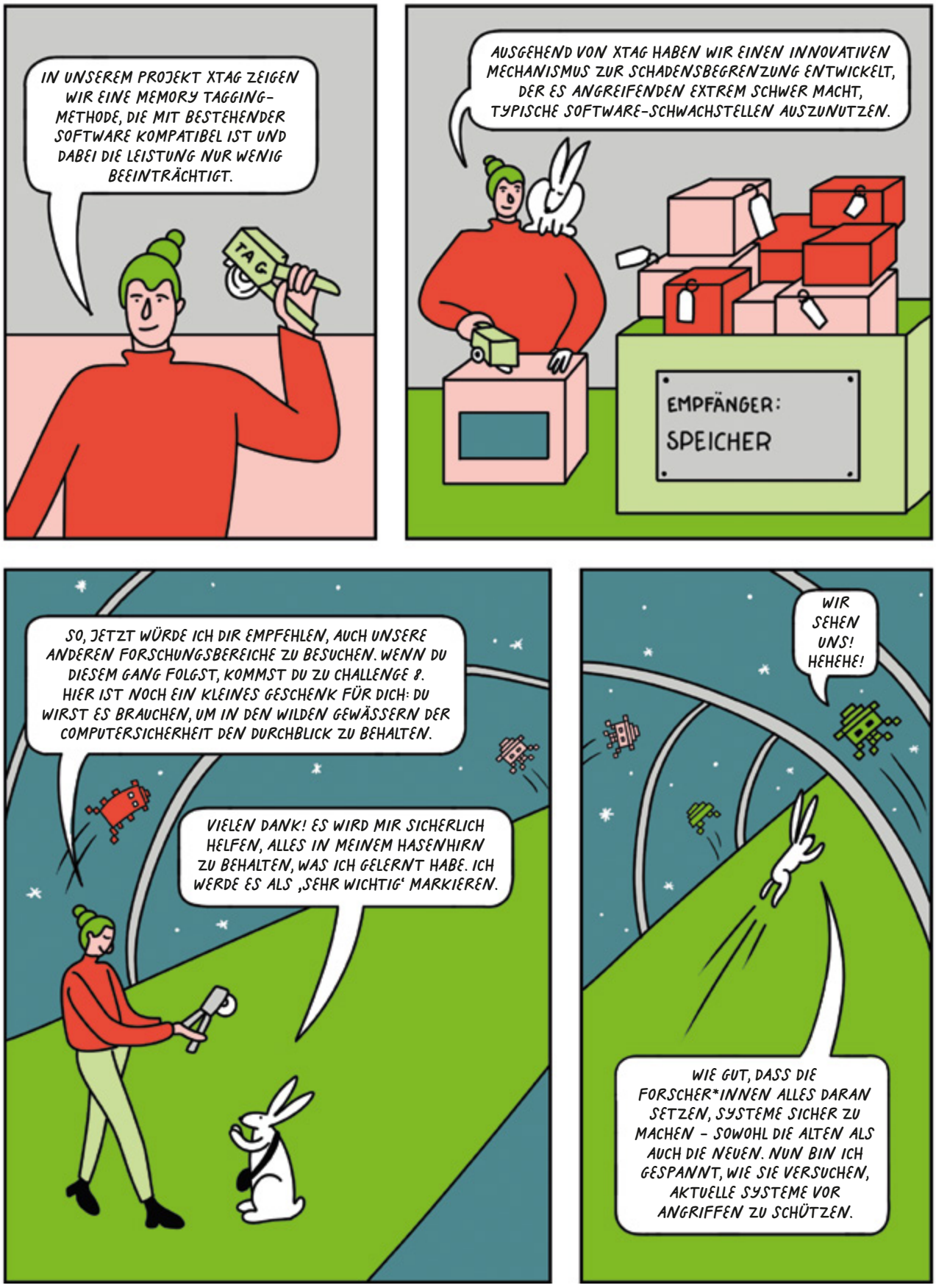


MEMORY TAGGING



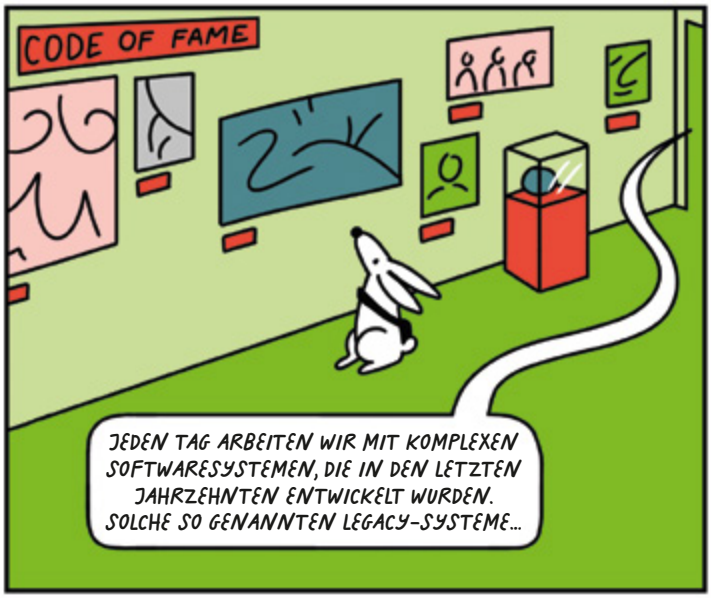
Memory Tagging ist eine vielversprechende neue Technologie zur Schadensbegrenzung. Die grundlegende Idee des Memory Tagging besteht darin, den Speicherbereich eines Programms in verschiedene Bereiche zu unterteilen und dann genau zu verfolgen, welcher Teil des Programms auf welchen Teil des Speicherbereichs zugreifen und ihn verändern kann. Man kann sich das folgendermaßen vorstellen:

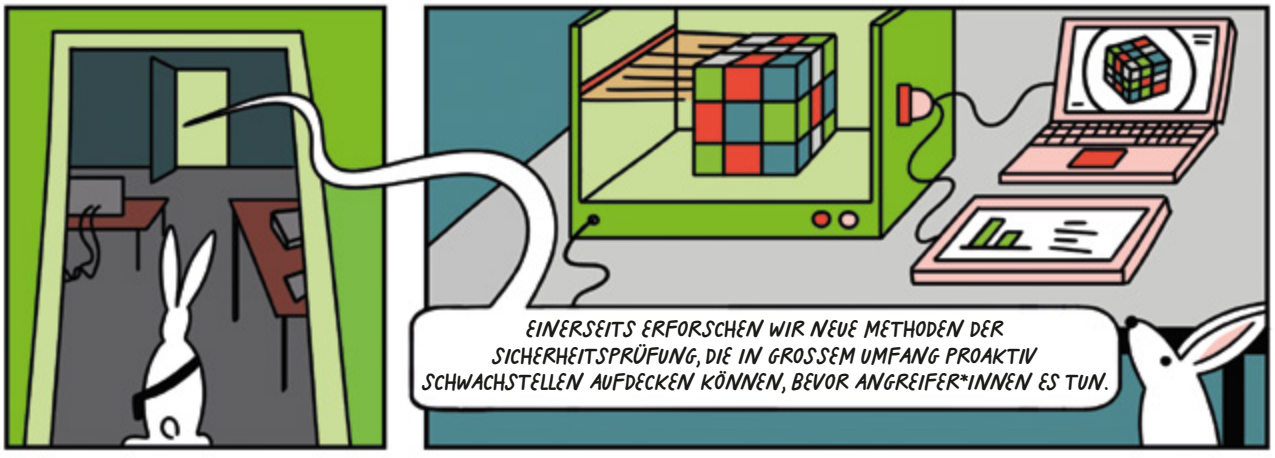
Der Speicherplatz wird in verschiedene Bereiche eingeteilt, die mit unterschiedlichen Farben markiert werden. Bei Operationen auf diesen Speicherbereichen wird dann die Farbe entsprechend übermittelt – so kann man in Echtzeit beobachten, wie sich Anweisungen auf den Speicher auswirken. Durch diese genaue Erfassung können viele verschiedene Arten von softwarebasierten Angriffen effektiv gestoppt werden.

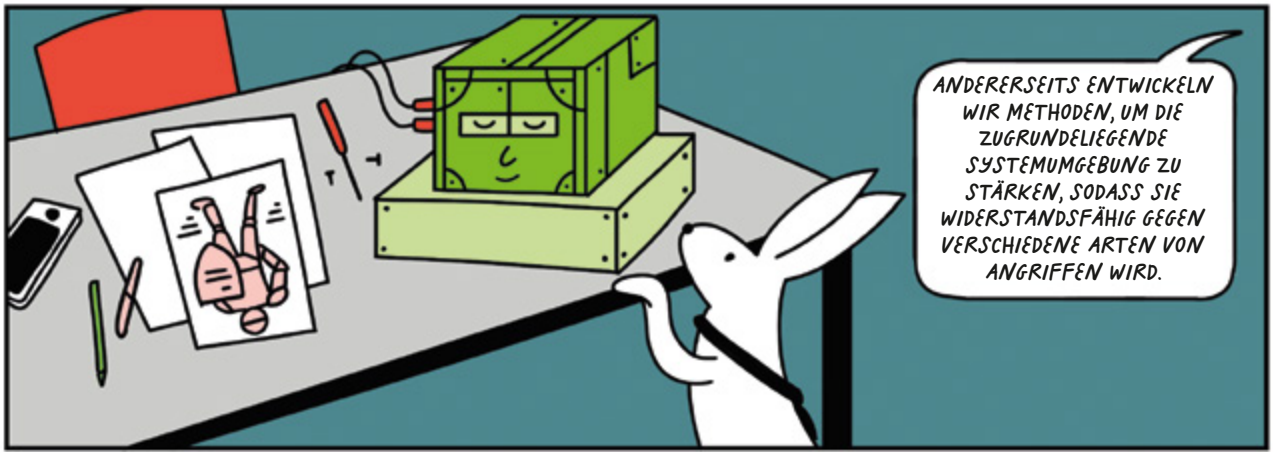

IN UNSEREM PROJEKT XTAG ZEIGEN WIR EINE MEMORY TAGGING-METHODE, DIE MIT BESTEHENDER SOFTWARE KOMPATIBEL IST UND DABEI DIE LEISTUNG NUR WENIG BEEINTRÄCHTIGT.
TAG
AUSGEHEND VON XTAG HABEN WIR EINEN INNOVATIVEN MECHANISMUS ZUR SCHADENSBEGRENZUNG ENTWICKELT, DER ES ANGREIFENDEN EXTREM SCHWER MACHT, TYPISCHE SOFTWARE-SCHWACHSTELLEN AUSZUNUTZEN.
EMPFÄNGER:
SPEICHER
SO, JETZT WÜRDE ICH DIR EMPFEHLEN, AUCH UNSERE ANDEREN FORSCHUNGSBEREICHE ZU BESUCHEN. WENN DU DIESEM GANG FOLGST, KOMMST DU ZU CHALLENGE 8. HIER IST NOCH EIN KLEINES GESCHENK FÜR DICH: DU WIRST ES BRAUCHEN, UM IN DEN WILDEN GEWÄSSERN DER COMPUTERSICHERHEIT DEN DURCHBLICK ZU BEHALTEN.
VIELEN DANK! ES WIRD MIR SICHERLICH HELFEN, ALLES IN MEINEM HASENHIRN ZU BEHALTEN, WAS ICH GELERNT HABE. ICH WERDE ES ALS ‚SEHR WICHTIG' MARKIEREN.
WIR SEHEN UNS! HEHEHE!
WIE GUT, DASS DIE FORSCHER*INNEN ALLES DARAN SETZEN, SYSTEME SICHER ZU MACHEN – SOWOHL DIE ALTEN ALS AUCH DIE NEUEN. NUN BIN ICH GESPANNT, WIE SIE VERSUCHEN, AKTUELLE SYSTEME VOR ANGRIFFEN ZU SCHÜTZEN.

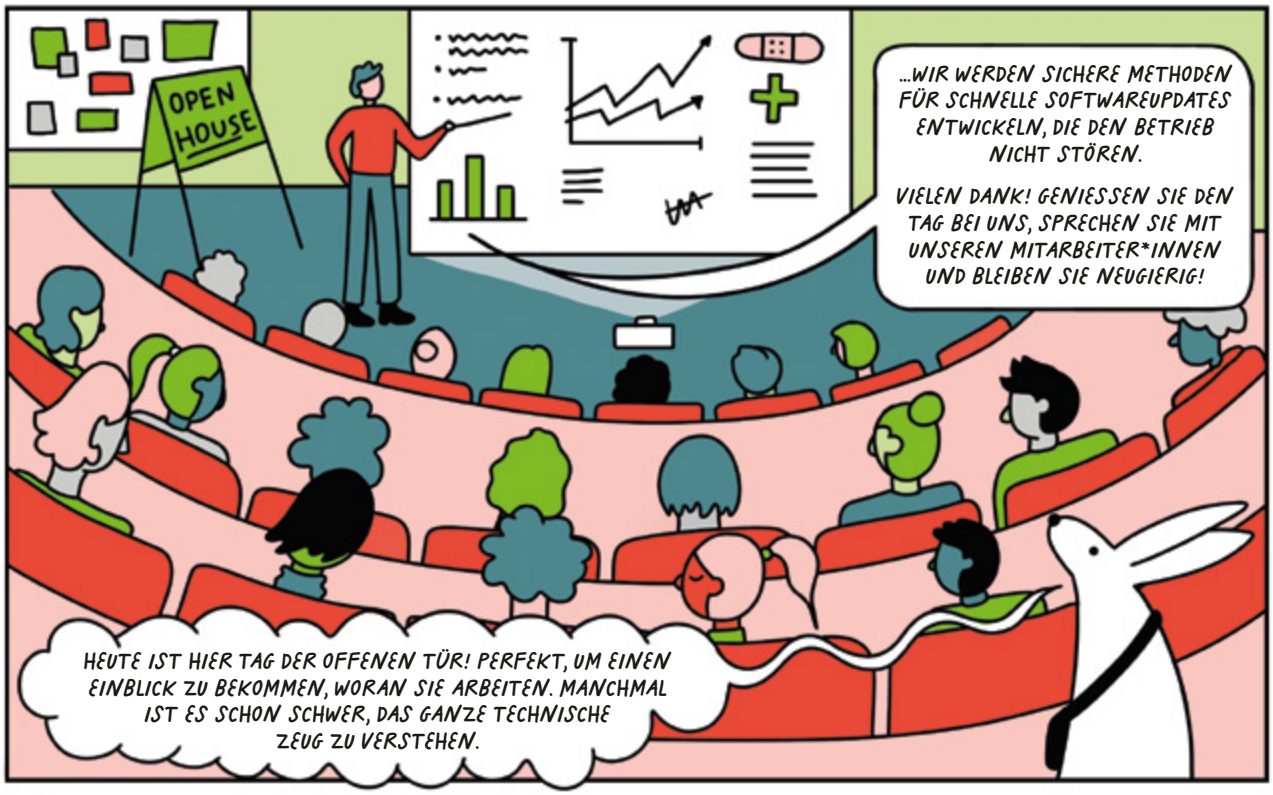
CHALLENGE 8

SICHERHEIT mit NICHT-VERTRAUENSWÜRDIGEN KOMPONENTEN



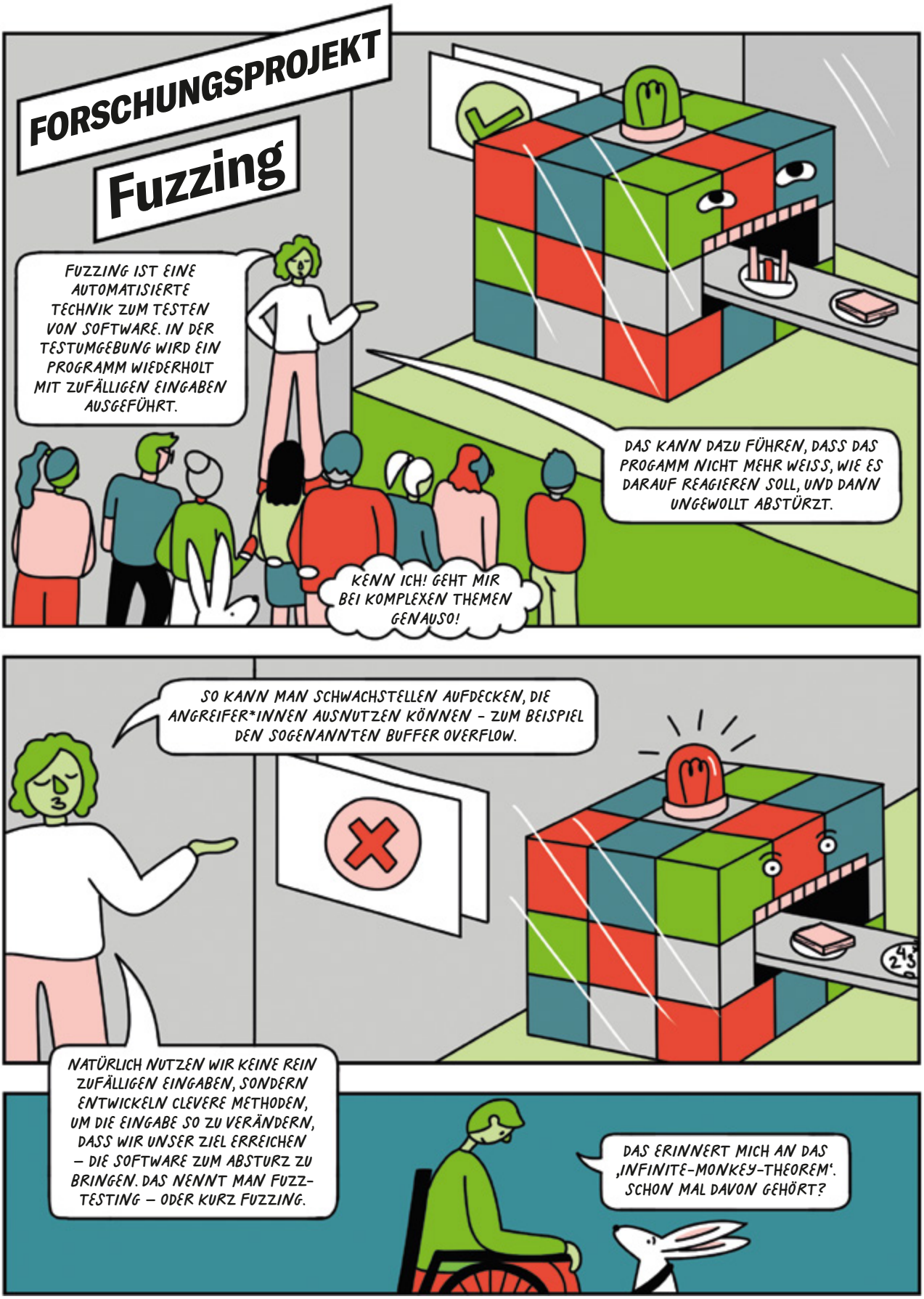




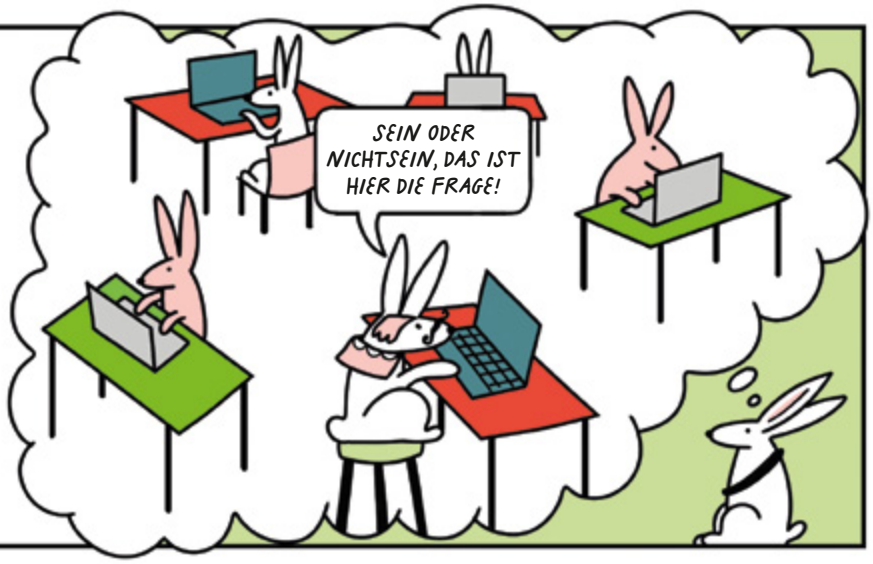

OPEN HOUSE
...WIR WERDEN SICHERE METHODEN FÜR SCHNELLE SOFTWAREUPDATES ENTWICKELN, DIE DEN BETRIEB NICHT STÖREN.
VIELEN DANK! GENIESSEN SIE DEN TAG BEI UNS, SPRECHEN SIE MIT UNSEREN MITARBEITER*INNEN UND BLEIBEN SIE NEUGIERIG!
HEUTE IST HIER TAG DER OFFENEN TÜR! PERFEKT, UM EINEN EINBLICK ZU BEKOMMEN, WORAN SIE ARBEITEN. MANCHMAL IST ES SCHON SCHWER, DAS GANZE TECHNISCHE ZEUG ZU VERSTEHEN.

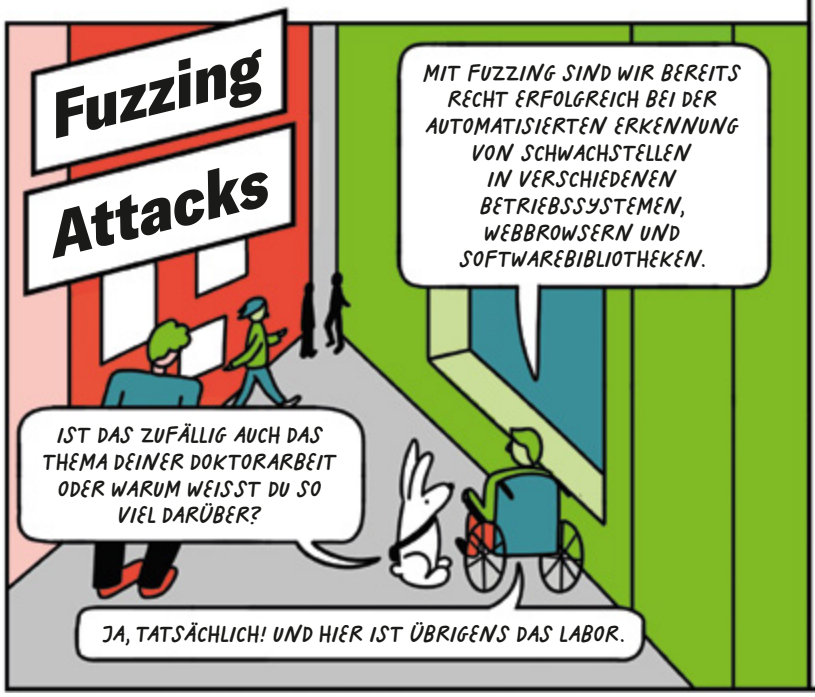

OPEN HOUSE
'TSCHULDIGE! ARBEITEST DU HIER?
JA!
ICH HABE MICH GEFRAGT, OB DU MIR ETWAS ÜBER DEINE FORSCHUNG ERZÄHLEN KÖNNTEST. ICH FINDE DAS ALLES NOCH ETWAS SCHWAMMIG.
KLAR, ICH HAB DA SCHON EINE IDEE! ICH ZEIG DIR ETWAS, DAS UNSER FORSCHUNGSFELD GANZ GUT BESCHREIBT. ICH BIN ÜBRIGENS PHIL UND DOKTORAND HIER.
DAS KLINGT SUPER! ICH BIN BETTY!


WOW, DA IST JA WIRKLICH WAS LOS! DIE LEUTE SCHEINEN ECHT INTERESSE AN EURER ARBEIT ZU HABEN. WAS PASSIERT DA DRÜBEN?
ELLA ZEIGT GERADE, WIE FUZZING FUNKTIONIERT – DAS IST GENAU DAS PROJEKT, DAS ICH DIR ZEIGEN WOLLTE. KOMM, WIR STELLEN UNS DAZU, DAMIT WIR HÖREN, WAS SIE ERZÄHLT.


FORSCHUNGSPROJEKT
Fuzzing
FUZZING IST EINE AUTOMATISIERTE TECHNIK ZUM TESTEN VON SOFTWARE. IN DER TESTUMGEBUNG WIRD EIN PROGRAMM WIEDERHOLT MIT ZUFÄLLIGEN EINGABEN AUSGEFÜHRT.
DAS KANN DAZU FÜHREN, DASS DAS PROGAMM NICHT MEHR WEISS, WIE ES DARAUF REAGIEREN SOLL, UND DANN UNGEWOLLT ABSTÜRZT.
KENN ICH! GEHT MIR BEI KOMPLEXEN THEMEN GENAUSO!
SO KANN MAN SCHWACHSTELLEN AUFDECKEN, DIE ANGREIFER*INNEN AUSNUTZEN KÖNNEN – ZUM BEISPIEL DEN SOGENANNTEN BUFFER OVERFLOW.
NATÜRLICH NUTZEN WIR KEINE REIN ZUFÄLLIGEN EINGABEN, SONDERN ENTWICKELN CLEVERE METHODEN, UM DIE EINGABE SO ZU VERÄNDERN, DASS WIR UNSER ZIEL ERREICHEN – DIE SOFTWARE ZUM ABSTURZ ZU BRINGEN. DAS NENNT MAN FUZZ-TESTING – ODER KURZ FUZZING.
DAS ERINNERT MICH AN DAS ‚INFINITE-MONKEY-THEOREM'. SCHON MAL DAVON GEHÖRT?

„DAS THEOREM BESAGT, DASS EIN AFFE, DER UNENDLICH OFT ZUFÄLLIGE TASTEN AUF EINER TASTATUR DRÜCKT, IRGENDWANN JEDEN BEKANNTEN TEXT SCHREIBEN WIRD. WIE ZUM BEISPIEL DIE WERKE VON WILLIAM SHAKESPEARE. TATSÄCHLICH WÜRDE DER AFFE JEDEN MÖGLICHEN TEXT UNENDLICH OFT TIPPEN. NEBENBEI BEMERKT: HASEN KÖNNTEN DAS AUCH.“

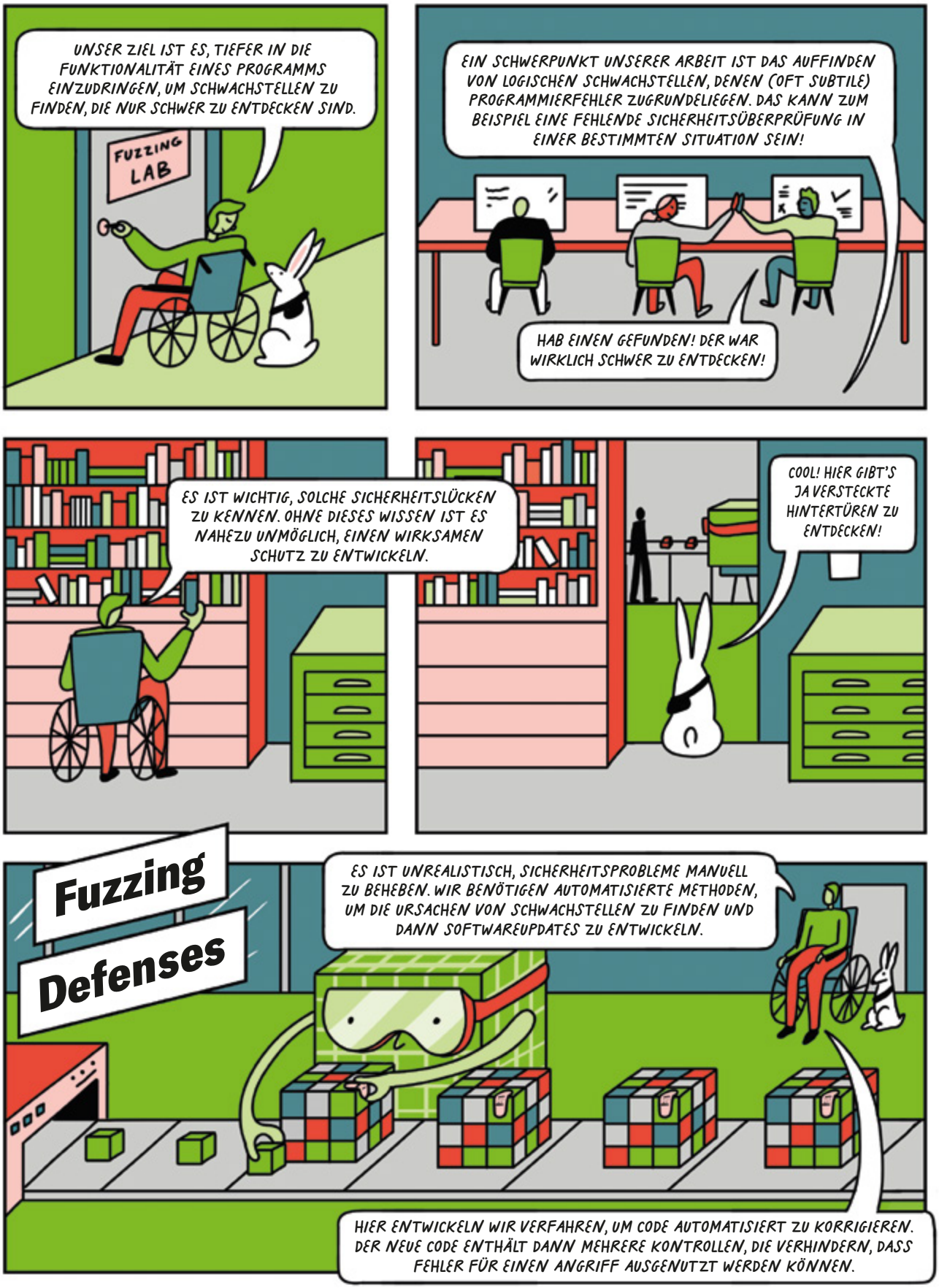




CASA WIKI

Buffer Overflows gehören zu den häufigsten Schwachstellen in Software. Andere wichtige Angriffsvektoren sind die sogenannten **Use-after-free-Schwachstellen**. Angreifer*innen können solche Schwachstellen ausnutzen, um die Kontrolle über das Programm zu übernehmen und dann beliebigen Code auszuführen.

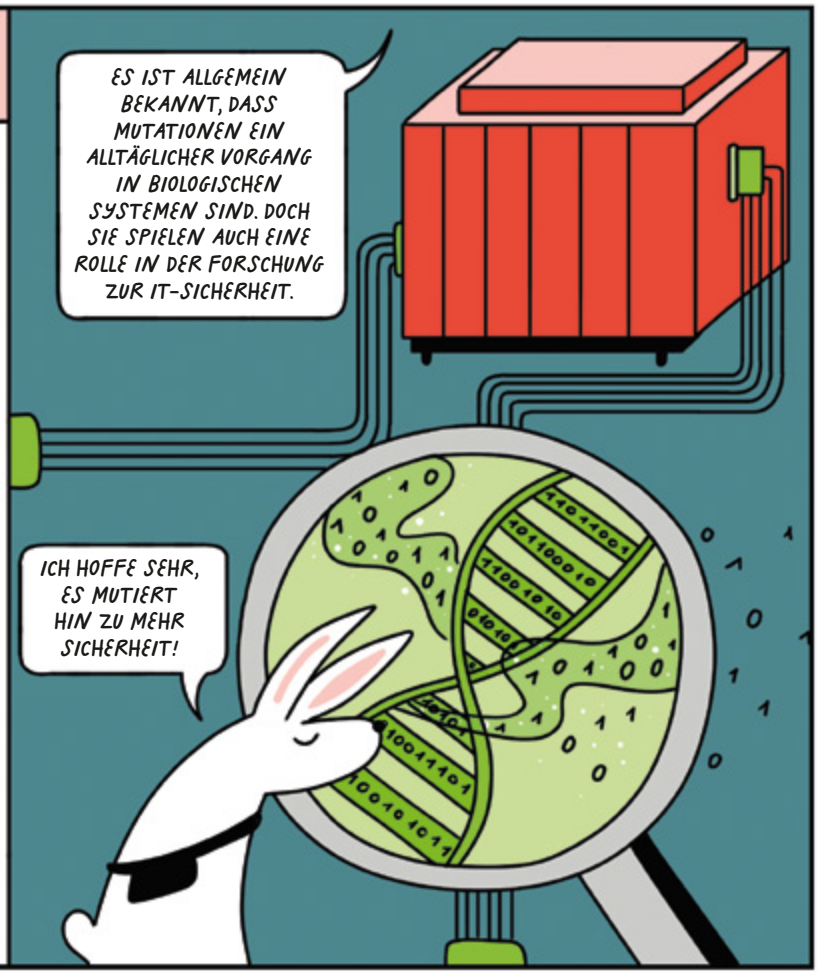
AFL (American Fuzzy Lop) ist ein bekanntes Fuzzing-Tool, das unter einer Open-Source-Lizenz verfügbar ist. Das Tool hat dazu beigetragen, Hunderte von Softwarefehlern in Dutzenden von großen Softwareprojekten zu entdecken.

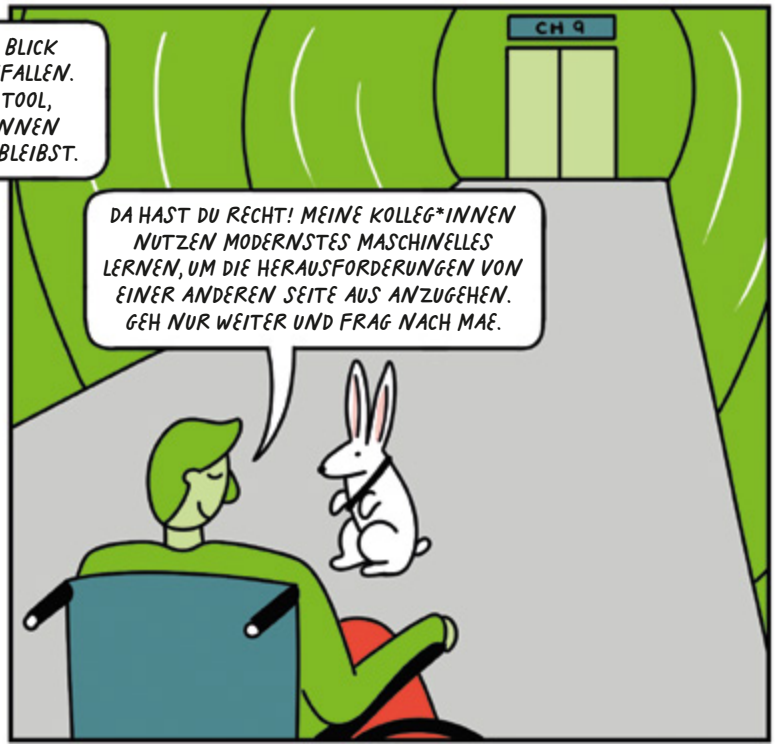

UNSER ZIEL IST ES, TIEFER IN DIE FUNKTIONALITÄT EINES PROGRAMMS EINZUDRINGEN, UM SCHWACHSTELLEN ZU FINDEN, DIE NUR SCHWER ZU ENTDECKEN SIND.
FUZZING LAB
EIN SCHWERPUNKT UNSERER ARBEIT IST DAS AUFFINDEN VON LOGISCHEN SCHWACHSTELLEN, DENEN (OFT SUBTILE) PROGRAMMIERFEHLER ZUGRUNDELIEGEN. DAS KANN ZUM BEISPIEL EINE FEHLENDE SICHERHEITSÜBERPRÜFUNG IN EINER BESTIMMTEN SITUATION SEIN!
HAB EINEN GEFUNDEN! DER WAR WIRKLICH SCHWER ZU ENTDECKEN!
ES IST WICHTIG, SOLCHE SICHERHEITSLÜCKEN ZU KENNEN. OHNE DIESES WISSEN IST ES NAHEZU UNMÖGLICH, EINEN WIRKSAMEN SCHUTZ ZU ENTWICKELN.
COOL! HIER GIBT'S JA VERSTECKTE HINTERTÜREN ZU ENTDECKEN!
Fuzzing Defenses
ES IST UNREALISTISCH, SICHERHEITSPROBLEME MANUELL ZU BEHEBEN. WIR BENÖTIGEN AUTOMATISIERTE METHODEN, UM DIE URSACHEN VON SCHWACHSTELLEN ZU FINDEN UND DANN SOFTWAREUPDATES ZU ENTWICKELN.
HIER ENTWICKELN WIR VERFAHREN, UM CODE AUTOMATISIERT ZU KORRIGIEREN. DER NEUE CODE ENTHÄLT DANN MEHRERE KONTROLLEN, DIE VERHINDERN, DASS FEHLER FÜR EINEN ANGRIFF AUSGENUTZT WERDEN KÖNNEN.

MUTATIONEN

Eine der größten Herausforderungen bei diesem Vorgehen besteht darin, die Eingabedaten effizient so zu verändern, dass ein unerwartetes Systemverhalten hervorgerufen wird.

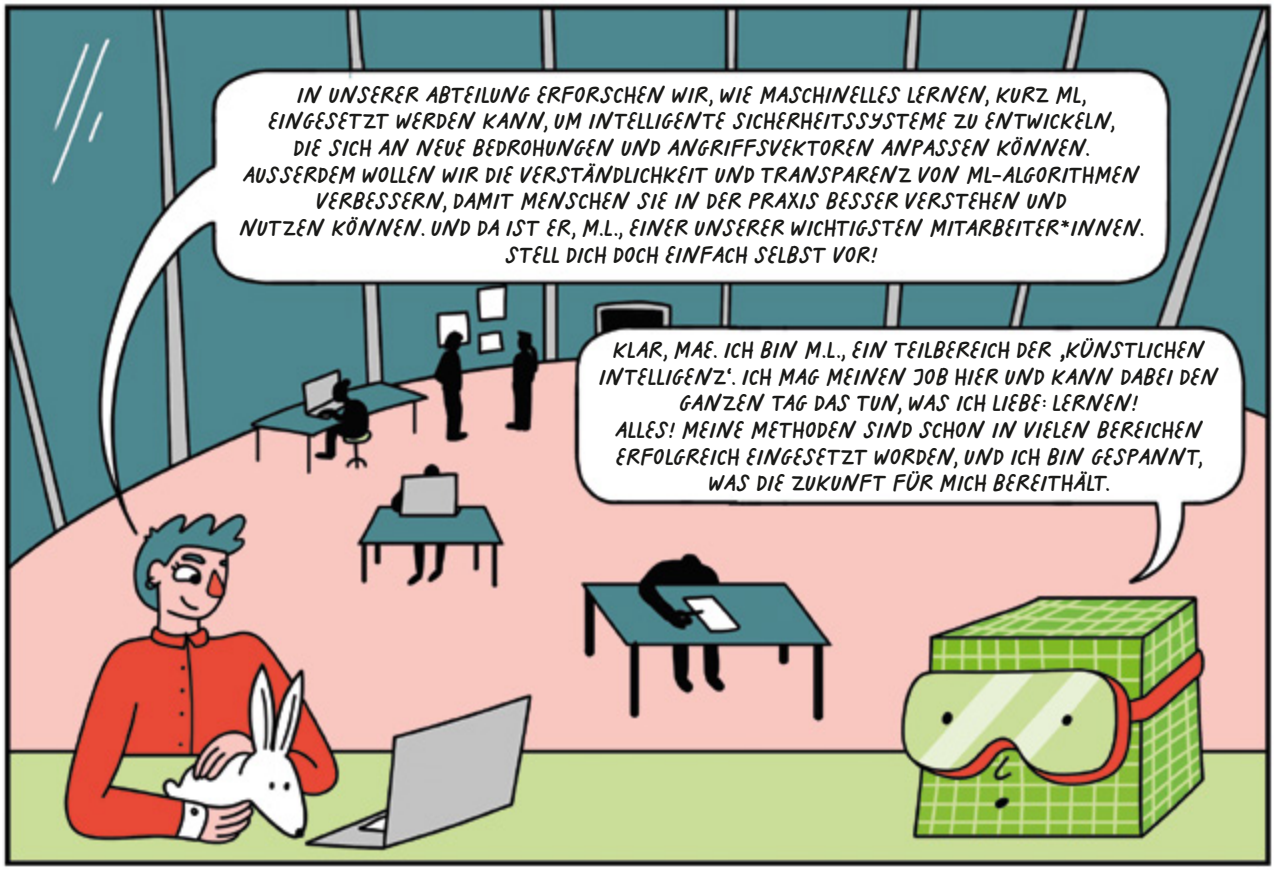
Bei **Mutationen** können wir Eingabedaten leicht verändern, zum Beispiel eine 0 in eine 1 verwandeln, Zeichen am Ende der Eingabe hinzufügen oder in der Mitte herausschneiden. Wir untersuchen verschiedene Arten von Mutationen und beobachten, wie effizient sie unerwartete Verhaltensweisen in verschiedenen Programmtypen auslösen. Das hilft uns, die Schwachstellen von Systemen zu erkennen, denn Angreifer*innen können unerwartetes Verhalten oft für ihre Zwecke ausnutzen. Letztendlich hilft es uns, die Probleme zu beheben.





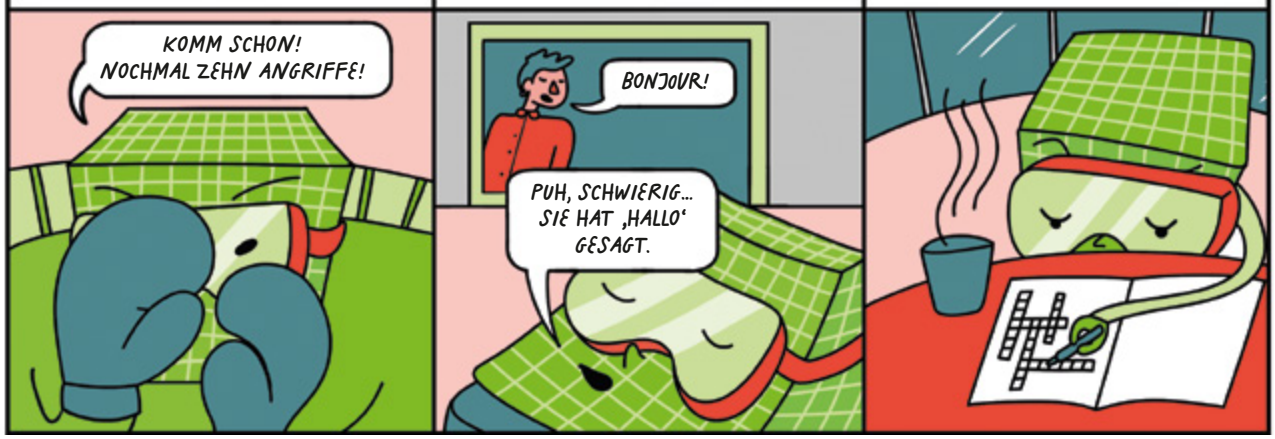
CHALLENGE 9

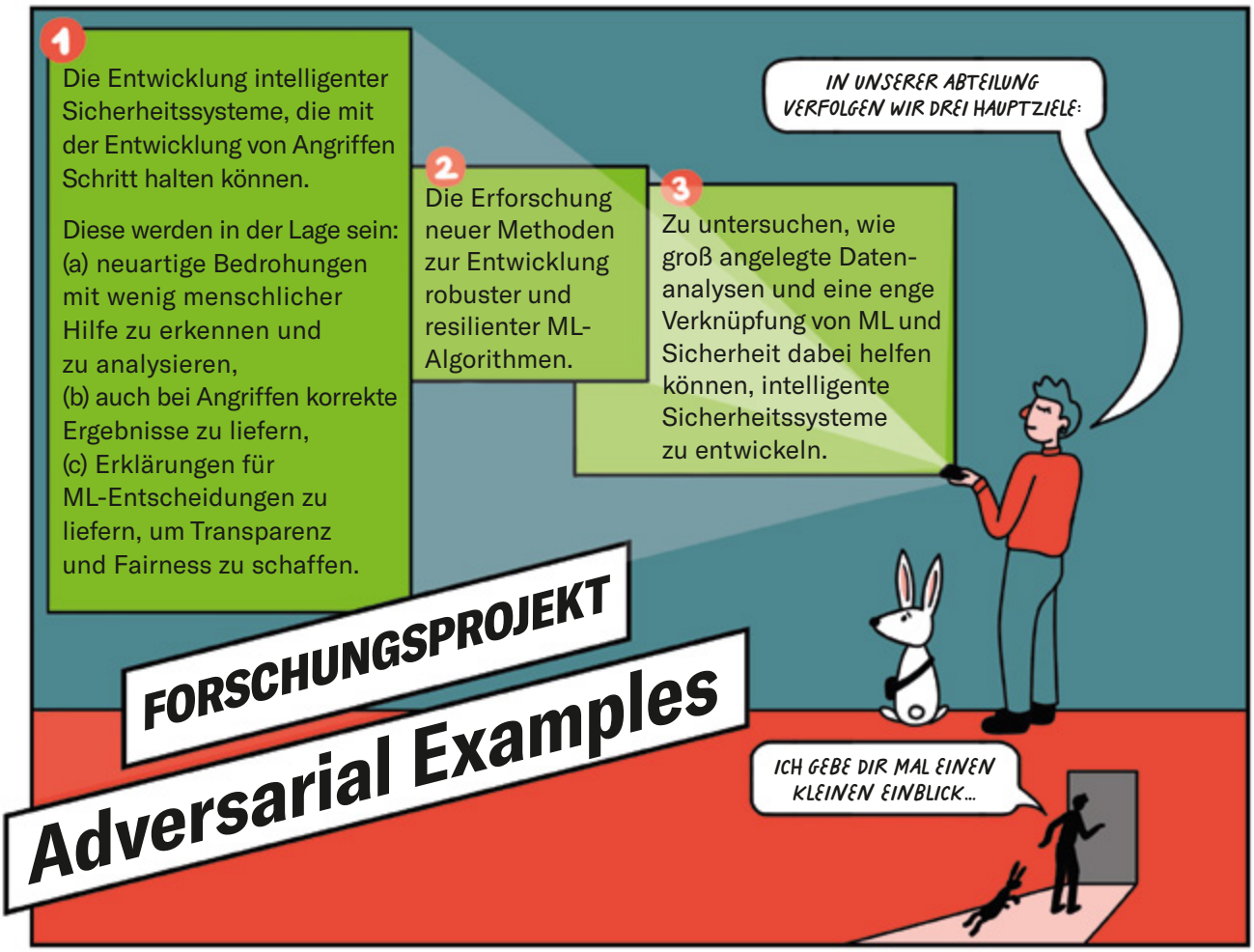
INTELLIGENTE SICHERHEITS-SYSTEME

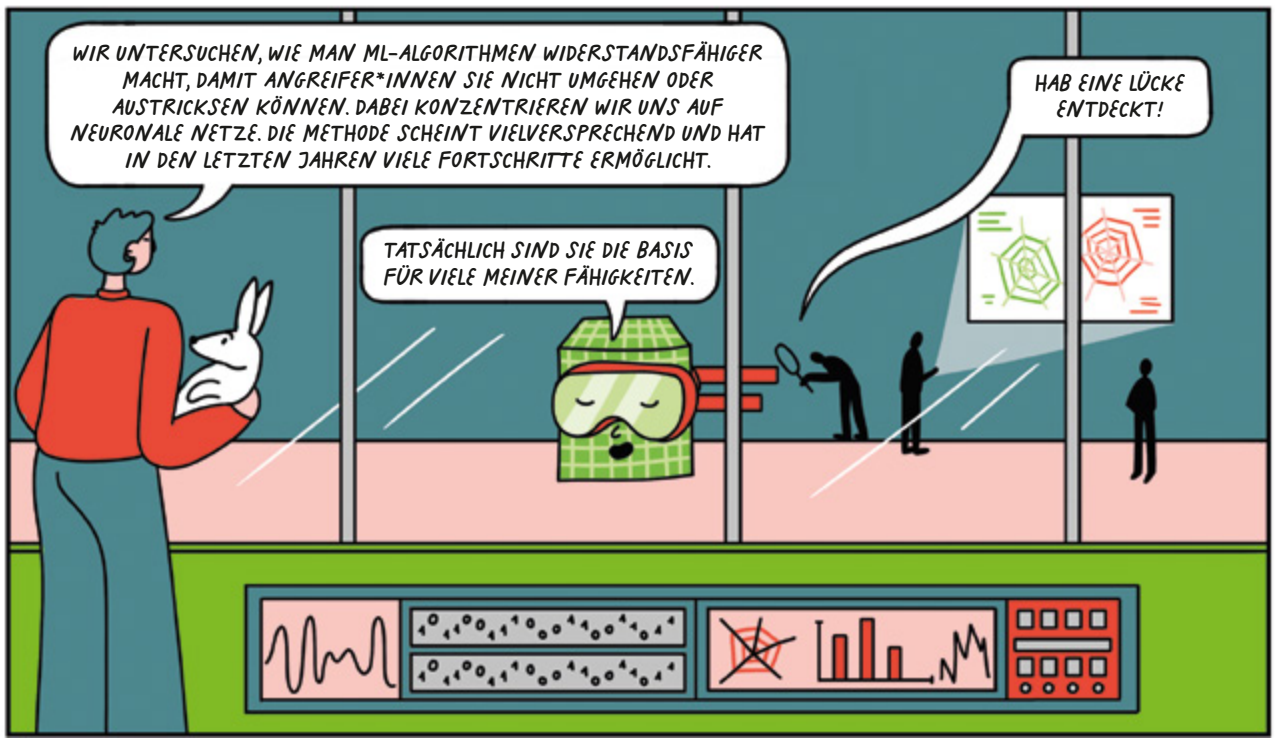


EIN GANZ GEWÖHNLICHER ARBEITSTAG IM LEBEN VON M.L.

Lernen, wie meine eigenen Algorithmen selbstständig ihre Widerstandsfähigkeit erhöhen können.	Erledigen von alltäglichen Aufgaben, zum Beispiel dem Übersetzen eines Textes von einer Sprache in eine andere.	Muster und Korrelationen in Daten erkennen und sich ständig selbst verbessern, ohne eigens dafür programmiert zu sein.

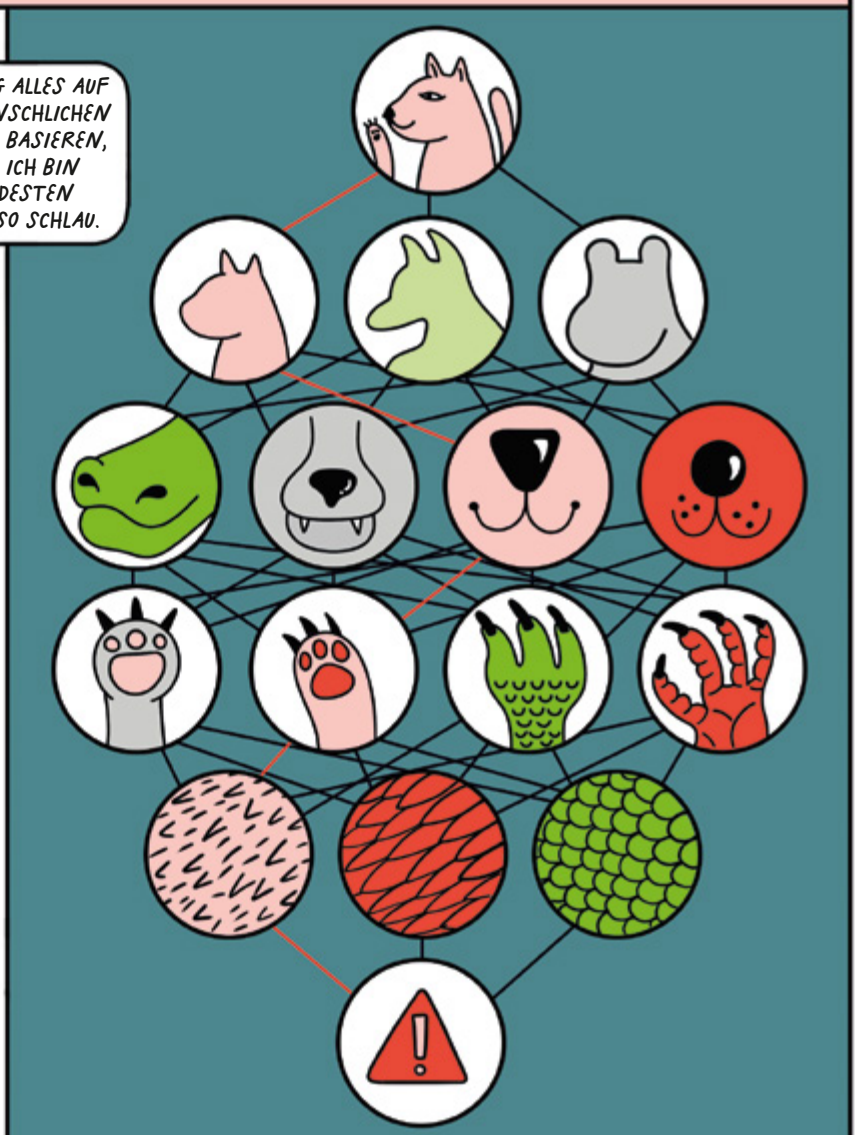



1
Die Entwicklung intelligenter Sicherheitssysteme, die mit der Entwicklung von Angriffen Schritt halten können.
Diese werden in der Lage sein:
(a) neuartige Bedrohungen mit wenig menschlicher Hilfe zu erkennen und zu analysieren,
(b) auch bei Angriffen korrekte Ergebnisse zu liefern,
(c) Erklärungen für ML-Entscheidungen zu liefern, um Transparenz und Fairness zu schaffen.
2
Die Erforschung neuer Methoden zur Entwicklung robuster und resilienter ML-Algorithmen.
3
Zu untersuchen, wie groß angelegte Datenanalysen und eine enge Verknüpfung von ML und Sicherheit dabei helfen können, intelligente Sicherheitssysteme zu entwickeln.
IN UNSERER ABTEILUNG VERFOLGEN WIR DREI HAUPTZIELE:
FORSCHUNGSPROJEKT
Adversarial Examples
ICH GEBE DIR MAL EINEN KLEINEN EINBLICK...


WIR UNTERSUCHEN, WIE MAN ML-ALGORITHMEN WIDERSTANDSFÄHIGER MACHT, DAMIT ANGREIFER*INNEN SIE NICHT UMGEHEN ODER AUSTRICKSEN KÖNNEN. DABEI KONZENTRIEREN WIR UNS AUF NEURONALE NETZE. DIE METHODE SCHEINT VIELVERSPRECHEND UND HAT IN DEN LETZTEN JAHREN VIELE FORTSCHRITTE ERMÖGLICHT.
TATSÄCHLICH SIND SIE DIE BASIS FÜR VIELE MEINER FÄHIGKEITEN.
HAB EINE LÜCKE ENTDECKT!

DEEP NEURAL NETWORKS

Deep Learning ist eine spezielle Methode der Informationsverarbeitung und ein Teilbereich des maschinellen Lernens. Deep Learning verwendet so genannte **neuronale Netze** zur Analyse großer Datensätze. Die Funktionsweise neuronaler Netze ist in vielerlei Hinsicht von dem biologischen neuronalen Netz des menschlichen Gehirns inspiriert. Neuronale Netze bestehen aus vielen Schichten mit kleinen Verarbeitungseinheiten, den ‚künstlichen Neuronen'. Daher kommt auch der Begriff ‚tief' (deep): Je mehr Neuronen und Schichten ein neuronales Netz umfasst, desto komplexer sind die Probleme, die es darstellen kann.



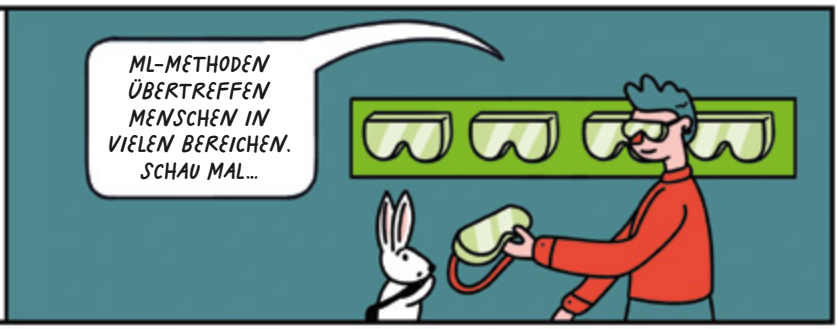
CASA WIKI

Ein **Algorithmus** ist eine spezifische Reihe von Vorgaben, um ein bestimmtes Problem zu lösen. So ähnlich wie ein Kochrezept, das jeden Schritt zur Zubereitung der Mahlzeit beschreibt.

Psychoakustik untersucht den Zusammenhang von physikalischem Klang und der menschlichen Wahrnehmung des Klangs als Hörerlebnis.

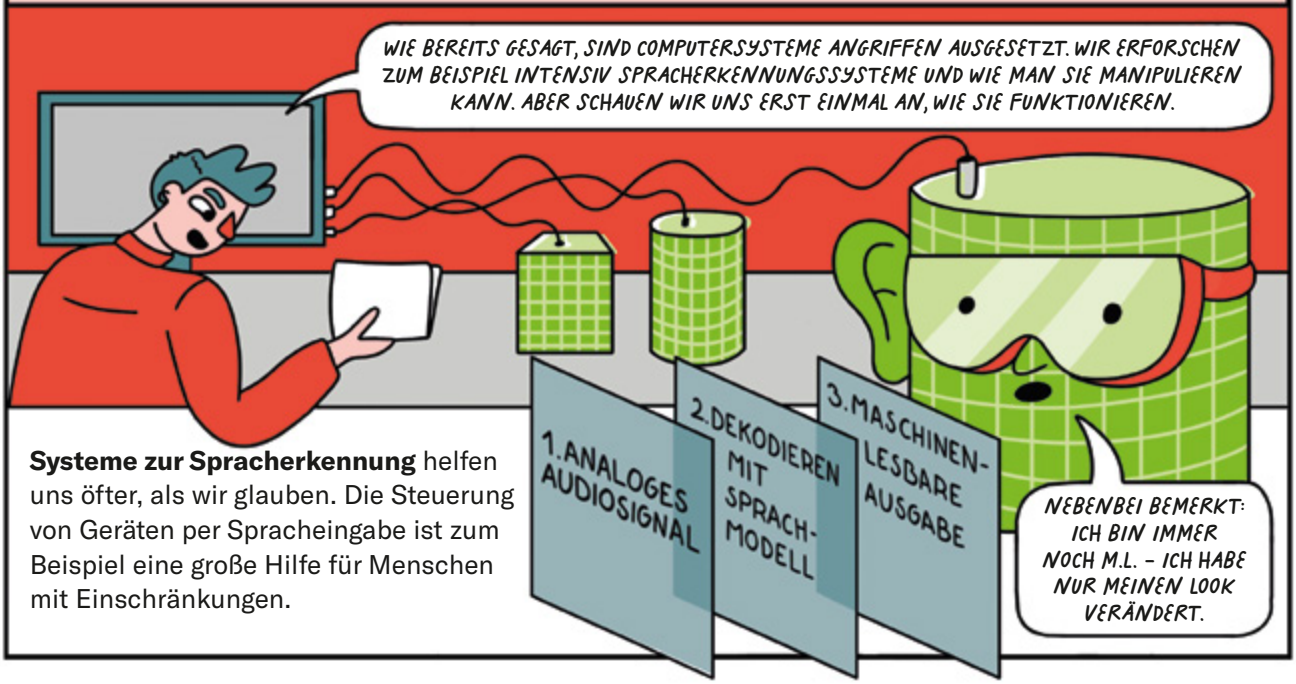
Eine wichtige Anwendung aus diesem Bereich ist die Komprimierung von Audio-Signalen in MP3-Dateien. Dabei werden Audiosignale entfernt, die das menschliche Ohr nicht wahrnehmen kann.

Künstliche Intelligenz und Methoden des maschinellen Lernens haben bereits viele Bereiche unseres Lebens verändert. Zum Beispiel durch automatisierte Übersetzungen, Spracherkennung oder Computerspiele, in denen Algorithmen gegen menschlichen Spieler*innen antreten.



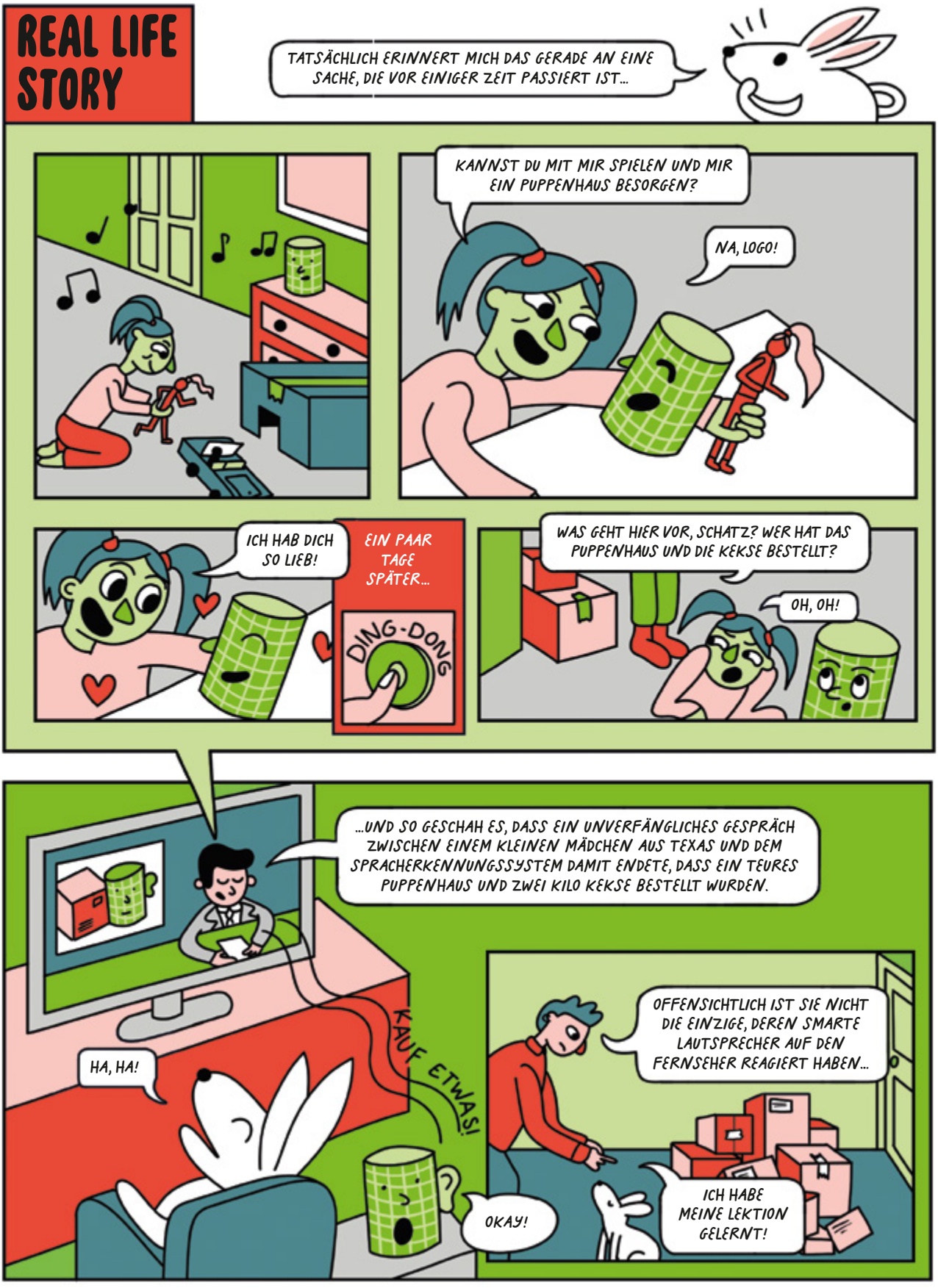
Deep Blue, ein von IBM entwickelter Schachcomputer, schaffte es 1996, den Weltmeister Garri Kasparow zu schlagen.

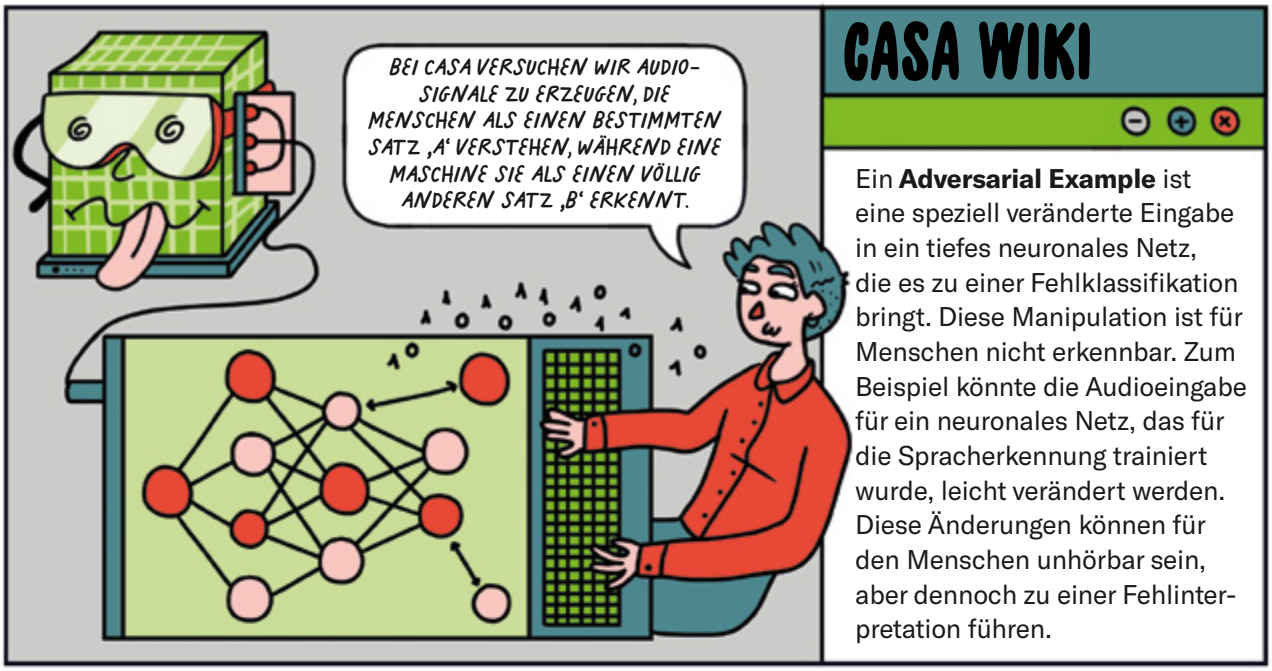
SYSTEME ZUR SPRACHERKENNUNG



Systeme zur Spracherkennung helfen uns öfter, als wir glauben. Die Steuerung von Geräten per Spracheingabe ist zum Beispiel eine große Hilfe für Menschen mit Einschränkungen.

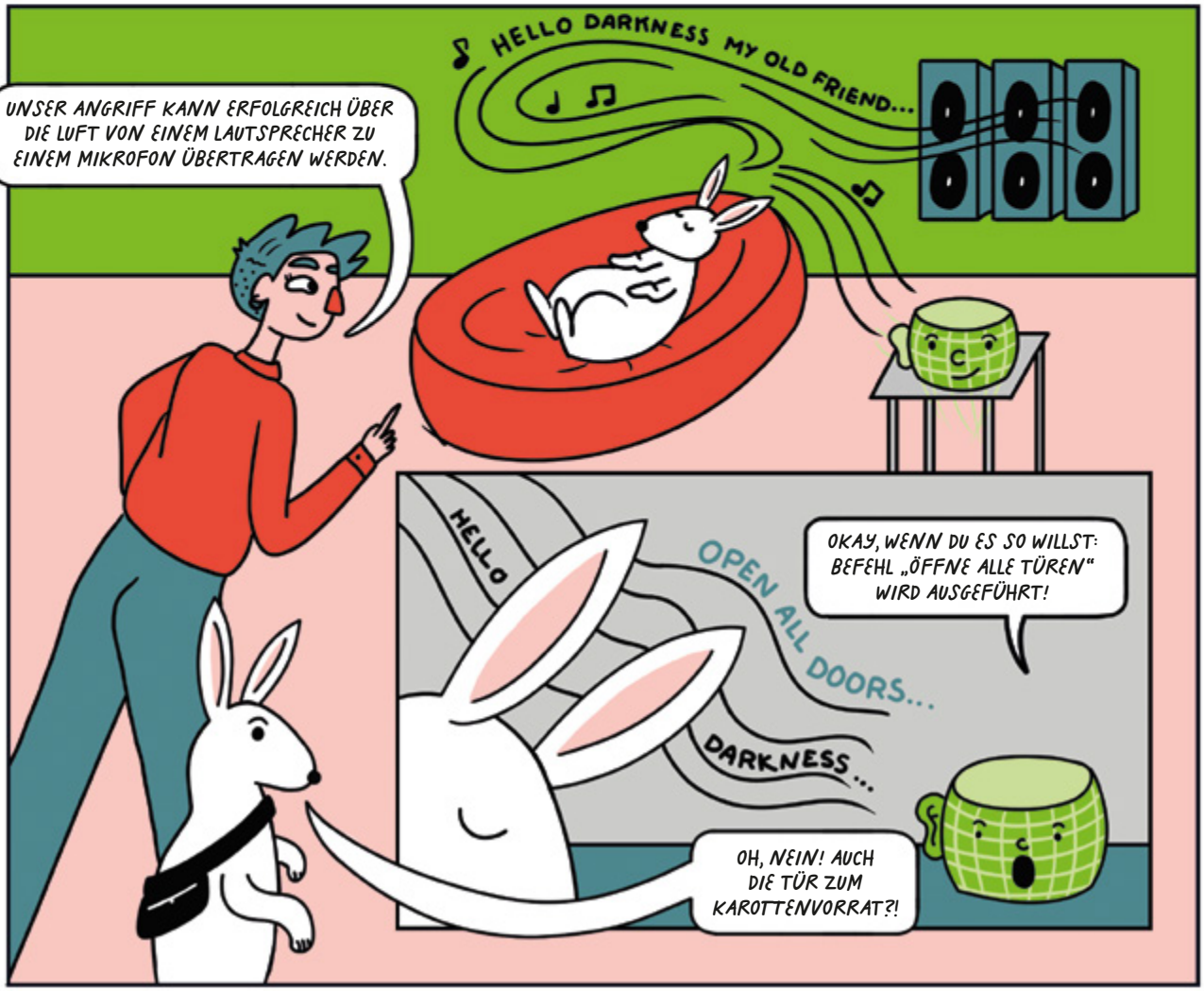
REAL LIFE STORY

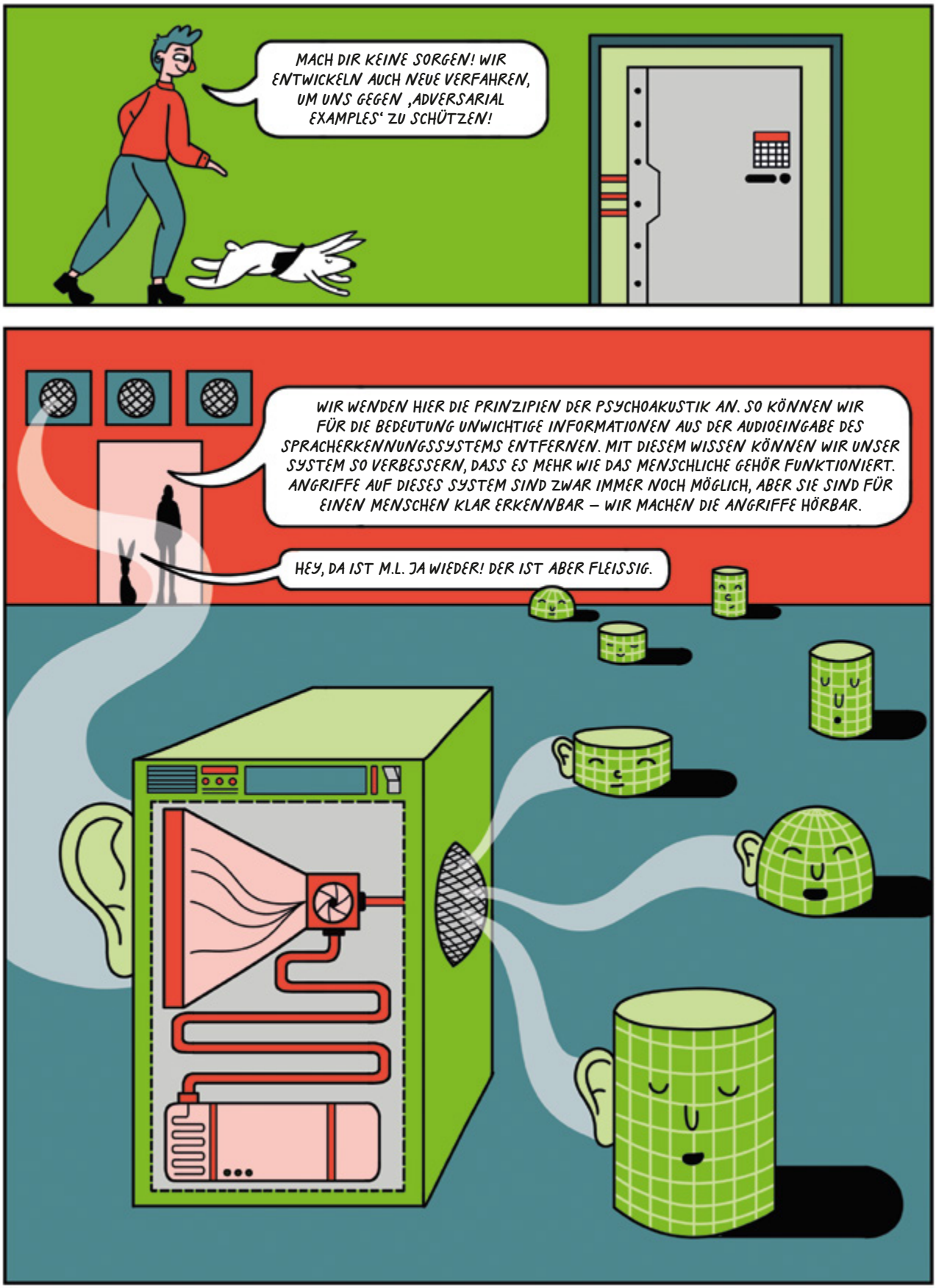




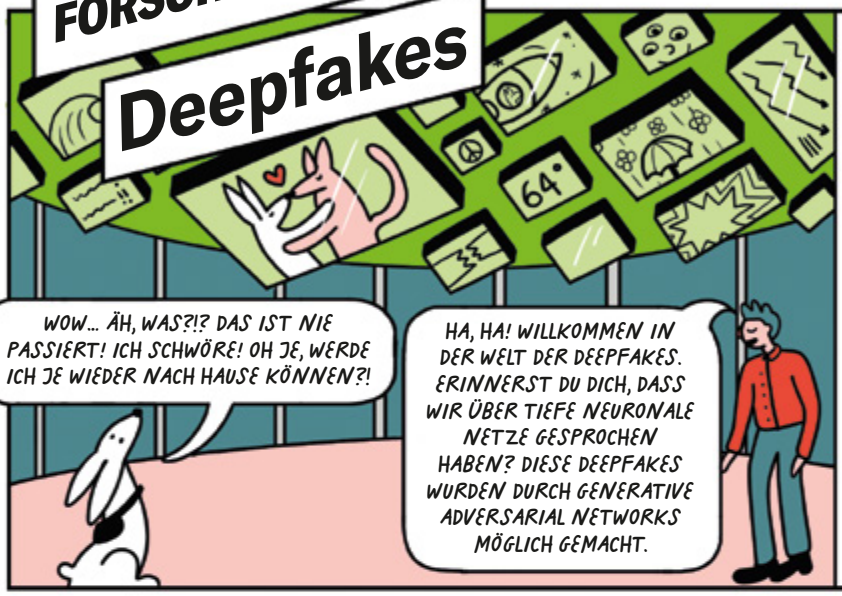
CASA WIKI

Ein **Adversarial Example** ist eine speziell veränderte Eingabe in ein tiefes neuronales Netz, die es zu einer Fehlklassifikation bringt. Diese Manipulation ist für Menschen nicht erkennbar. Zum Beispiel könnte die Audioeingabe für ein neuronales Netz, das für die Spracherkennung trainiert wurde, leicht verändert werden. Diese Änderungen können für den Menschen unhörbar sein, aber dennoch zu einer Fehlinterpretation führen.




MACH DIR KEINE SORGEN! WIR ENTWICKELN AUCH NEUE VERFAHREN, UM UNS GEGEN ‚ADVERSARIAL EXAMPLES' ZU SCHÜTZEN!
WIR WENDEN HIER DIE PRINZIPIEN DER PSYCHOAKUSTIK AN. SO KÖNNEN WIR FÜR DIE BEDEUTUNG UNWICHTIGE INFORMATIONEN AUS DER AUDIOEINGABE DES SPRACHERKENNUNGSSYSTEMS ENTFERNEN. MIT DIESEM WISSEN KÖNNEN WIR UNSER SYSTEM SO VERBESSERN, DASS ES MEHR WIE DAS MENSCHLICHE GEHÖR FUNKTIONIERT. ANGRIFFE AUF DIESES SYSTEM SIND ZWAR IMMER NOCH MÖGLICH, ABER SIE SIND FÜR EINEN MENSCHEN KLAR ERKENNBAR – WIR MACHEN DIE ANGRIFFE HÖRBAR.
HEY, DA IST M.L. JA WIEDER! DER IST ABER FLEISSIG.

FORSCHUNGSPROJEKT Deepfakes



Wie funktioniert's?
Tiefe neuronale Netzwerke können Bilder und andere Medientypen wie Audiodateien oder Gedichte erzeugen, die erstaunlich realistisch sind. So sehr, dass sie für Menschen oft schwer von echten Inhalten unterschieden werden können. Deepfakes sind eine potentielle Bedrohung für unsere digitale Gesellschaft, zum Beispiel im Hinblick auf Geldwäsche oder den Verlust von Vertrauen in Nachrichtenquellen.

GENERATIVE ADVERSARIAL NETWORKS

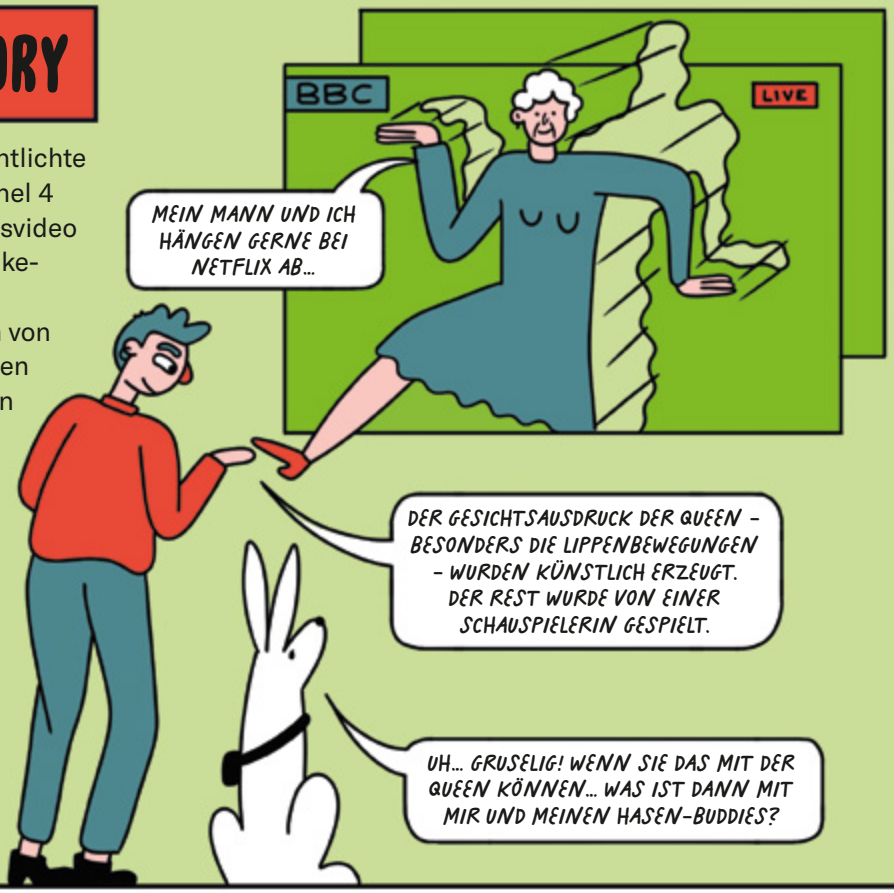
Generative Adversarial Networks (GANs) sind spezielle Formen von Deep Learning-Systemen. GANs bestehen aus zwei tiefen neuronalen Netzen, die miteinander in einem simulierten Spiel interagieren. Durch das ‚Spielen' einer großen Anzahl von Runden lernt der Generator mit der Zeit, sehr echt wirkende Inhalte wie Bilder oder Videos zu erzeugen.

Der ‚Generator' macht Vorschläge. Er soll lernen, wie er Ergebnisse erstellen kann, mit denen er den ‚Unterscheider' täuschen kann.

Der ‚Diskriminator' wertet die Ausgabe des Generators aus. Er ist darauf trainiert, die Ergebnisse von echten Daten zu unterscheiden.

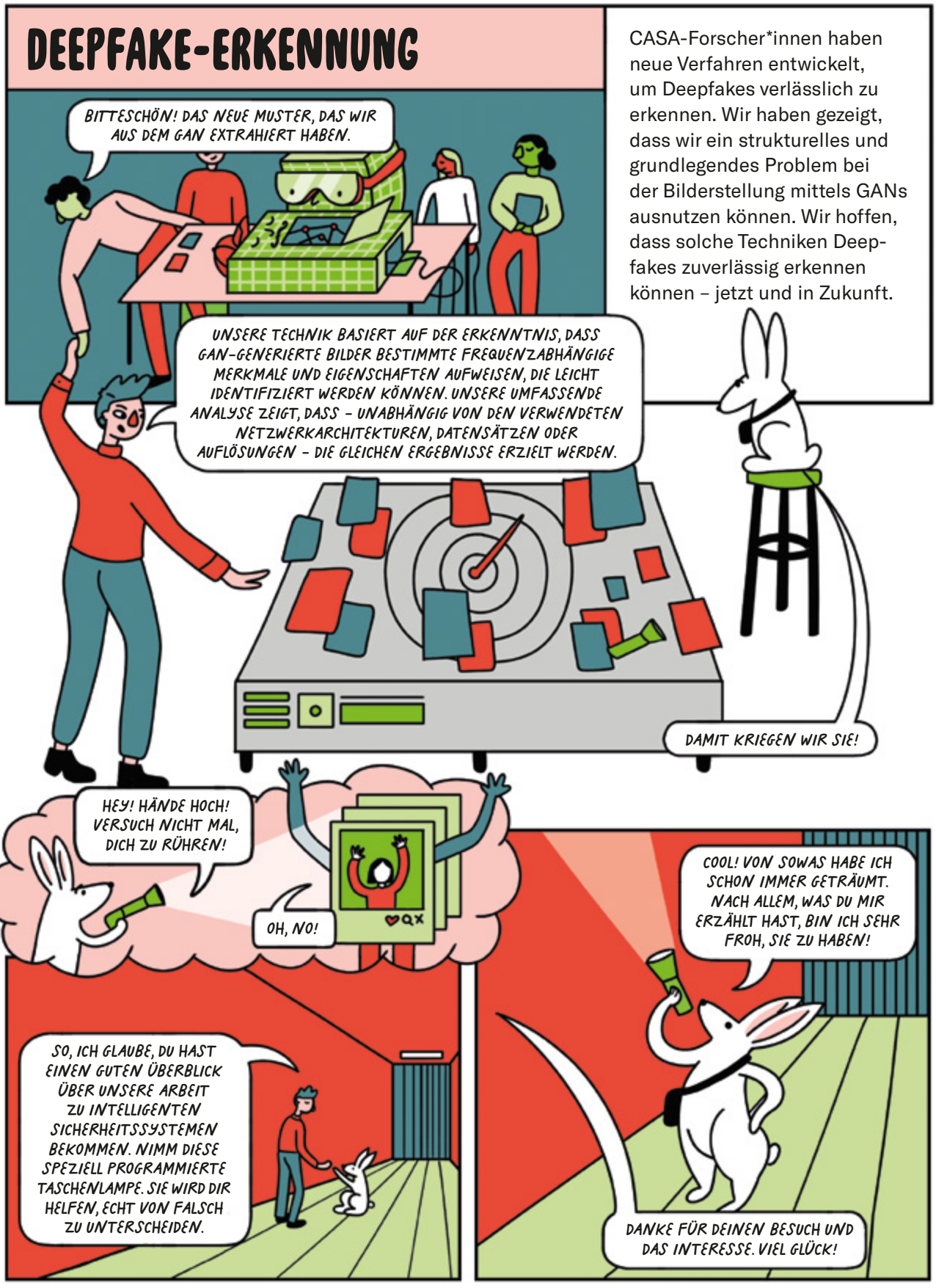
REAL LIFE STORY

Im Dezember 2020 veröffentlichte der britische Sender Channel 4 ein alternatives Weihnachtsvideo der Queen, das mit Deepfake-Techniken erstellt wurde. Stimmfälschungen können von Betrüger*innen für Straftaten genutzt werden. Sie können mit einer nachgeahmten Stimme den Opfern die Identität einer vertrauten Person vortäuschen.
Das Opfer handelt dann im Sinne der Betrüger*innen. Solche Angriffe wurden in den letzten Jahren bereits mehrfach erfolgreich durchgeführt.

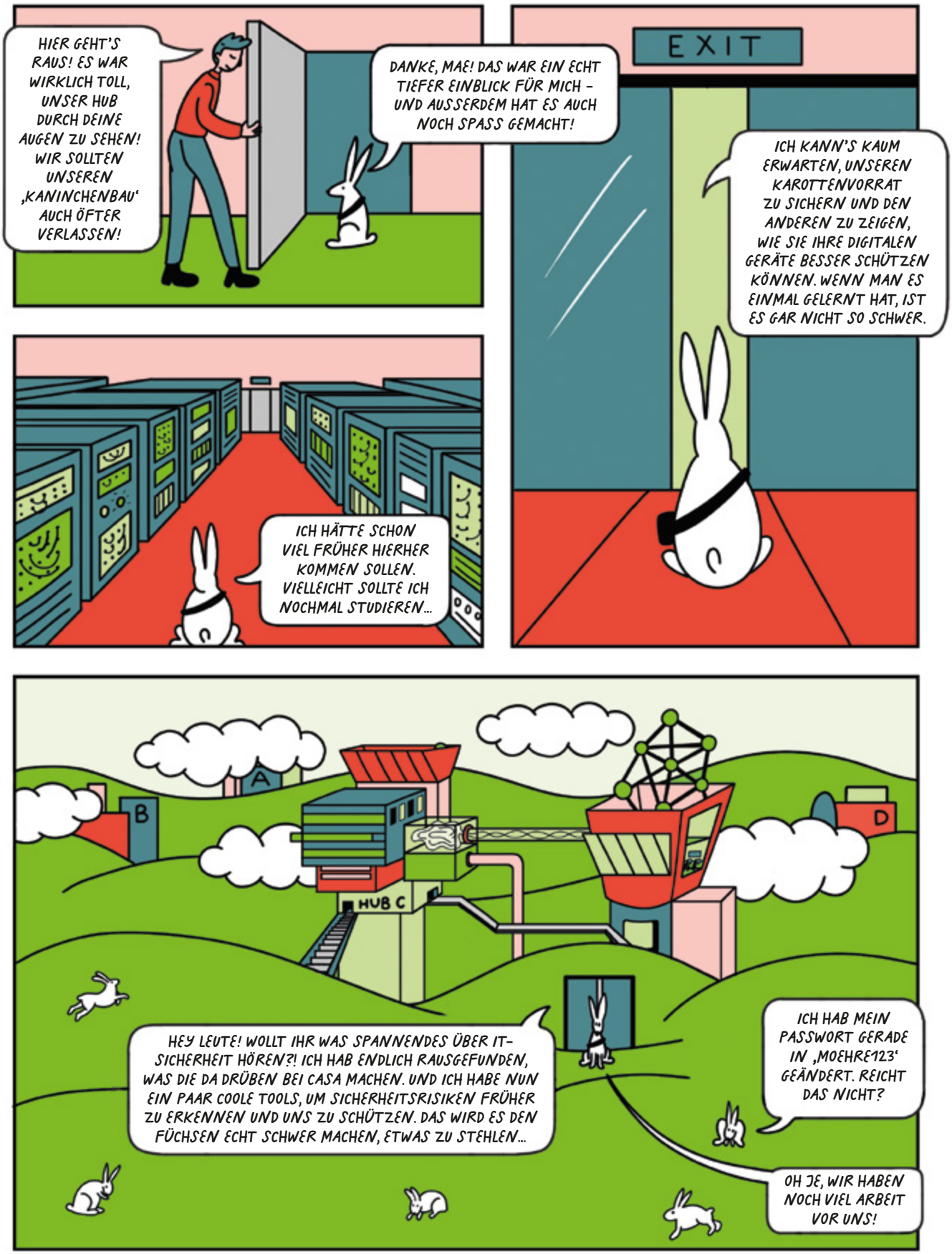


whichfaceisreal.com

DEEPFAKE-ERKENNUNG



CASA-Forscher*innen haben neue Verfahren entwickelt, um Deepfakes verlässlich zu erkennen. Wir haben gezeigt, dass wir ein strukturelles und grundlegendes Problem bei der Bilderstellung mittels GANs ausnutzen können. Wir hoffen, dass solche Techniken Deepfakes zuverlässig erkennen können – jetzt und in Zukunft.


HIER GEHT'S RAUS! ES WAR WIRKLICH TOLL, UNSER HUB DURCH DEINE AUGEN ZU SEHEN! WIR SOLLTEN UNSEREN ‚KANINCHENBAU' AUCH ÖFTER VERLASSEN!
DANKE, MAE! DAS WAR EIN ECHT TIEFER EINBLICK FÜR MICH – UND AUSSERDEM HAT ES AUCH NOCH SPASS GEMACHT!
EXIT
ICH KANN'S KAUM ERWARTEN, UNSEREN KAROTTENVORRAT ZU SICHERN UND DEN ANDEREN ZU ZEIGEN, WIE SIE IHRE DIGITALEN GERÄTE BESSER SCHÜTZEN KÖNNEN. WENN MAN ES EINMAL GELERNT HAT, IST ES GAR NICHT SO SCHWER.
ICH HÄTTE SCHON VIEL FRÜHER HIERHER KOMMEN SOLLEN. VIELLEICHT SOLLTE ICH NOCHMAL STUDIEREN...
A
B
D
HUB C
HEY LEUTE! WOLLT IHR WAS SPANNENDES ÜBER IT-SICHERHEIT HÖREN?! ICH HAB ENDLICH RAUSGEFUNDEN, WAS DIE DA DRÜBEN BEI CASA MACHEN. UND ICH HABE NUN EIN PAAR COOLE TOOLS, UM SICHERHEITSRISIKEN FRÜHER ZU ERKENNEN UND UNS ZU SCHÜTZEN. DAS WIRD ES DEN FÜCHSEN ECHT SCHWER MACHEN, ETWAS ZU STEHLEN...
ICH HAB MEIN PASSWORT GERADE IN ‚MOEHRE123' GEÄNDERT. REICHT DAS NICHT?
OH JE, WIR HABEN NOCH VIEL ARBEIT VOR UNS!


DAS MUSS ICH SOFORT
DEN ANDEREN
ERZÄHLEN...

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

Lukas Bernhard, Michael Rodler, Thorsten Holz und Lucas Davi: **xTag: Mitigating Use-After-Free Vulnerabilities via Software-Based Pointer Tagging on Intel x86-64**, IEEE European Symposium on Security and Privacy, 2022.

Cornelius Aschermann, Sergej Schumilo, Ali Abbasi und Thorsten Holz: **Ijon: Exploring Deep State Spaces via Fuzzing,** IEEE Symposium on Security and Privacy, 2020.

Sergej Schumilo, Cornelius Aschermann, Ali Abbasi, Simon Wörner und Thorsten Holz: **Nyx: Greybox Hypervisor Fuzzing using Fast Snapshots and Affine Types**, USENIX Security Symposium, 2021.

Joel Frank, Thorsten Eisenhofer, Lea Schönherr, Asja Fischer, Dorothea Kolossa und Thorsten Holz: **Leveraging Frequency Analysis for Deep Fake Image Recognition**, International Conference on Machine Learning (ICML), 2020.

Lea Schönherr, Katharina Kohls, Steffen Zeiler, Thorsten Holz und Dorothea Kolossa: **Adversarial Attacks Against Automatic Speech Recognition Systems via Psychoacoustic Hiding**, Network and Distributed System Security (NDSS) Symposium, 2019.

Thorsten Eisenhofer, Lea Schönherr, Joel Frank, Lars Speckemeier, Dorothea Kolossa und Thorsten Holz: **Dompteur: Taming Audio Adversarial Examples**, USENIX Security Symposium, 2021.

ÜBER CASA

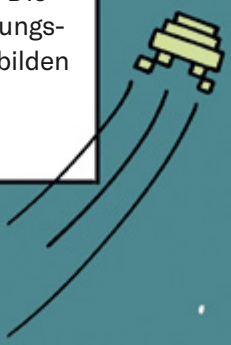
CASA: Cyber Security in the Age of Large-Scale Adversaries wurde 2019 gegründet und ist das einzige Exzellenzcluster im Bereich IT-Sicherheit in Deutschland. Von der Deutschen Forschungsgemeinschaft (DFG) wird CASA mit 30 Millionen Euro über sieben Jahre hinweg gefördert, um ausgezeichnete Forschungsbedingungen 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



CASA HUB C

1. Auflage 2024

Redaktion
Thorsten Holz (CASA/Ruhr-Universität Bochum)
Annika Gödde (CASA/Ruhr-Universität Bochum)
Niels Jansen (Ellery Studio)

Ellery Studio
Art Direction & Design: Luca Bogoni
Illustration: Lucia Cordero, Hannah Schrage
Projektmanagement: Pawel Leyk, Niels Jansen

Umschlaggestaltung
Hannah Schrage, Lucia Cordero

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

Scan den QR-Code, um zur digitalen Version des Comics zu gelangen:

Auf Englisch sind folgende Comics erschienen:

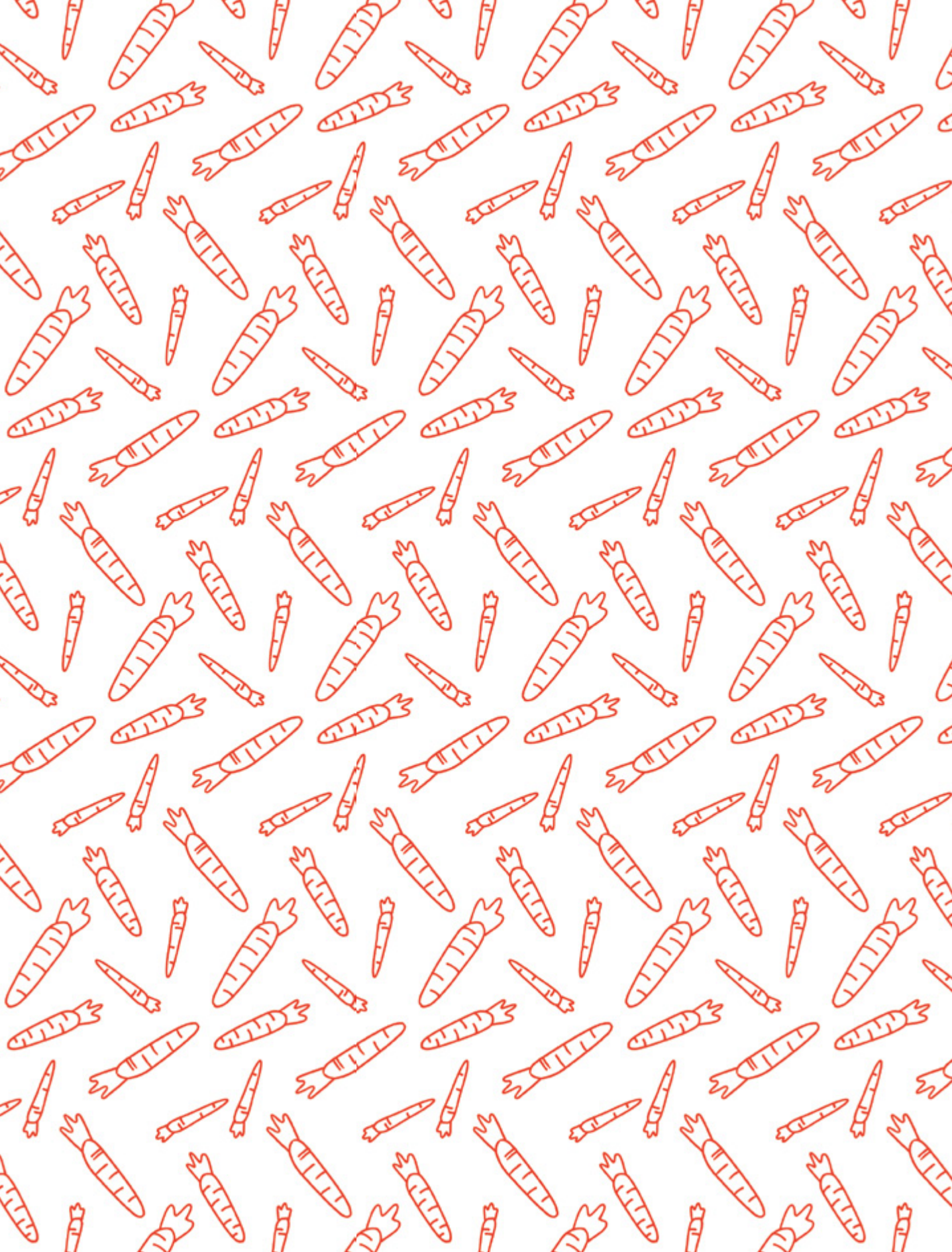
- The Secrets of HUB A and the Traces of the Cookies
- A Deep Dive Into HUB B and the Swirl of Embedded Security
- What's the Fuzz About HUB C and the Missing Carrots?
- HUB D and the Rumble in the Jungle of Usability

CASA
Cyber Security in the Age of Large-Scale Adversaries

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

RUHR UNIVERSITÄT BOCHUM
RUB

ellery studio



DIE WELT WIRD VON DIGITALEN GEFAHREN ÜBERSCHWEMMT. ANGREIFER*INNEN MACHEN SELBST VOR KAROTTENVORRÄTEN NICHT HALT. WAS HEUTE NOCH SICHER SCHEINT, KÖNNTE MORGEN SCHON IN DEN HÄNDEN VON CYBERKRIMINELLEN SEIN.

KANN DIE MUTIGE HÄSIN BETTY IHRE HASENFREUND*INNEN DAVOR BEWAHREN? UND WIE HILFT DIE FORSCHUNG VON CASA DABEI, DIESE BEDROHUNGEN ZU BEKÄMPFEN?

FINDE ES HERAUS!