2. Jan 19.26.47 RES213_Usable_Security

Willkommen zum Forschungspodcast der Helmholtz-Gemeinschaft.

Ich bin Holger Klein.

Karolin Gutauf ist Informatikerin und arbeitet in der Forschungsgruppe Usable Security am CISPA, Helmholtz Zentrum für Informationssicherheit, und sie gehört zu den Helmholtz Juniors.

Hallo Karolin.

Hallo Holger.

Helmholtz Juniors.

Was ist das?

Das ist die Doktorandenvertretung aller Helmholtz Zentren.

So wie so ein Betriebsrat?

Wir haben im Gegensatz zu einem Betriebsrat keine Rechte in dem Sinne und auch keinen Rechtsschutz quasi.

Die sind ja kündigungssicher.

Aber wir vertreten wie ein Fachschaftsrat die Anliegen aller Doktoranden in den Helmholtz Zentren.

Macht ihr denn in den Helmholtz Juniors, findet da auch ein richtiger

wissenschaftlicher Austausch statt?

Oder passiert das auf einer anderen Plattform wieder?

Wissenschaftlicher Austausch in dem Sinne, dass wir natürlich persönlich über unsere Forschung reden und so erzählen, ich mache das.

So wie wir jetzt gerade.

Genau, aber es ist nicht mit dem Ziel, dass wir irgendwie Kollaborationen eingehen, also nicht mit dem Hauptziel, sondern eher, dass wir uns halt kennenlernen.

Und Helmholtz Juniors, da geht es halt auch wirklich eher darum, wie geht es uns, was kann man bei Doktoranden verbessern, was sind Probleme, die auftauchen.

Ein großes Thema ist zum Beispiel auch Power Abuse, Sexual Abuse.

Was wird da an den Zentren gemacht?

Was können wir da in unser Zentrum mitnehmen?

Wofür können wir uns einsetzen?

Wo können wir halt sagen, hier, das wird an einem anderen Zentrum so gemacht.

Die haben da gute Erfahrungen mitgemacht, können wir das nicht bei uns auch so machen?

Und da ist halt so ein ständiger Austausch zwischen den Zentren einfach.

Bevor wir noch weiter abschweifen, lass uns doch mal über deine Arbeit reden, deswegen sind wir ja eigentlich zusammengekommen.

Forschungsgruppe Usable Security.

Bei Dingen, die ich nicht verstehe oder die ich nicht auf Anhieb begreife, frage ich immer nach dem Gegenteil.

Was ist denn eigentlich Unusable Security?

Viel, was wir heute benutzen. (lacht) Ja.

Zum Beispiel?

Passwörter.

Passwörter sind Unusable Security?

Unnütze Sicherheit?

Unnutzbare.

Unnutzbare Sicherheit.

Also ich meine, man kann sie schon nutzen, aber mit Passwörtern kommt man schnell an die Grenzen von dem, wozu sie fähig wären, einfach da wir eingeschränkt sind.

Man ist in seiner Memory-Fähigkeit eingeschränkt.

Okay, ich kann mir nicht diese ganzen coolen Passwörter, die aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen bestehen, merken.

Genau.

Ja, aber ich habe doch einen Passwortmanager.

Genau, der macht das.

Das ist eine Art und Weise, wie das einfacher geht.

Aber natürlich ist da immer noch dieser Punkt dazwischen, dass man irgendwo hingehen muss, man muss ein Passwort eingeben und dann hat man dieses Passwort, was in der Gegend rumfliegt.

Manche Leute schreiben sich das ja auch zum Beispiel dann auf.

Manche Leute versuchen trotzdem, Passwörter sich zu merken.

Ich habe das auch, also ich habe auch bei bestimmten Sachen habe ich das, dass ich Passwörter habe, die ich mir merke.

Bei anderen Sachen habe ich sie auch im Passwortmanager drin.

Aber es ist halt immer dieser Zwischenstep drin, das Passwort, der eigentlich dadurch sicher ist, dass man eine bestimmte Buchstaben-Zahlen-Kombination hat.

Und je zufälliger die ist, also dass sie nicht im Wörterbuch steht oder so, desto sicherer ist sie ja quasi.

Was sie natürlich aber unmerkbarer macht.

Was ist denn dann usable security and privacy?

Aber privacy ist ja klar, das ist, wenn die Tür zu ist.

Nicht unbedingt.

Also usable security and privacy ist ein interdisziplinärer Forschungsbereich, dahingehend, dass wir quasi an der Schnittstelle zwischen Mensch-Maschine-Interaktion oder im Englischen Human-Computer-Interaction und also Human-Computer-Interaction-Forschung und Security-Forschung, auf Deutsch Sicherheitsforschung, agieren und versuchen, Sicherheitsaspekte eben nutzbar zu machen.

Und Passwörter sind da ein großer Teil, Authentifizierungsverfahren sind da ein großer Teil.

Passwort ist doch ein Authentifizierungsverfahren.

Genau, Passwort ist ein Authentifizierungsverfahren.

Fingerprint ist ein Authentifizierungsmechanismus.

Andere biometrische Verfahren, ich weiß nicht, vielleicht hast du schon mal von Passkeys gehört, das ist auch ein Authentifizierungsverfahren.

Das habe ich aber nicht wirklich verstanden.

Das gibt es bei mir, im Browser passiert das manchmal, aber ich habe nicht wirklich verstanden, was das ist.

Das ist ein Authentifizierungsverfahren, bei dem du quasi nicht mehr mitkriegst, was im Hintergrund abläuft, sondern du sagst deiner Device nur, ich möchte mich da einloggen und deine Device wurde aber irgendwann mit der Seite oder der Applikation, wo du dich einloggen möchtest, verbunden.

Das ist ein Vertrauensvorschuss sozusagen.

Diese Webseite ist grundsätzlich vertrauenswürdig, wenn ich sage, ich möchte mich anmelden, dann möchte ich das auch.

Ja, das stimmt in dem Sinne schon, aber zum Beispiel, wenn eine andere Webseite vorgibt, also zum Beispiel, nehmen wir Google als Beispiel, wenn ich ein Passkey bei Google habe, dann kann ich mich mit diesem Passkey auch nur bei Google einloggen.

Wenn jetzt eine andere Webseite vorgibt, Google zu sein, kann ich mich mit diesem Passkey nicht dort einloggen, weil diese Seite, auch wenn sie aussieht wie Google, hat sie nicht die Credentials, die ich bräuchte, um mich dort einloggen zu können.

Das Ganze nennt sich Private Public Key Crypto, das ist ein Schlüsselaustauschverfahren.

Okay, das im Hintergrund, das ist was wir früher mühsam in unsere E-Mail-Clients eingepflegt haben.

Genau.

So was wie PGP, nur halt unsichtbar für mich.

Genau, PGP, ja, so ähnlich.

Okay.

Genau.

Ja, für dich reicht's.

Ich hoffe, dass ich da jetzt auch nichts Falsches sage.

Oh mein Gott, ich habe von PGP ab... Also, du sagst, du arbeitest an der Schnittstelle Mensch-Maschine.

Interaktion.

Interaktion.

Und Security.

Und du bist Informatikerin, aber an der Schnittstelle zum Menschen, das ist doch, ist das nicht eher Psychologie?

Arbeitet ihr mit Psychologen auch dazu?

Wir arbeiten tatsächlich auch mit Psychologen zusammen.

Also, wir haben auf der einen Seite diese Schnittstelle zwischen Mensch-Maschine-Interaktion und Security.

Und auf der anderen Seite arbeiten wir auch als Psychologen, Sozialwissenschaftler zusammen.

Wir machen empirische Forschung tatsächlich.

Also, wir machen quantitative oder qualitative Forschung.

Und was natürlich aus der Sozialwissenschaften und aus der Psychologie kommt.

Wie sieht die aus, diese empirische Forschung?

100 Leute müssen mal hier klicken?

So kann sie aussehen.

Das kommt ein bisschen darauf an, was man erreichen möchte.

Also, das, was ich vor allen Dingen bis jetzt viel gemacht habe, ist, neue Felder ein bisschen so ausleuchten.

Zum Beispiel habe ich mir angeguckt in meinem letzten Paper, was Client-Side-Scanning eigentlich ist.

Hast du schon mal was von Client-Side-Scanning gehört?

Ja, das ist, wenn eine Behörde gerne mitlesen würde, was ich in meinen verschlüsselten Messenger-Botschaften schreibe, das aber nicht darf und darum irgendetwas auf meinem Smartphone macht, das dazu führt, dass sie trotzdem mitlesen kann.

Wir machen das mal ganz anders.

Caro, was ist Client-Side-Scanning?

Ich finde, du hattest da schon sehr viele sehr sinnvolle Punkte drin.

Also, sehr high-level gesehen ist Client-Side-Scanning, wenn man auf einem Endnutzergerät nach bestimmtem Material gezielt sucht.

So, und das Ganze kommt daher, dass Messenger-Dienste angefangen haben, Ende-zu-Ende-Verschlüsselung einzuführen, was ja erstmal nicht schlecht ist.

Nur führt das eben dazu, dass bestimmte Sachen serverseitig nicht mehr gemacht werden können.

Zum Beispiel, was serverseitig super oft gemacht wird, ist, dass nach Missbrauchsmaterial gesucht wird.

Also, dass wenn eine Nachricht, also quasi, ich schicke dir jetzt eine Nachricht, und die kommt aber nicht, also die fliegt nicht direkt zu dir aufs Handy, sondern die geht über einen Server drüber.

Und auf dem Server wird dann, wenn ich dir zum Beispiel ein Bild schicke, wird

dieses Bild gehashed, also hash heißt, dass eine sehr komprimierte Form dieses Bildes in Textform gespeichert wird.

Das ist also, jedes Bild kann quasi als Zahlenstring dargestellt werden, als Zahlenbuchstabenstring.

Klar, weil also Helligkeitsunterschiede, Kontrastunterschiede, die einfach aufnotiert werden dann am Stück, oder wie?

Nee, also ein Hash ist, dass man etwas nimmt und versucht klein zu machen.

Also zum Beispiel, ich versuche das mal ganz einfach zu erklären, dass wenn ich einen roten Apfel habe, dann mappe ich den auf die Farbe rot.

Und dann habe ich eine grüne Birne und die mappe ich auf grün.

So, und dann kann ich das mit verschiedenen Früchten so machen, aber das Problem ist, es gibt halt mehrere rote Früchte, es gibt mehrere grüne Früchte, die würden ja alle in die gleiche Schublade fallen quasi.

Und bei einem Hash ist quasi das Ziel, dass man was Großes auf was Kleines mappen kann, aber dass, egal, also wenn ich zwei verschiedene große Sachen auf zwei kleine Sachen mappe, dass die dann immer trotzdem unterschiedlich sind.

Das heißt, ich muss irgendwie dem Mapping des grünen Apfels auf grün noch irgendwie mitgeben, dass er ein Apfel ist, damit er nicht mit einer Birne verwechselt wird, die auch grün ist.

Genau, zum Beispiel.

Und das wird aber einfach durch Zahlen und Buchstabenkombinationen gemacht.

Also ich werfe den grünen Apfel in eine Box und ich schüttel die Box und aus der Box kommt ein Wort raus.

So, irgendein Wort, keine Ahnung, Prinzessin.

So, und immer wenn ich einen grünen Apfel in diese Box reinwerfe, kommt das Wort Prinzessin raus.

Und immer wenn ich eine grüne Birne reinwerfe, kommt das Wort Topfpflanze raus.

Also diese Box hat irgendeinen Algorithmus drin, der das, was vorne reinkommt, auf ein bestimmtes Wort mappt.

Und immer wenn ich das Gleiche reinwerfe, kommt hinten das Gleiche raus.

Dann muss sich aber irgendwann der Box per Algorithmus gesagt haben, wie sie Birnen von Äpfeln unterscheidet.

Genau.

Das heißt, sie muss alle Birnen und alle Äpfel kennen.

Und wenn ich das jetzt auf Kinderschändungsmaterial übertrage, dann muss doch eigentlich der Algorithmus, der meine Fotos durchsucht, jedes einzelne Missbrauchsbild schon mal gesehen haben, oder nicht?

Ja, da kommen wir als nächstes hin.

Also diese Hashing-Funktion, der ist das erstmal vollkommen egal, was auf einem Bild drauf ist.

Die nimmt einfach dieses Bild und alles, was mit Computer zusammenhängt, basiert ja am Ende auf Nullen und Einsen.

Also das sind mathematische Funktionen auf irgendeine Art und Weise.

Und diese Hashing-Funktion nimmt quasi das Bild und komprimiert dieses Bild runter auf eine Buchstaben-Zahlen-Zeichenfolge.

Und diesem Algorithmus ist vollkommen egal, ob da ein Pferd drauf ist oder ein grüner Apfel oder was auch immer da drauf ist.

Weil der Algorithmus kann das auch nicht wissen.

Wir können das wissen, wenn wir auf dieses Bild drauf gucken, aber der Algorithmus weiß das nicht.

Und was jetzt passiert, ist, dass dieser Hash erstellt wird.

Und es gibt eine Datenbank, die wird, ich glaube, also die größte Datenbank, die es gibt und die mir auch bekannt ist, ist die von NICMIC, das ist das National Center for Missing and Exploited Children.

Die sammeln Missbrauchsdarstellungen, hashen die.

Also die machen genau das Gleiche und dann werden die Hashes jeweils verglichen.

Und wenn dann da ein Match ist, also wenn zwei Hashes gleich sind, also einer aus dieser Datenbank und einer von den Bildern, die über diesen Server drüber gehen, dann wurde quasi ein Treffer gefunden.

Und das, was ich jetzt erklärt habe, basiert quasi auf kryptografischem Hashing.

Es gibt auch noch andere Verfahren, da gehe ich gleich noch mal drauf ein.

Aber das ist im Prinzip das, was passiert, wenn ich dir ein Bild schicke, was nicht

verschlüsselt ist, dann wird auf dem Server geprüft, ob das eine Missbrauchsdarstellung ist.

Und mit der Einführung von Ende zu Ende Verschlüsselung bei Messenger-Diensten geht das ja nicht mehr.

Nee, weil da kommt sowieso nur Zahlensalat bei Raum.

Genau.

Wenn ich jetzt dir eine Nachricht schicke, dann weiß der Server nicht, ob ich dir ein Bild von einem grünen Apfel geschickt habe oder von einem blauen Pferd oder was auch immer.

Das weiß der Server einfach nicht.

Und jetzt gab es ja in der Vergangenheit schon verschiedene andere Optionen, wie man versucht hat, das zu umgehen, also dass man trotzdem kontrollieren kann, dass Leute kein Kindesmissbrauchsmaterial teilen.

Das geht trotz Ende zu Ende Verschlüsselung serverseitig?

Nein, also man versucht, Verfahren zu finden, um das zu machen.

Und eine Idee, auf die man gekommen ist, ist eben Client-Side-Scanning, dass man quasi das Scanning vom Server auf den Client umlegt.

Das bringt natürlich aber neue Probleme mit und das wollte Apple tatsächlich in 2021 einführen.

Also Client-Side-Scanning auf ihren Endgeräten, dass statt auf dem Server auf dem Endgerät nach Kindesmissbrauchsmaterial gesucht wird.

Und da gab es einen riesigen Backlash von der Privacy-Community und der

Security-Community, weil das Problem ist, dass Client-Side-Scanning, je nachdem wie es implementiert ist, eine Überwachungssoftware sein kann.

Ich kann da ja an beliebigen, also wenn, ich stelle mir das gerade so vor, also wenn ich Client-Side-Scanning machen will, dann muss mein Smartphone jeden Tag um Mitternacht eine neue Hash-Liste von irgendeinem Server importieren.

Wenn ich dann irgendetwas mit meinem Messenger mache, wird irgendwas, was ich da rein tue, gehashed und mit dieser Liste abgeglichen.

Das heißt, es könnte ja theoretisch auch jemand einfach in diese Liste ein Hash für Ausdrücke, Worte, Phrasen reinschreiben und meine Inhalte auch daraufhin überprüfen und dann gegebenenfalls irgendwo eine rote Fahne hochgehen lassen, weil der Holger hat mit irgendeiner anderen Person Witze über, weiß ich nicht, anschlagsrelevante Ziele im Regierungsviertel Berlins oder sowas gemacht und auf einmal steht die Staatsanwaltschaft beziehungsweise die Polizei vor meiner Tür.

Genau.

Das wäre möglich.

Ja, also man muss da immer noch darauf aufpassen, dass, also Algorithmen, die auf Bildmaterial ausgelegt sind, können natürlich, also man braucht andere Algorithmen, je nachdem, ob man Bildmaterial hasht oder Text hasht, aber das Grundprinzip hast du quasi verstanden, ist, dass man nicht technisch sagen kann, wenn man nach Kindesmissbrauchsmaterial scannen möchte, dass auch in dieser Datenbank wirklich nur Kindesmissbrauchsmaterial drin ist und nicht vielleicht Propagandamaterial oder sowas.

Wenn das passieren würde, also wenn ich dieses Kleinzeitscanning hätte bei mir, wem könnte ich denn vertrauen, dass das alles mit rechten Dingen zu sich geht?

Das ist eben das Problem, weil technisch kann man das nur begrenzt absichern

und wir sind eben halt darauf gekommen, dass in dieser Debatte um Kleinzeitscanning, manchmal wird das auf EU-Ebene auch Chat-Kontrolle genannt, dass da viel drüber diskutiert wird, aber es nicht so ganz klar ist, über welche technischen Besonderheiten Leute eigentlich diskutieren.

Weil, und da hast du jetzt auch schon einige Sachen von angesprochen, man kann auch verschiedene Arten und Weisen scannen.

Man kann kryptografisch scannen, so mit dem kryptografischen Hashing, was ich eben versucht habe zu erklären.

Und das sind Algorithmen, die kommen aus der Sicherheitsforschung tatsächlich.

Dann gibt es Algorithmen, die kommen aus der Computer Vision Forschung eher, weil die eben auch leichte Änderungen auf Bildern zum Beispiel durchgehen lassen würden.

Das heißt, wenn ich ein Bild von einem grünen Apfel nehme und dann beiße ich an einer Stelle ganz klein in den Apfel rein und mache davon nochmal ein Bild, dann würde dieser Algorithmus das aber als gleiches Bild erkennen.

Genau, also da gibt es verschiedene Varianten, wie man das scannen kann oder man könnte auch Machine Learning Algorithmen nehmen, die aber dann halt auch wieder nur eine Wahrscheinlichkeit geben, ob auf dem Bild wirklich ein Apfel ist oder nicht.

Und dann gibt es halt noch verschiedene andere Sachen, wie sich Client-Side-Scanning halt unterscheiden kann, je nachdem, über welche Implementierung man redet.

Ich überlege die ganze Zeit noch, wie man das so ausgestalten könnte, dass ich keine Sicherheitsbedenken mehr haben muss.

Ist das überhaupt möglich?

Könnte man den Algorithmus offenlegen, der das Hashing übernimmt?

Das natürlich, aber zum Beispiel bei den kryptografischen Hashing-Algorithmen, dass bei Wörtern könnte man da ähnliche Algorithmen nehmen, wie das, was passiert, wenn man Passwörter hasht.

Also das sind kryptografische Verfahren einfach, die sind auch öffentlich zugänglich, weil diese Verfahren einfach öffentlich zugänglich gemacht werden, aus dem Grund, weil sie auch dadurch sicher sind, dass sie öffentlich zugänglich sind.

Bei diesem sogenannten Perceptual Hashing-Verfahren ist es halt auf der anderen Seite so, das sind diese visuellen Verfahren.

Da gibt es schon Paper, das, was gleich aussehen kann, aber zwei verschiedene Sachen darstellt.

Also, dass da nur ganz leichte Sachen verändert worden sind und dass aber dann die Bilder zum Beispiel auf der einen Seite nicht mehr als gleich erkannt werden oder dass sie eben als gleich erkannt werden, auch wenn sie eigentlich zwei komplett verschiedene Sachen zeigen für das Auge.

Das heißt, man hat bei diesem Perceptual Hashing-Verfahren keine hundertprozentige Sicherheit mehr, wenn mir der Algorithmus sagt, das ist ein grüner Apfel, dass das wirklich ein grüner Apfel ist.

Kann man das Client-Side-Scanning in einer solchen Weise ausgestalten, dass ich keine Fragen mehr habe?

Meiner Meinung nach nicht.

Die Sache ist, es gibt, also jeder von uns hat auf eine gewisse Art und Weise

schon Client-Side-Scanning-Algorithmen auf seinen Endgeräten.

Zum Beispiel dein Virusscanner.

Eigentlich macht der auch Client-Side-Scanning.

Ich habe einen Virusscanner?

Nein, das ist ein Adblocker.

Das ist ein Adblocker, der macht wahrscheinlich auch Client-Side-Scanning.

Ja, auf eine gewisse Art und Weise, ja.

Oder ich weiß nicht, was du für ein Handy hast, aber ich habe ein iPhone und da wird mir zum Beispiel eine Liste angezeigt von Leuten, die auf Fotos sind von mir.

Und da kann ich angeben, das ist der Paul, das ist der Max, das ist die Lea.

Voll gruselig, ja, habe ich auch.

Genau, das ist aber auch eine Art von Client-Side-Scanning, weil da halt quasi was gescannt wird und dann werden Informationen zusammen aggregiert.

Und das, was wir aber in Bezug auf Client-Side-Scanning und Kindesmissbrauchsmaterial auch rausgefunden haben, ist, dass es halt sehr darauf ankommt, ob man für eine Technologie den Nutzer als Beneficiary von dieser Technologie ansieht, also dass der was davon hat, oder ob man den Nutzer als Gegner ansieht.

Also, dass man denkt, dass diese Person etwas falsch gemacht hat.

Und bei Client-Side-Scanning, um nach Kindesmissbrauchsmaterial zu suchen, wird ja der Nutzer immer unter Generalverdacht gestellt.

Und das ist ein riesengroßes Problem.

Und das ist meiner Meinung nach, sollte man auch keine Technologie bauen, die den Nutzer erst mal unter Generalverdacht stellt, weil das einfach zu sehr vielen Problemen führen kann.

Wie genau hat deine Forschung am Client-Side-Scanning denn jetzt ausgesehen?

Wir haben uns angeguckt, was Leute eigentlich unter Client-Side-Scanning verstehen und welche Erwartungen sie haben und welche Auswirkungen sie sehen können.

Also Erwartungen und Auswirkungen, wenn man das für Client-Side-Scanning einsetzen würde.

Und die Sache mit Client-Side-Scanning ist, für Kindesmissbrauchsmaterial gab es das zu dem Zeitpunkt nicht, gibt es ja auch immer noch nicht.

Und deswegen haben wir mit Experten darüber gesprochen und haben versucht, deren mentale Modelle abzufragen.

Mentale Modelle?

Ja, genau.

Ein mentales Modell ist die Art und Weise, wie wir die Welt um uns herum uns erklären.

Okay, ist das, um das wissenschaftlich zu bearbeiten, musst du standardisieren.

Gibt es da, wie sieht das aus?

Also wir haben ja mentale Modelle von allem.

Aber wenn ich dich nach deinem mentalen Modell von einem Stuhl frage, kannst du das wahrscheinlich einfacher beantworten, als wenn ich dich nach deinem mentalen Modell von einem Fahrrad frage, weil Fahrrad schon ein bisschen komplizierter aufgebaut ist als ein Stuhl.

Und alles, was sich mit Informatik beschäftigt, ist ja erstmal auch inhärent abstrakt.

Also das ist ja nichts, was man erstmal anfassen kann.

Wir haben ja Endgeräte, die quasi uns diesen Zugang dazu ermöglichen.

Aber das, was da drin passiert, das ist ja für ganz viele Menschen, also ich verstehe da auch nicht alles, was passiert, aber das ist sehr kompliziert.

Und was wir halt eben machen, wir versuchen, diese mentalen Modelle teilweise abzufragen, um zu verstehen, okay, wo ist denn der, also wie ist denn der Wissensstand von Nutzern oder von Experten, wie verstehen die das?

Also so wie du das eben mit mir gemacht hast?

Genau.

Was weißt du denn darüber?

Genau.

Okay.

Und das haben wir quasi mit Experten gemacht zum Thema Client-Side-Scanning, haben uns mit denen hingesetzt und haben gefragt, was verstehst du unter Client-Side-Scanning?

Natürlich ein bisschen elaborierter, wir hatten da eine ausgearbeitete Interview-Guideline und dann haben wir diese Information gesammelt und ausgewertet und da quasi ein großes mentales Modell gebaut.

Wir nennen das aggregiertes mentales Modell, weil die Sache mit Client-Side-Scanning ist, dass Leute verschiedene mentale Modelle hatten, aber diese mentalen Modelle nicht unbedingt falsch waren, sondern einfach verschiedene Aspekte beschrieben haben.

Zum Beispiel, dass manche Leute gesagt haben, okay, wir benutzen kryptographisches Hashing, wir benutzen Perceptual Hashing, wir benutzen Machine Learning oder dass sie gesagt haben, wir scannen Texte oder Bilder.

Das sind ja alles verschiedene Sachen, die aber erstmal nicht falsch sind, wenn man Client-Side-Scanning so erklärt, sondern das sind einfach verschiedene Seiten der gleichen Sache.

Ihr hattet euer aggregiertes mentales Modell und was habt ihr damit gemacht?

Das war ein Ergebnis von unserem Paper.

Ach so, das Modell selbst ist das Ergebnis?

Ja, genau, das Modell selbst war ein Ergebnis unseres Papers und dann eben Erwartungen, die Leute an Client-Side-Scanning im Kontext von Kindesmissbrauch gestellt haben.

Die mentalen Modelle haben wir uns tatsächlich nicht im Kontext von Kindesmissbrauchsmaterial angeguckt, weil diese mentalen Modelle sehr übergreifend sind und da auch nur in sehr kleinen Teilen kontextbezogen sind.

Und dann haben wir uns eben diese Erwartungen und Implikationen kontextbezogen auf Kindesmissbrauchsmaterial angeguckt und da sind auch

ziemlich interessante Sachen rausgekommen.

Zum Beispiel haben wir rausgefunden, das geht jetzt eher in die Erwartungsrichtung, und da erwarten einfach viele, dass Client-Side-Scanning, sollte es jemals für Kindesmissbrauchsmaterial eingeführt werden, dass es einfach anderweitig missbraucht werden würde.

Und dann bei den Implikationen zum Beispiel haben wir rausgefunden, dass es halt, also es gibt auf verschiedenen Ebenen Implikationen und eine Einführung könnte zum Beispiel auch dazu führen, dass Leute einfach weniger technische Geräte benutzen, weil sie sich eben so beobachtet fühlen, weil sie ja quasi von ihrem Endgerät unter Generalverdacht gestellt werden würden.

Gerade wenn zum Beispiel dieses Client-Side-Scanning, wenn es Sachen finden würde, diese reporten würde an die Polizei oder an den Electronic Service Provider oder so.

Und dann insbesondere, wenn das auch nicht den Nutzern mitgeteilt wird, dass das passiert.

Naja, früher oder später kriegst du es mit, weil wie ich eben sagte, dann steht die Polizei bei dir vor der Tür und dann ist Beweislastumkehr.

Dann muss ich belegen, dass es ein unverfängliches Foto war, das ich da gepostet habe.

Das könnte durchaus sein.

Das kommt natürlich auf die Rechtslage an.

Was aber auch erwartet wird, dadurch, dass diese, also dass nur kryptographische Algorithmen quasi zu 100% sagen können, ja, das ist etwas oder das ist nicht etwas.

Und zwar das auch nur so lange, bis sie nicht kaputt gemacht werden.

Also dass das eben quasi zwei verschiedene Sachen auf genau den gleichen kleinen Wert mappen.

Genau, also da können nur kryptographische Algorithmen hundertprozentig sagen, etwas ist etwas oder etwas ist etwas nicht.

Und bei den anderen Arten von Algorithmen gibt es normalerweise immer eine Zone, wo falsche Treffer rauskommen können.

Und da wird erwartet, dass die aber bei der Masse an Bildern, die wir weltweit haben, so groß sein wird, dass quasi komplette Systeme einfach vollkommen überlastet werden.

Das klingt gerade so, als wäre das technisch auch eher fragwürdig.

Ist das technisch möglich?

Also ist mein Smartphone leistungsfähig genug, um das theoretisch zu leisten?

Also so ein Kleinsight-Scanning nach jedem Foto, das ich hin und her schicke?

Das kommt auf die Umsetzung an, tatsächlich.

Mit Sicherheit könnte man es auf eine Art und Weise bauen, dass es möglich wäre.

Also auf dem Gebiet bin ich keine Expertin.

Das ist einfach meine persönliche Meinung.

Da gibt es aber auch verschiedene Varianten.

Also man könnte zum Beispiel die Datenbank an Hashes auf dem Endgerät storen.

Man könnte es so machen, dass jeder Hash quasi zu einem Server geschickt wird.

Dann ist aber auch wieder das Problem, na ja, der Hash könnte ja eigentlich auch verraten, was auf meinem Endgerät liegt, wenn der Algorithmus kaputt wäre.

Da kommen direkt sehr, sehr viele Punkte, die mit reinspielen, je nachdem, wie dieser Algorithmus halt aufgebaut wäre.

Alleine schon der Umstand, dass der Hash von meinem Smartphone zu einem Server geschickt wird, das ist ja schon wieder ein Angriffsvektor.

Also ich muss ja nur den Hash abfangen und das mit der Liste abgleichen.

Und dann weiß ich, was du auf deinem Telefon gerade tust.

Das kann ja auch nicht in meinem Interesse dann ja auch sein.

Ja, also das muss auch nicht sein, dass ein Hash das Gerät verlässt.

Es kann auch sein, dass der Hash erst das Gerät verlässt, wenn wirklich ein Treffer gefunden wurde.

Aber das sind alles so Implementierungsdetails, wovon halt auch die Art und Weise der Implementierung abhängig ist.

Aber was zum Beispiel auch eine Art von Client-Side-Scanning ist und was auch in diese Richtung geht, Apple hat sogenannte Sensitive Content Warnings eingeführt, die Nacktbilder verschleiern.

Das kann man bei Apple-Geräten einstellen.

Das wird auch bei Kinder-Accounts per Default an, dass Nacktbilder quasi geblurrt werden.

Und ich glaube, das funktioniert auf dem gleichen Algorithmus wie den, den die auch bei Client-Side-Scanning einführen wollten.

Aber woher weiß das denn, dass das ein Nacktbild ist?

Das kann ja auch sein, dass das einfach nur jemand ist, der keine Haare hat, so wie ich und darum sehr viel Haut zeigt.

Theoretisch könnte das falsch anschlagen.

Und dann steht da auch, ich weiß jetzt nicht mehr, was bei Apple genau steht, aber da steht irgendeine Warnung, da könnten Nacktfotos hinten dran sein.

Überleg dir, ob du dir das angucken möchtest.

Und die Sache ist aber, ob dahinter wirklich Nacktfotos sind oder nicht, weiß ich erst, wenn ich mir das angeguckt habe, weil dieser Algorithmus keine hundertprozentige Eindeutigkeit darüber geben kann, ob das wirklich eins ist oder nicht.

Mustererkennung können wir besser.

Ja, also natürlich sind da AIs mittlerweile auch ganz gut drin, aber das basiert dann auch auf den Daten, die da hinten dran liegen.

Was, also ihr habt euer mentales Modell.

Was mache ich mit dem?

Was fange ich mit dem Ding jetzt an?

Was wir erst mal wollten, was uns ganz, ganz wichtig war, ist eine Grundlage schaffen, dass sich Leute hinsetzen können, wenn sie über Client-Side-Scanning reden, dass sie sagen können, okay, ich meine jetzt das.

Eine Diskussionsgrundlage und zwar eine fundierte.

Genau.

Genau, dass sie wirklich sich hinsetzen können, diese verschiedenen Punkte abgehen können und sagen können, hier meine ich das, da meine ich das.

Dass man halt wirklich über was Ähnliches diskutieren kann, weil je nachdem, wie diese Art und Weise, diese Implementierung von Client-Side-Scanning quasi aussieht, hat es natürlich auch andere Auswirkungen auf die Erwartungen und die daraus folgenden Implikationen.

Was anderes, was ich gelesen habe, ist, dass du mit zwei Kolleginnen zusammen knapp 100.000 Dollar von Google abgreifen konntest, bei deren Trust and Safety Research Awards.

Was habt ihr denen gesagt, was ihr mit dem Geld machen wollt, dass ihr es gekriegt habt?

Das passt da ganz gut hinten dran.

Mit meiner Supervisorin und einem Kollegen haben wir diesen Antrag eingereicht.

Da geht es um Sicherheitsmaßnahmen in Ende-zu-Ende-verschlüsselten Chats.

Da sind wir so ein bisschen draufgekommen, weil ...

Und da bist du ja quasi auch draufgekommen, Client-Side-Scanning ist jetzt nicht so wirklich die Lösung des Problems, um Kindesmissbrauchsmaterial

einzuschränken, meiner Meinung nach.

Der Kollege, Matthias Fassel, und ich und unsere Supervisorin Katharina Krompolz, wir haben uns eben zusammengesetzt und haben überlegt, na ja, was kann man da denn ansonsten machen?

Und sind dann eben auf die Idee gekommen, na ja, was kann man Kindern, Jugendlichen, Erwachsenen mit an die Hand geben, dass sie informierte Entscheidungen treffen können, wenn sie in potenziell riskanten Situationen in Messengern sind.

Potenziell riskant immer bezogen auf Kindesmissbrauchsmaterial oder abstrakt?

Da haben wir tatsächlich die Erweiterung von Kindesmissbrauchsmaterial auf Kindesmissbrauch und Kindesausbeutung, also vor allen Dingen im Hinblick auf sexuelle Risiken erweitert.

Weil wir gesagt haben, okay, also diese Kindesmissbrauchsmaterial-Einschränkung, also dass das weniger verteilt werden, würde durch die Einführung von Client-Side-Scanning, was ja auch umgegangen werden kann, wenn man dann wieder einfach die Applikationen nicht nutzt, die das einfach benutzen.

Und da dachten wir, na ja, wie können wir da von einer anderen Perspektive einfach drauf gucken?

Und so ist eben diese Idee gekommen, weil Matthias, der hat, also genau, ich habe dieses Client-Side-Scanning-Paper mit Deviantu geschrieben.

Matthias war bei der Europäischen Kommission und hat dann ein Praktikum gemacht, ein Internship.

Und ich habe den in Brüssel besucht.

Und dann haben wir darüber geredet, dass wir Client-Side-Scanning nicht gut finden dahin gehen, dass es das Problem löst, weil es das Problem auch einfach nicht lösen würde, sondern es wäre halt ein Teil des Puzzles.

Und dann haben wir überlegt, na ja, was können wir machen?

Und haben einen Blog-Beitrag von Karen Melchior gefunden oder Matthias hatte den, glaube ich, gefunden und hat mir den gezeigt.

Und da hat sie drüber geredet über Dinge, die man in Chats machen kann direkt.

Und dann dachten wir, na ja, das ist ja eigentlich eine voll coole Idee und haben das quasi weiterentwickelt zu dieser Forschungsidee, wie können Sicherheitsmaßnahmen in Ende-zu-Ende verschlüsselten Messengern aussehen.

Und das haben wir als Forschungsprojekt bei Google eingereicht und haben dafür Geld bekommen.

Habt ihr damit schon angefangen?

Also was sind diese Dinge, die man in Chats machen kann?

Wir sind da gerade, also das ist ein aktuell laufendes Forschungsprojekt, wo wir gerade dran arbeiten.

Also das ist auch die Hauptsache, an der ich gerade arbeite.

Und was wir gerade machen, ist, dass wir mit Experten reden, welche Ideen die Leute haben.

Also wir reden mit Experten aus dem Kinderschutz, von Trust and Safety.

Wir wollen auch mit Leuten von Electronic Service Providern reden, mit der Polizei.

Was Leute, die sich quasi mit diesem Thema Kinderschutz über ihren Beruf beschäftigen, was die für Ideen haben, was man in Chats einfach Leuten mit an die Hand geben könnte.

Wir fokussieren uns quasi wirklich darauf, was für Schutzmaßnahmen in Chatsituationen einfach genutzt werden können.

Also das, was man zum Beispiel von Instagram kennt, ist, dass man Leute blockieren kann oder man kann Dinge reporten.

Das sind die Schutzmaßnahmen, die es eben heute gibt.

Es gibt diese Sensitive Content Warning bei Apple oder ich glaube, das heißt Conversation Safety bei den Kinderaccounts.

Instagram hat jetzt ganz viele Sachen eingeführt, um gegen Sextortion vorzugehen, um das ein bisschen besser in den Griff zu kriegen auf der Plattform.

Was die auch machen, ist, dass die eben Nacktbilder blören, dass Kinder sich an Vertrauenspersonen wenden können.

Und also das sind Sachen, die gibt es oder die werden aktuell eingeführt.

Und warum wir quasi trotzdem mit Experten reden, ist, dass wir uns halt überlegt haben, naja, ist das aber alles, was man machen kann?

Kann man da nicht vielleicht mehr machen?

Ist das wirklich das, was Kindern und Jugendlichen hilft?

Vor allen Dingen, wenn bei Instagram ist das zum Beispiel so, da habe ich, ich habe am Mittwoch erst einen Vortrag über mein Forschungszimmer gehalten und

da habe ich diese Sicherheitsfeatures von Instagram draufgepackt.

Und da war eine Seite, da war von oben bis unten Text, wenn dann diese Hilfe-Seite kam.

Und das ist halt auch die Frage, naja, können 15-Jährige damit umgehen?

Lesen die sich das dann überhaupt durch?

Niemand liest sich das durch, oder?

Ja, und dann ist halt die Frage, wie können wir halt diese Information, die Kinder und Jugendliche brauchen oder junge Erwachsene oder auch Erwachsene überhaupt, also jeder Mann, wie können wir diese Information einfach bestmöglich darstellen?

Und das ist quasi so das Ziel, wo wir drauf hinarbeiten wollen mit diesem Forschungsprojekt.

Und das ist dann auch wieder die Aufgabe der Informatik, diese Darstellungsfrage zu lösen.

Aber die psychologische oder sozialpsychologische Seite dieser Arbeit ist dann überhaupt erst mal das Reden mit Leuten und im Grunde das Sammeln mentaler Modelle dafür.

Ja, ich weiß nicht, ob man das wirklich so krass teilen kann.

Es ist eben empirische, also das, was wir gerade machen, ist quasi das Thema explorativ aufzuarbeiten, weil die Sache ist auch, und das war uns auch ganz wichtig, wir wollten nicht direkt mit Jugendlichen reden.

Also wir haben jetzt zum Beispiel in unsere Experten auch junge Erwachsene mit einvernehmlicher Sexting-Erfahrung aufgenommen, also 18- bis 21-Jährige, die

eben schon selber Einverständnis dazu geben dürfen, dass sie an einer Studie teilnehmen können, aber halt noch nicht sehr lange aus dieser Jugend, aus dieser unteren 18-Perspektive raus sind, dass wir die auch fragen, na ja, was würdet ihr in diesen Situationen empfehlen?

Fallen euch da Dinge ein?

Und wir versuchen halt eben, diese Informationen zu sammeln und das explorativ aufzuarbeiten, um das dann zu nehmen, um mit eben jungen Erwachsenen und älteren Teenagern darüber zu reden und zu sagen, sagen zu können, okay, wir haben diese Ideen gesammelt, was haltet ihr davon, wie würdet ihr die umsetzen?

Würde euch das helfen, würde euch das überhaupt nicht helfen?

Was würdet ihr verändern, um quasi einen Anhaltspunkt zu haben, der ein bisschen weitergeht als, ja, wir benutzen Nacktfilter und ihr könnt jemanden blockieren und ihr könnt jemanden reporten und ihr könnt euch an Vertrauenspersonen wenden.

Wie bist du eigentlich als Informatikerin zur empirischen Forschung gekommen?

Wolltest du eigentlich lieber empirisch forschen und hast versehentlich Informatik studiert?

Wie kommt das?

Normal scheint mir das nicht.

Also ich wollte eigentlich Pilotin werden.

Wenn ich will.

Ja, das hat aber nicht funktioniert.

Ich bin nicht multitaskingfähig, das hat mir die Lufthansa bescheinigt.

Und darum arbeitest du lieber seriell in der Informatik?

Naja, so viel Multitasking muss ich hier nicht machen.

Genau, also mein Plan B war quasi Informatik zu studieren.

Und das ist aber, also Pilot sein, ich bin eigentlich ganz froh, dass ich keine Pilotin geworden bin, weil ich da auch immer dachte so, ich kann das ein paar Jahre machen und dann ist mir das zu langweilig.

Deswegen bin ich eigentlich auch ganz froh, dass ich Informatik studiert habe.

Und dann habe ich tatsächlich Bachelor und Master gemacht und bin dann in die Industrie gegangen und habe da als Application Owner und Business Analystin gearbeitet und dachte dann so, naja, ich möchte jetzt was Neues machen.

Und dann hat eine sehr gute Freundin von mir, hat gemeint, die war schon als Doktorandin in Katharinas Gruppe, die hatte gerade ein paar Monate vorher angefangen und die meinte zu mir, Caro, dieses Thema wird dir gefallen.

Und ich habe mir ein Paper durchgelesen und fand das super spannend.

Welches Paper war das?

Ich weiß nicht mehr, wie es hieß, aber das ist ein Paper von Katharina, da ging es um Force-Touch-Pins.

Also normalerweise, wenn man Pins eingibt, gibt man ja quasi einfach nur eine Zahlenkombination ein, also eins, zwei, drei, vier.

Und Katharina hatte sich angeguckt, ob man Pins auch mit verschiedenem Druck

eingeben kann.

Also das Problem an Pins ist ja, man kann, also wenn ich die eingebe und du stehst neben mir, dann siehst du ja, was meine Pin ist.

So, das Ganze nennt sich Shoulder Surfing.

Und das will man ja eigentlich verhindern.

Und was Katharina sich dann angeguckt hat mit ein paar, also mit Kollegen, das hat sie nicht alleine gemacht, war, ob man eben Pins mit unterschiedlichem Druck eingeben kann und ob das auch funktioniert, dass man dann trotzdem immer wieder die gleiche Pin eingibt.

Also auch immer mit dem gleichen Druck.

Ach so, das heißt, ich müsste mir merken, welchen Druck ich ausgeübt habe auf eine Stelle.

Okay.

Genau.

Und das hat aber tatsächlich auch ganz gut funktioniert.

Und ich fand dieses Paper so interessant, dass ich gedacht habe, boah, ja, da würde ich gerne drin arbeiten.

Das würde ich gerne die nächsten paar Jahre machen.

Und dann habe ich mich beworben.

Und dann hat das ein paar Monate gedauert, bis Katharina eine freie Stelle hatte.

Und dann hat sie sich, also glücklicherweise für mich, hat sie sich gedacht, dass wir das zusammen ausprobieren können.

Und dann habe ich bei ihr als Doktorandin angefangen.

Musst du eigentlich, wenn du IT Security machst, musst du doch noch immer so Fragen beantworten.

Wann bist du das letzte Mal auf Phishing reingefallen und so was?

Das musste ich tatsächlich noch nie beantworten.

Echt?

Wann bist du das letzte Mal auf Phishing reingefallen?

Ähm, ich weiß ehrlich gesagt nicht, ob ich jemals Opfer von Phishing geworden bin, weil ich ziemlich viele Sachen einfach ignoriere.

So, also E-Mails, wenn, wenn, ich habe auch, das, das regt, also das findet eine Freundin von, eine, eine spezielle Freundin, und zwar die, die mich auch auf die Doktorandenstelle gebracht hat.

Ich finde das furchtbar.

Ich glaube, ich habe auf meinem privaten E-Mail-Account 40.000 ungelesene E-Mails, weil ich die einfach dann so, einfach übergehe.

Ich könnte nachts nicht schlafen, wenn da so eine Zahl steht.

Das sagt sie auch, und mir ist das einfach, mir ist das vollkommen egal.

Bei mir sind es 16, und das macht mich nervös.

Es gibt zwei Arten von Menschen.

Ganz offensichtlich.

Mir ist das vollkommen egal, ob ich da 40.000 habe oder 10, keine Ahnung, es ist mir einfach egal.

Okay, dann kommt jetzt die, zum Ausstieg sozusagen, kommt jetzt die Standard-Journalisten-Frage an IT-Security-Leute.

Was sind deine Top-3-Security-Tipps für Normalverbraucher?

Meine Top-3-Security-Tipps?

Backups machen.

No backup, no mercy.

Und da, und das ist das, was ich tatsächlich mache, es so einfach wie möglich machen.

Also mein Handy-Backup, das ist zwar mit, also es ginge mit Sicherheit sicherer, aber mein Handy-Backup wird in die iCloud gemacht, weil ich mich da um nichts kümmern muss.

Und mein Computer-Backup wird über meinen Bildschirm gemacht.

Jedes Mal, wenn ich meinen Computer an meinen Bildschirm anschließe, wird da automatisch, also hängt da die Backup-Festplatte dran.

Und dann passiert das Backup im Hintergrund.

Also da einfach Verfahren für einen finden, die so low barrier wie möglich sind.

Weil also bei mir, ich bin da ganz furchtbar drin.

Wenn es nicht einfach geht, dann mache ich das nicht.

Ja, das ist ja sowieso, das ist auch so ein grundsätzliches Problem mit allen möglichen Fragen der IT-Security.

Also jetzt auf Anwenderseite, wir hatten es ja vorhin von PGP.

Das hat einfach mal einen halben Tag gedauert, bis ich das so weit durchdrungen hatte, dass ich meine E-Mails verschlüsseln konnte.

Und dann hat es in der Hälfte der Fälle trotzdem nicht funktioniert.

Und irgendwann habe ich halt gedacht, ja komm, dann lasse ich es.

Deswegen gibt es Usable Security & Privacy, damit wir solche Sachen besser machen.

Bei PGP hat das semi-gut funktioniert.

Ich hoffe, dass wir das bei anderen Sachen besser hinkriegen.

Bei welchen Sachen würdest du das gerne besser hinkriegen?

Hast du da schon eine Ahnung, wo es so schöne One-Click-Lösungen gibt, auf die ich mich auch verlassen kann?

Ich hoffe, dass wir irgendwann von Passwörtern wegkommen.

Ich weiß nicht, wie wir das machen.

Ich glaube, das wird auch noch ganz lange dauern, weil wir bis jetzt immer noch keine sinnvolle Alternative gefunden haben.

Weil alles, was wir bis jetzt haben, kommt halt auch mit Nachteilen einher.

Also Passkeys zum Beispiel, das wird aktuell ein bisschen, also das fängt an, dass Leute das mehr mitkriegen und so.

Passkeys bei Apple wurden dahingehend eingeführt, dass die über die Cloud synchronisiert werden.

Was eigentlich wieder zu einem Sicherheitsproblem führen kann.

Und dann hat man zum Beispiel bei Fingerabdruck, hast du das Problem, dass jemand einen Fingerabdruck nachbauen kann.

Wenn jemand dein Gesicht irgendwie, also wenn jemand Face-ID austricksen kann, dann kannst du dein Gesicht quasi auch nicht mehr benutzen.

Und wir haben quasi mit diesen ganzen Authentifizierungsmechanismen, die wir heute kennen, gibt es immer irgendwelche Nachteile.

Und da hoffe ich, dass wir irgendwann an den Punkt kommen, wo wir was finden, wo wir sagen können, also dass wir was finden, wo wir sagen können, das da ist sicher und es ist einfach benutzbar.

Und da gibt es auch tatsächlich noch nichts am Horizont, was weiß ich, Laser, Iris-Scanner wie in diesem Agentenfilm oder so was, nur halt in winzig klein, sodass es auch benutzbar ist?

Naja, da hast du halt auch das Problem, wenn jemand da rausfindet, wie er Iris... - Ein Auge nachmacht.

Ja genau, wie er ein Auge nachmacht, dann kannst du dein Auge nicht mehr benutzen.

Weil das ist das Problem eben mit biometrischen Daten.

Du kannst sie nicht verändern.

Das heißt, wenn jemand anderes sich für dich ausgeben kann, dann hast du ein Problem. - Dann kann er das, für immer.

Genau, und das ist ja aber auch wieder zum Beispiel der Vorteil bei Passwörtern.

Wenn jemand dein Passwort rauskriegt, dann kannst du es ändern.

Wenn jemand deinen Fingerabdruck klaut, deinen Fingerabdruck kannst du nicht so einfach ändern.

Tipp zwei.

Mein Tipp zwei ist, wenn irgendwas nicht funktioniert, ist meistens nicht, also in 99 Prozent der Fälle, nicht der Nutzer schuld.

Das musst du noch mal ein bisschen ausführen.

Also ich dachte, das wäre dann immer Fehler 35, also der 35 Zentimeter vorm Bildschirm sitzt.

Nein. - Okay.

Was ist denn dann Schuld?

Der Geist in der Maschine.

Ja, so in etwa.

Also meistens, in den meisten Fällen wirklich, wenn irgendwas nicht funktioniert, ist die Technik schuld.

Beziehungsweise, ich möchte keine Schuldzuweisung machen, aber dann wurde im Prozess, als diese Technologie entwickelt wurde, eben irgendwas nicht bedacht.

Zum Beispiel, wenn ich mit meinem Passwortmanager auf einer Webseite ein Passwort eingeben möchte, und das funktioniert nicht, weil die Webseite das halt schlecht implementiert hat und das einfach nicht kompatibel ist mit dem Passwortmanager.

Kenne ich.

So, dann denke ich natürlich zuerst mal, okay, ich bin das Problem.

Aber eigentlich ist halt die Komplikation …

Das Erste, was ich mache, ist zu gucken, ob ich ein Update meines Passwortmanagers verpasst habe.

Das ist aber eigentlich halt wahrscheinlich eher das Problem auf der Webseiteseite als auf deiner Seite.

Das sind aber doch sehr beruhigende Nachrichten.

Im Zweifelsfall war ich's nicht.

Das ist ganz schön.

Man hat halt Menschen sehr lange erzählt, dass sie das Problem sind, wenn irgendwas am Computer nicht funktioniert.

Mit Sicherheit gibt's da auch Sachen, wo man mehr wissen könnte oder so.

Aber meiner Meinung nach sollte man schon dahin kommen, dass Sachen

einfach verständlich sind, ohne dass man erst mal ganz, ganz viel lernen muss.

Natürlich ist das bei mancher Software utopisch.

Also Adobe, Photoshop, weiß ich nicht, ob wir da irgendwann hinkommen, weil diese Software einfach so mächtig ist.

Weiß ich auch nicht, ob wir da hinkommen wollen.

Mit Sicherheit gibt's manche Sachen, die man nutzerfreundlicher machen kann.

Aber wenn ich jetzt irgendwie ein Passwort wo eingebe oder wenn ich mir einen Account mache, dann will ich, dass das intuitiv und einfach funktioniert.

Weil ich möchte, dass es sicher funktioniert.

Ich möchte, dass es schnell geht.

Ich möchte, dass es einfach ist.

Ja, mich interessiert nur das Ergebnis und nicht der Prozess.

Genau.

Ich möchte eben einen Account machen.

Ich möchte nicht erst mal noch lernen, wie Verschlüsselung funktioniert zum Beispiel.

Oder was man jetzt machen muss, damit man ein sicheres Passwort kriegt oder so.

Mhm.

Tipp drei.

Das sag ich meiner Mama auch immer.

Erst mal grundsätzlich Sachen ignorieren.

Zum Beispiel, wenn man E-Mails bekommt, die man nicht erwartet.

Wenn man einen Telefonanruf bekommt, den man nicht erwartet.

Erst mal kritisch sein.

Also erst mal kritisch drauf gucken, was ist es?

Habe ich wirklich einen neuen Sohn?

Genau.

Und da also lieber auf einem anderen Weg erst mal nachfragen, ob das wirklich so gemeint ist.

Also wirklich über einen anderen Kommunikationsweg mit der Person oder der Organisation in Kontakt treten und rausfinden, ob das wirklich so gemeint ist.

Vor allen Dingen, wenn es zeitkritische Sachen sind.

Nichts ist, also es gibt sehr wenige Sachen, die so zeitkritisch sind, dass man nicht nochmal irgendwo nachfragen kann.

Weil wir sind nicht die Rettungsstelle.

Was muss man denn machen, damit man ein sicheres Passwort bekommt?

Ein Passwortmanager nutzen. *lachen* Karolin Guthoff, vielen Dank.

Gerne.

Vielen Dank für die Einladung.

Musik *Musik* [Musik] [Abspann]