

Forum Strafverteidigung, 5. Dezember 2025 in Zürich

Das Handy im Strafverfahren: Technische Fragen

Rechtsanwalt Martin Steiger



**Smartphone: Was muss die
Verteidigung über technische
Fragen wissen?**

Wie können Polizei und Staatsanwaltschaft
unter Umständen gegen den Willen der
Inhaber:in auf Daten zugreifen, die auf
einem Smartphone gespeichert sind?

Eigentlich: Was alle wissen müssen!

Wichtig: Wenn Sicherheitsbehörden sich
Zugriff verschaffen können, gilt das
grundsätzlich auch für jede Täterschaft

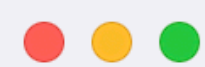


Smartphone: Ich habe viel zu verbergen,
nämlich mein gesamtes digitales Leben!

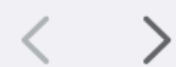
«[Smartphones sind] nicht bloss in der Lage, **enorme Mengen an [...] Daten** zu speichern (insbesondere in Applikationen aus den Bereichen Social Media, Gesundheit, Finanzen, Dating, usw.), sondern vereinen Telefon, Computer, Fotoapparat, Videokamera, Musikplayer, Wecker, Kalender, Agenda, Telefon- und Adressverzeichnis, Bezahlungssystem und vieles mehr in einem einzigen Gerät [...]. [Es] hat heute als notorisch zu gelten, dass privat genutzte Smartphones in der Regel eine **Vielzahl sensibler Daten** enthalten, welche die **höchstpersönliche Sphäre ihrer Inhaberin [...] tangieren** [...].»

Anders gefragt: Welcher Zugriff auf Nutzerdaten ist unabhängig von der Rechtslage auf welchem Weg möglich?

Berechtigte Annahme: Was technisch
möglich ist, wird auch gemacht



Private



als.wikipedia.org/wiki/Edward_Snowden



WIKIPEDIA
Di frei Enzyklopedy



[Finanzielli Hilf](#) [Nöis Benutzerkonto aalege](#) [Aamälde](#)



Edward Snowden

[90 Sproche](#)

[Artikel](#)

[Diskussion](#)

[Läse](#)

[Ändere](#)

[Quälltäxt bearbeite](#)

[Versionsgschicht](#)

[Wärchzügchäschtl](#)

Dr **Edward Joseph Snowden** (* [21. Juni 1983](#) z [Elizabeth City, North Carolina](#)) isch en [US-amerikanische](#) Whistleblower. Syni Enthillige hän Yyblick gee in s Uusmaß vu dr wältwyte Iberwachigs- un Spionagepraktike vu Ghaimdiensch, vor allem vu dr Verainigte Staate un vu Großbritannie. die hän im Summer 2013 di Global Iberwachigs- un Spionageaffäre uusglest.

Doderfir isch er meefach vu Nitregierigsorganisationen uuszaichnet un fir dr [Friidesnobelbryys](#) nominiert wore. Am 24. Septämber 2014 het er dr [Right Livelihood Award](#), vylmol *Alternative Nobelbryys* gnännt, iberchuu.^[1]

Dr Snowden isch en ehmolige Agänt, wu as tächnischi Fachchraft fir di US-amerikanische Ghaimdiensch [CIA](#), [NSA](#) un [DIA](#) gschaftt het.^[2] Bis Mai 2013 het er im Ufdrag vu dr NSA as Sischemadminischtrator fir s

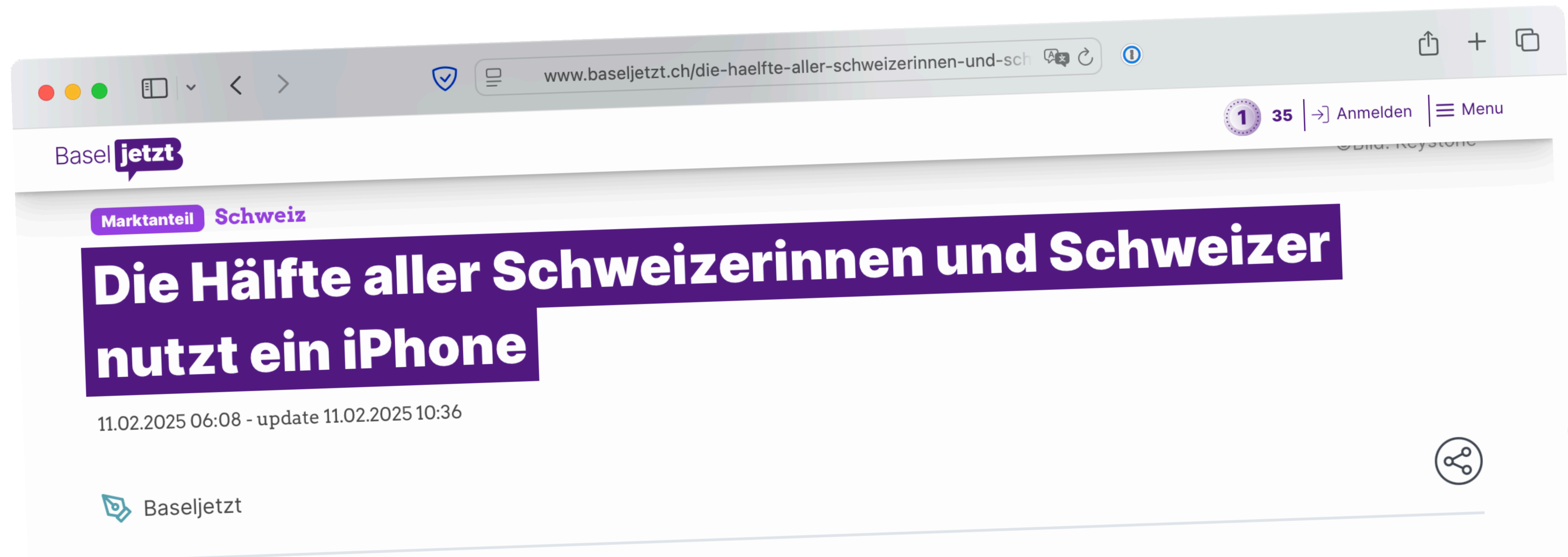


dr Edward Snowden
(2013)

Standard bei modernen Smartphones:

Hardware-basierte Verschlüsselung bietet
wirksamen Schutz vor physischem Zugriff

Beispiel: iPhone 15+ (2023) mit Betriebssystem iOS 18+ (2024+)

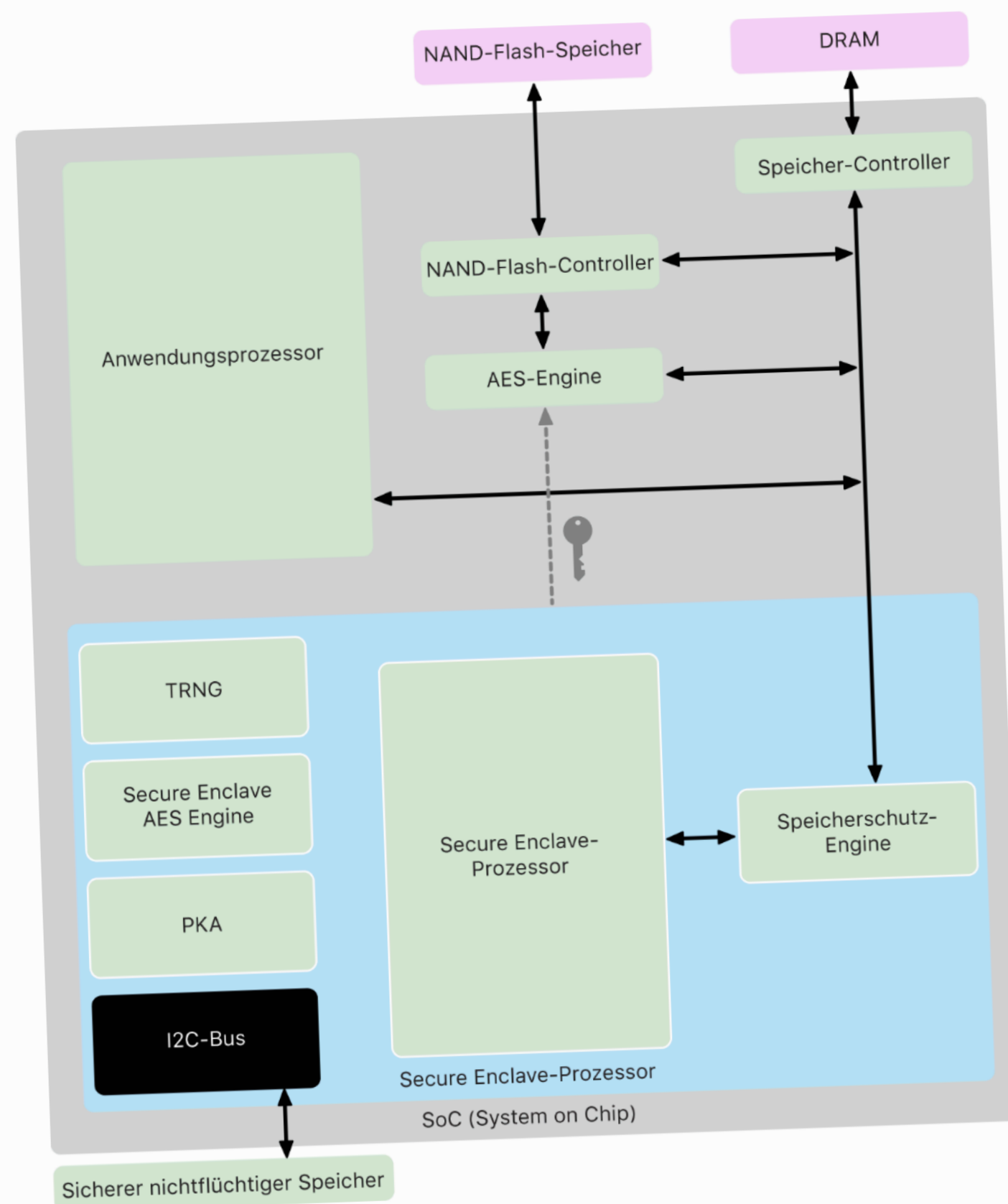


Secure Enclave

Die Secure Enclave ist ein dediziertes sicheres Subsystem in den aktuellen Versionen von iPhone, iPad, Mac, Apple TV, Apple Watch, Apple Vision Pro und HomePod.

Übersicht

Die Secure Enclave ist ein dediziertes sicheres Subsystem, das bei Apple in die [SoCs \(Systems on Chip\)](#) integriert ist. Die Secure Enclave ist vom Hauptprozessor isoliert, was eine zusätzliche Sicherheitsebene mit sich bringt, und ist darauf ausgelegt, die Sicherheit sensibler Benutzerdaten selbst dann zu gewährleisten, wenn der Kernel des Anwendungsprozessors kompromittiert werden sollte. Sie folgt denselben Designprinzipien wie das SoC insgesamt – ein Boot-ROM, das einen Hardware-Vertrauensanker etabliert, eine AES-Engine für effiziente und sichere kryptografische Operationen und geschützter Speicher. Die Secure Enclave umfasst keinen Speicher, verfügt aber über einen Mechanismus zum sicheren Speichern von Informationen auf dem angeschlossenen Speicher, der unabhängig von dem vom Anwendungsprozessor und dem Betriebssystem verwendeten NAND-Flashspeicher ist.

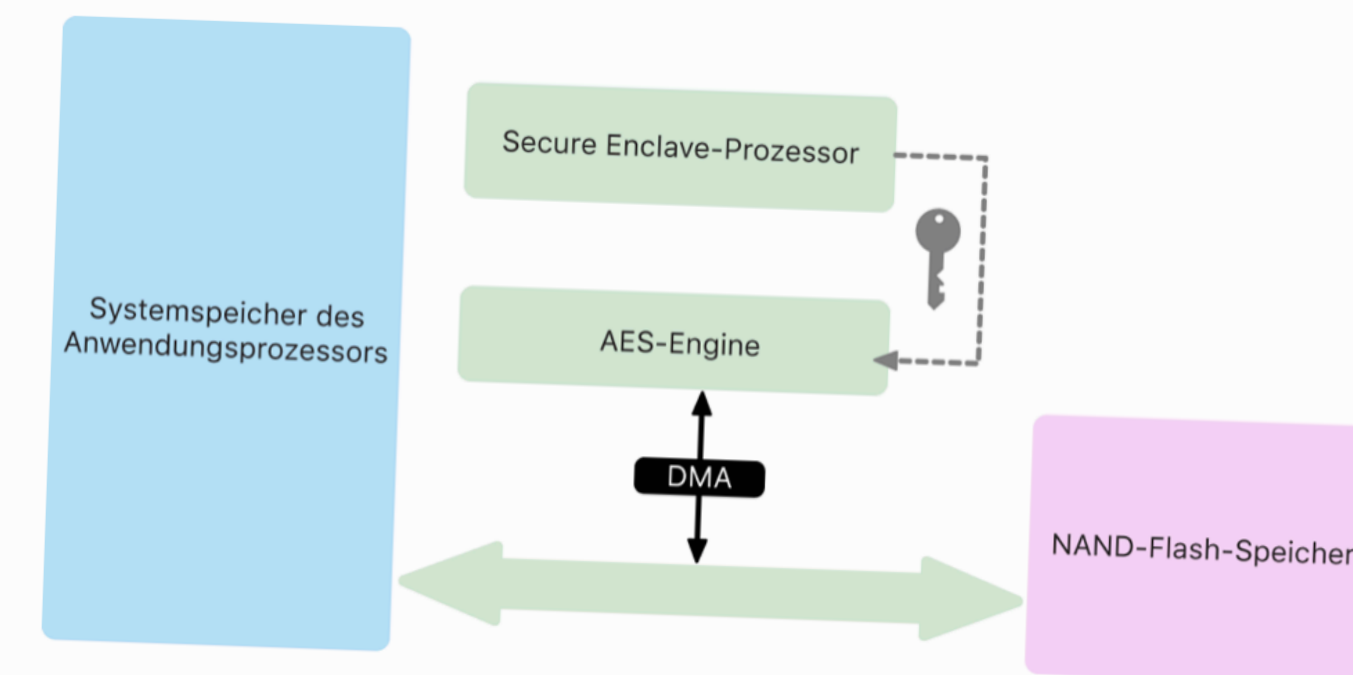


AES-Engine

Jedes Apple-Gerät mit einer Secure Enclave verfügt über eine dedizierte kryptografische AES-256-Engine (die „AES-Engine“), die sich im DMA-Pfad (Direct Memory Access) zwischen dem NAND (nicht flüchtigen) Flash-Speicher und dem Hauptspeicherspeicher befindet, was eine höchst effiziente Dateiverschlüsselung ermöglicht. Bei A9-Prozessoren oder Prozessoren einer neueren A-Reihe befindet sich das Subsystem des Flash-Speichers auf einem isolierten Bus, der nur über die DMA Crypto Engine auf den Speicher zugreifen kann, in dem die Benutzerdaten enthalten sind.

Beim Booten generiert das sepOS mithilfe von TRNG einen temporären Verpackungsschlüssel. Die Secure Enclave übermittelt diesen Schlüssel über dedizierte Drähte an die AES-Engine, sodass ein Zugriff durch irgendwelche Software außerhalb der Secure Enclave ausgeschlossen ist. Danach kann das sepOS den temporären Verpackungsschlüssel verwenden, um Dateischlüssel zu verpacken, die vom Dateisystemtreiber des Anwendungsprozessors verwendet werden. Wenn der Dateisystemtreiber eine Datei liest oder schreibt, sendet er den verpackten Schlüssel an die AES-Engine, die ihn entpackt. Die AES-Engine legt den unverpackten Schlüssel nie gegenüber Software offen.

Hinweis: Die AES-Engine ist eine Komponente, die sowohl von der Secure Enclave als auch der AES-Engine der Secure Enclave vollständig getrennt ist. Allerdings ist ihr Betrieb, wie im Folgenden beschrieben, eng mit der Secure Enclave verknüpft.

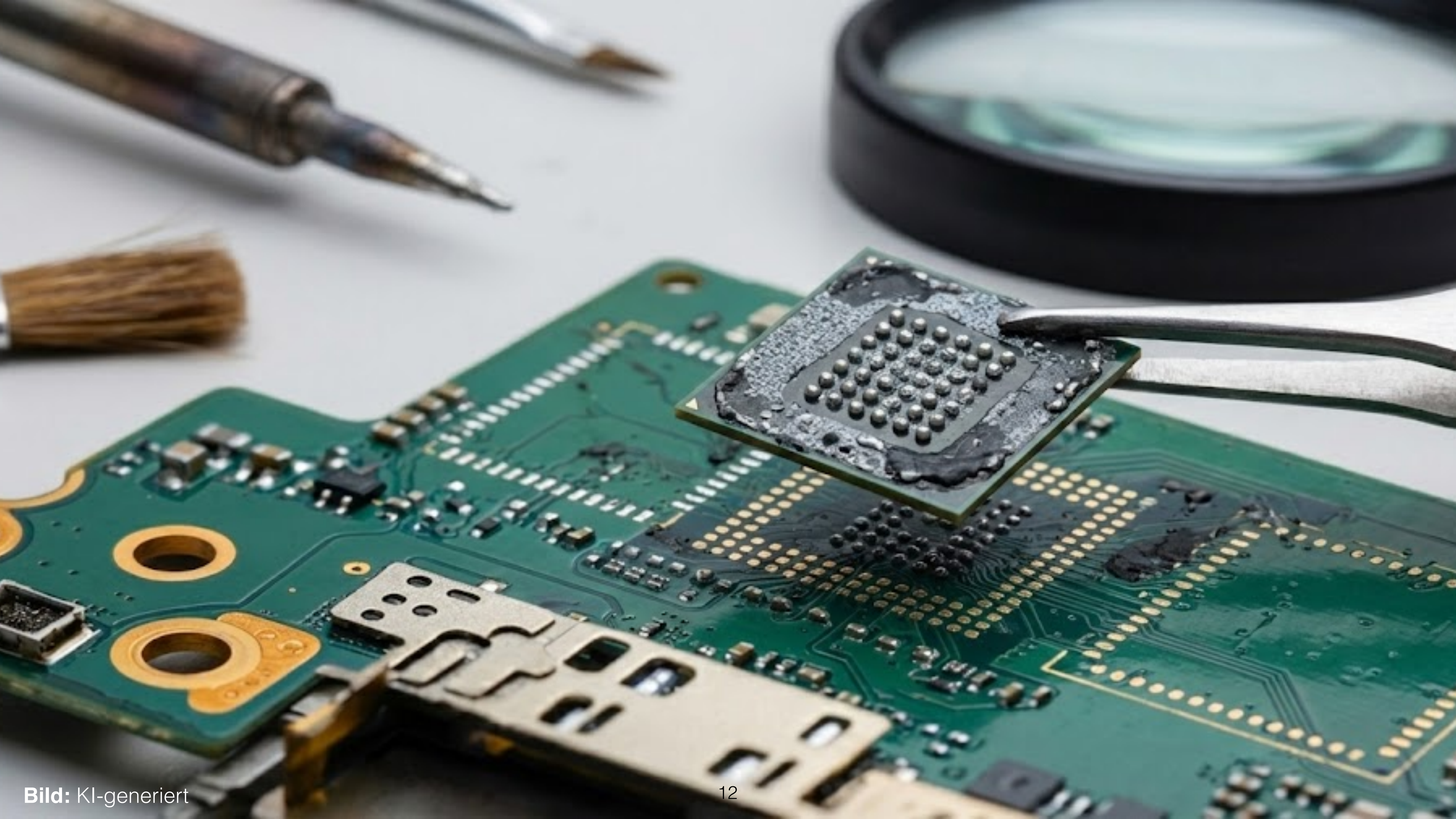


Public Key Accelerator

Der Public Key Accelerator (PKA) ist ein Hardwareblock, der für Operationen der asymmetrischen Kryptografie verwendet wird. Der PKA unterstützt Signier- und Verschlüsselungsalgorithmen auf Basis von RSA und ECC (Elliptic Curve Cryptography, Verschlüsselung mit elliptischen Kurven). Der PKA ist darauf ausgelegt, der Offenlegung von Informationen durch zeitliche Planung oder Seitenkanalattacken wie SPA oder DPA entgegenzuwirken.

Der PKA unterstützt Hardware- und Softwareschlüssel. Hardwareschlüssel werden aus der UID oder der GID der Secure Enclave hergeleitet. Diese Schlüssel verbleiben in der PKA- und sind nicht einmal für die sepOS-Software sichtbar.

Ergebnis: «Chip-off» ist nicht mehr
möglich oder sehr aufwendig



Schwachstelle: Wie entschlüsseln
Nutzer:innen ihre eigenen Daten, die
derart wirksam geschützt sind?

Hardware ID + Sperrcode = Schlüssel



Bild: KI-generiert

Erfreulich: Mit hoher Wahrscheinlichkeit
kein Zugriff auf Nutzerdaten
vor erster Entsperrung

«**Before First Unlock**» (**BFU**): Smartphone
(neu) gestartet, aber noch kein
Sperrcode eingegeben

Unerfreulich: Allenfalls möglicher Zugriff
auf Nutzerdaten nach erster Entsperrung

«**After First Unlock**» (**AFU**): Smartphone
ist eingeschaltet und der Sperrcode wurde
bereits eingegeben

«**Before First Unlock**»: Behörden
benötigen den Sperrcode für
Zugriff auf Schlüssel
und Nutzerdaten

«**Brute Force**»: Alle möglichen
Kombinationen durchprobieren



How escalating time delays discourage brute-force attacks

On iPhone, iPad, Mac, and Apple Vision Pro, to further discourage brute-force passcode attacks, there are escalating time delays after the entry of an invalid passcode, password, or PIN (depending on the device and the state the device is in), as shown in the table below.

Attempts	3	4	5	6	7	8	9	10 or more
iOS and iPadOS Lock Screen	None	1 minute	5 minutes	15 minutes	1 hour	3 hours	8 hours	Device is disabled and must connect to a Mac or PC
watchOS Lock Screen	None	1 minute	5 minutes	15 minutes	1 hour	3 hours	8 hours	Device is disabled and must connect to an iPhone
FileVault Login Window and Lock Screen	None	1 minute	5 minutes	15 minutes	1 hour	3 hours	8 hours	8 hours

Gegenmittel: «Rate Limit Bypass»

bzw. «Counter Reset» 

Bei erfolgreichem «Rate Limit Bypass» :

Schutz durch Sperrcode wird zu einem
ausschliesslichen Ratespiel

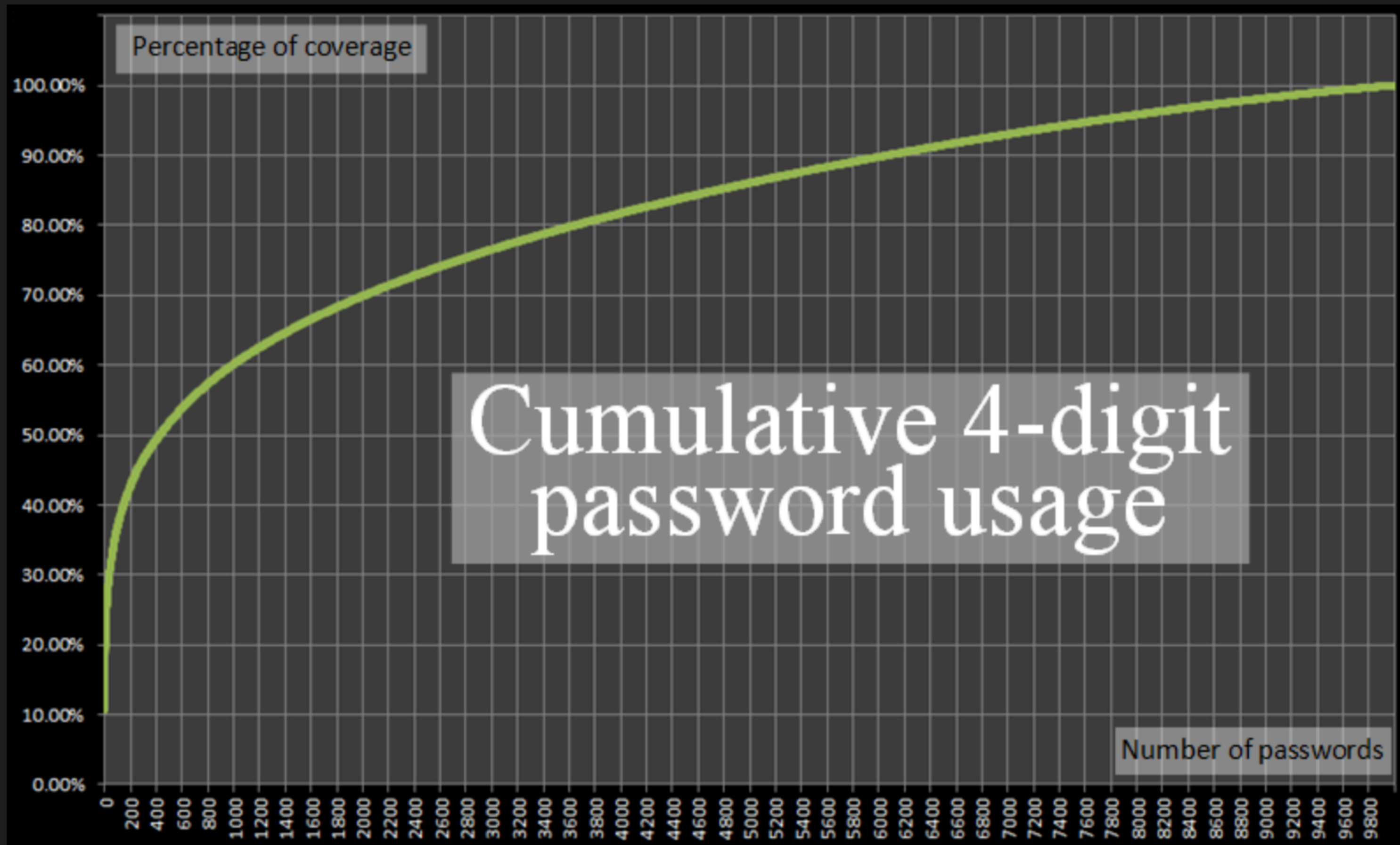
Deshalb: Je komplexer und vor allem
länger der Sperrcode, desto
besser der Schutz

Wie lange dauert allenfalls das Ratespiel?

- PIN mit 4 Ziffern: rund 7 Minuten
- PIN mit 6 Ziffern (Standard): rund 11 Stunden 🤨
- Passcode mit 5 Ziffern und 1 Buchstaben: rund 7 Tage
- Passcode mit 10 Ziffern und 2 Buchstaben: rund 85'000 Jahre
- Passcode mit 20 Ziffern und 4 Buchstaben: rund 57 Billionen Jahre

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	23 mins	48 mins
7	Instantly	Instantly	7 hours	24 hours	2 days
8	Instantly	1 hour	2 weeks	2 months	5 months
9	Instantly	2 days	2 years	10 years	31 years
10	Instantly	1 month	112 years	651 years	2k years
11	41 mins	3 years	5k years	40k years	153k years
12	7 hours	74 years	303k years	2m years	10m years
13	3 days	1k years	15m years	155m years	751m years
14	4 weeks	50k years	819m years	9bn years	52bn years
15	9 months	1m years	42bn years	596bn years	3tn years
16	8 years	33m years	2tn years	36tn years	257tn years
17	78 years	879m years	115tn years	2qd years	18qd years
18	776 years	22bn years	5qd years	142qd years	1qn years

Risiko «Mensch» : Verwendung
von gängigen Passcodes
wie «123456» oder «anwa1t»
(«Dictionary Attack»)



Statistically, *one third* of all codes can be guessed by trying just 61 distinct combinations!

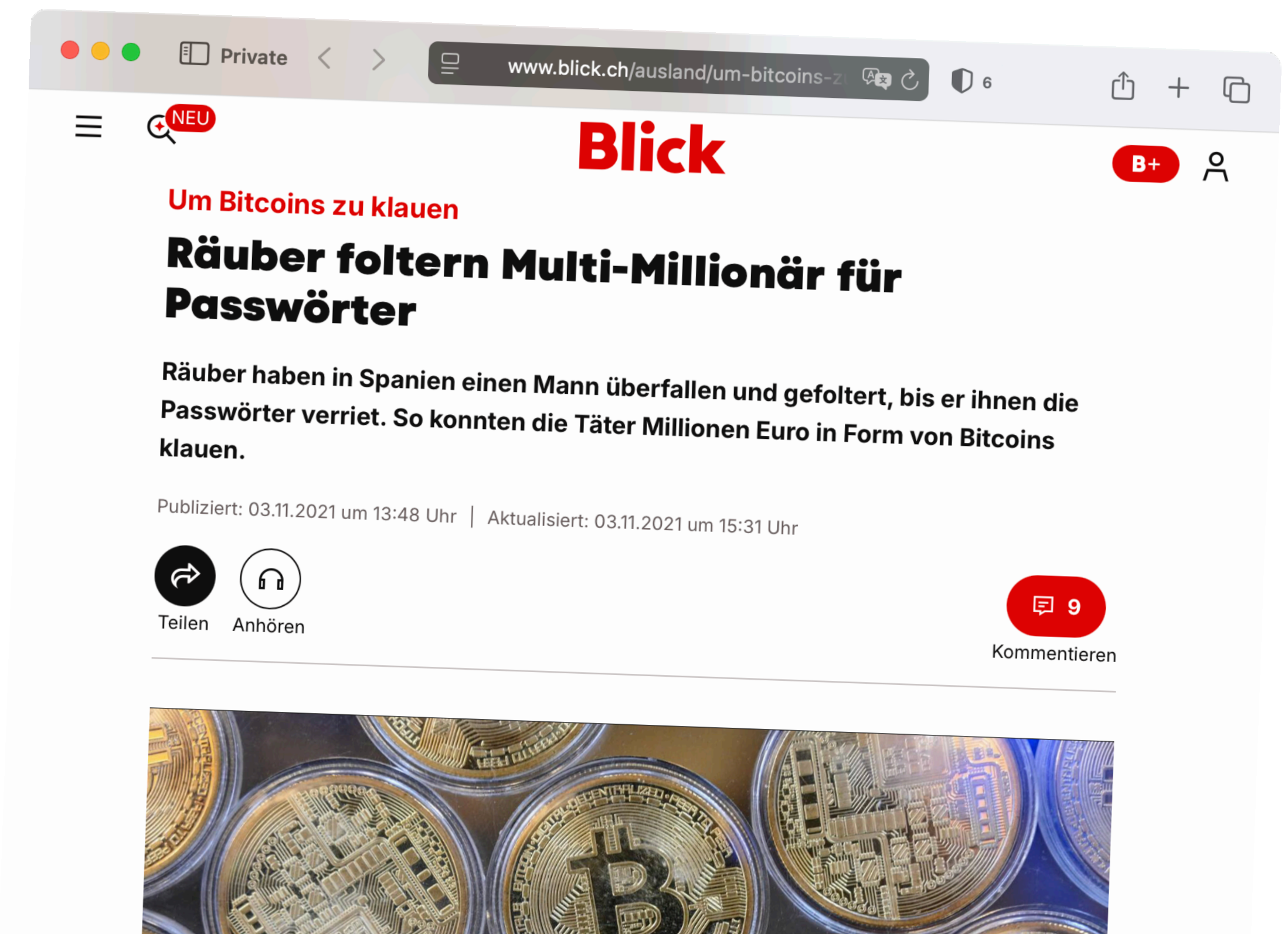
The 50% cumulative chance threshold is passed at just 426 codes (far less than the 5,000 that a random uniform distribution would predict). Paranoid yet?

Bottom of the pile

	PIN	Freq
#9980	8557	0.001191%
#9981	8557	0.001191%

BFU: Es geht allenfalls einfacher!

- Nutzer:in bei der Sperrcode-Eingabe beobachten, beispielsweise mit Videoüberwachung, auch nachträglich! 🔥
- Nutzer:in nett zureden 🚔
- Nutzer:in in Beugehaft setzen
- Nutzer:in foltern



«**After First Unlock**»: Auslesen von
Schlüsseln, die im Arbeitsspeicher liegen,
über «Zero Day»-Sicherheitslücken per
USB («Key Extraction» oder «Memory
Dump» mit «Kernel Exploit»)



Cellebrite

Warum Cellebrite

Der Weg zur Gerechtigkeit

Cellebrite versetzt Behörden in die Lage, ihre Ermittlungsabläufe zu modernisieren und die wachsende Lücke in der öffentlichen Sicherheit zu schließen, die durch die zunehmende digitale Raffinesse von Verbrechen und Beweismitteln entsteht.

Das Video ansehen

Der Schutz und Dienst für die Bürger ist schwieriger als je zuvor

Diese Trends verstärken sich...

POST-COVID-KRIMINALITÄT BOOM

~30%

Anstieg der Morde in CY2020

DIGITALE BEWEISE AN VORDERSTER FRONT

67%

der Straftaten haben jetzt eine wichtige digitale Komponente

MAGNET FORENSICS

MISE EN ROUTE

MAGNET GRAYKEY™

Beschleunigen Sie Ihre mobilen Ermittlungen

“Ohne GRAYKEY hätte ich meine Extraktionen nicht so schnell und so vollständig durchführen können. GRAYKEY arbeitet nicht nur schnell, sondern auch GUT! Ich kann mehr Daten in kürzerer Zeit erfassen als mit jeder anderen Extraktionsmethode.”

Jason Wilkins
Forensic Examiner
Clayton County Board of Commissioners

Magnet Graykey kann noch am selben Tag Zugriff auf die neuesten iOS- und Android-Geräte bieten, oft in weniger als einer Stunde.

NOCH HEUTE MIT EINEM EXPERTEN SPRECHEN

Schnellere mobile Forensik kann helfen, Leben zu retten

Magnet Graykey ist ein hochmodernes Forensik-Tool, das den rechtmäßigen Zugriff auf verschlüsselte Daten, und deren Extraktion, aus Mobilgeräten ermöglicht, um schneller mehr Fälle zu lösen.

MAGNET FORENSICS

FREE TRIAL

MAGNET AXIOM®

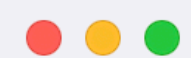
Wiederherstellung und Analyse von Beweisen in einem Fall

“Magnet AXIOM erweist sich als großartiges Tool zur effizienten Datenfilterung, wodurch die Zeit bis zur Beweissicherung erheblich verkürzt wird und den Ermittlern in besonderem Maße nützt.”

Chad Gish
CID/SISU Detective
Metropolitan Nashville Police Department

Prüfen Sie digitale Beweise aus Mobilgeräten, Clouds, Computern und Fahrzeugen sowie Extraktionen von Drittanbietern in einer einzigen Fallakte. Nutzen Sie leistungsstarke und intuitive Analysetools zur automatischen schnellen Auffindung sachdienlicher Beweise.

KOSTENLOS TESTEN



Expertise in eDiscovery und Digitale Forensik.

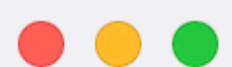
Ihr kompetenter Partner und Dienstleister für Digitale Forensik, Mobile Forensik, eDiscovery, Datenduplizierung, Netzwerkforensik und OSINT.

[Produkte ansehen](#)

Events

Nutzen Sie unsere Events für aktives Networking.





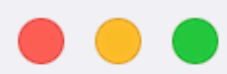
signal.org/blog/cellebrite-vulnerabilities/

[Get Signal](#)[Help](#)[Blog](#)[Developers](#)[Careers](#)[Donate](#)

The rite place at the Celleb...rite time

By a truly unbelievable coincidence, I was recently out for a walk when I saw a small package fall off a truck ahead of me. As I got closer, the dull enterprise typeface slowly came into focus: Cellebrite. Inside, we found the latest versions of the Cellebrite software, a hardware dongle designed to prevent piracy (tells you something about their customers I guess!), and a bizarrely large number of cable adapters.





signal.org/blog/cellebrite-vulnerabilities/

[Get Signal](#)[Help](#)[Blog](#)[Developers](#)[Careers](#)[Donate](#)

Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective

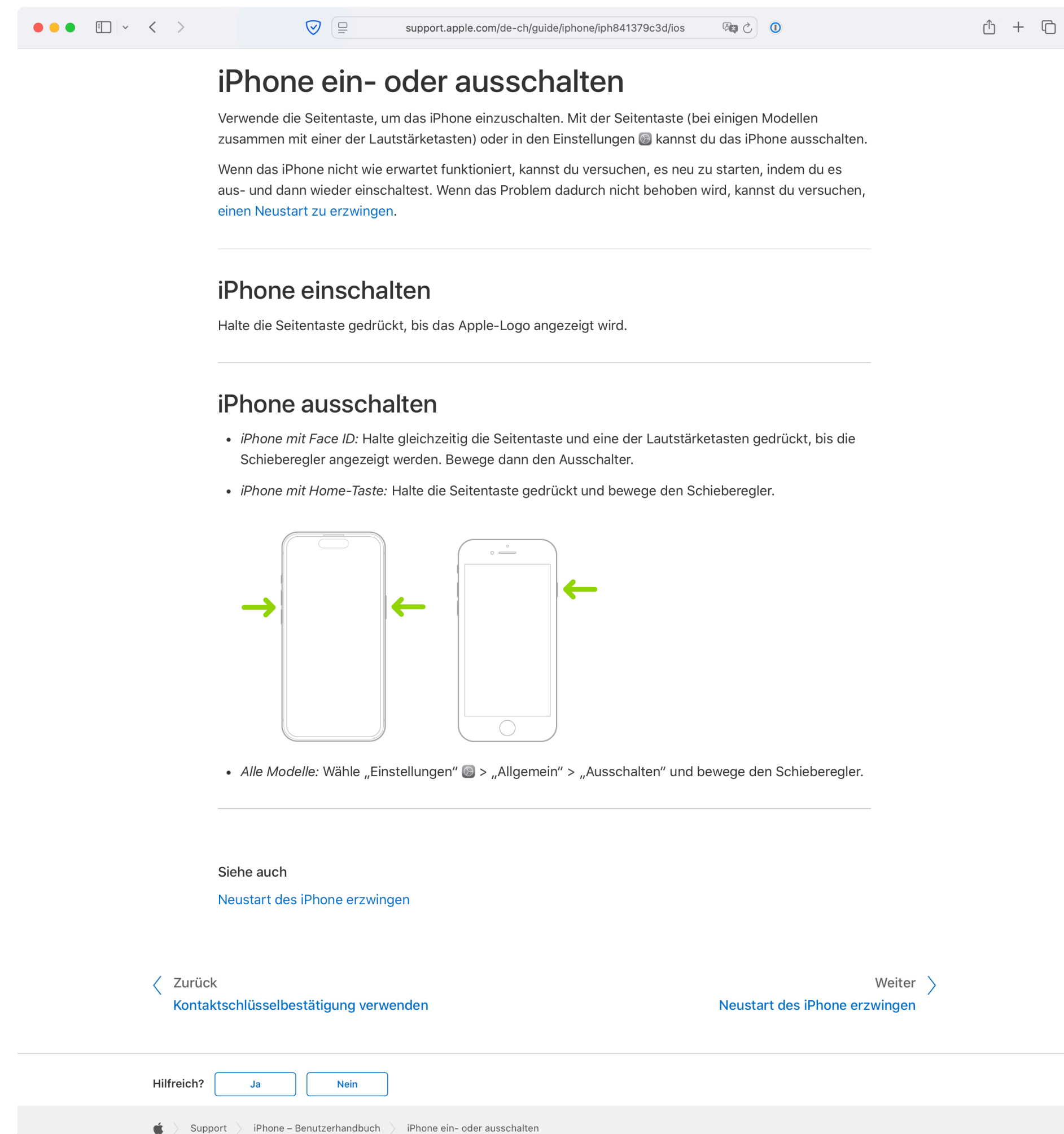
[moxie0](#) on 21 Apr 2021

Cellebrite makes software to automate physically extracting and indexing data from mobile devices. They exist within the grey – where enterprise branding joins together with the larcenous to be called “digital intelligence.” Their customer list has included authoritarian regimes in Belarus, Russia, Venezuela, and China; death squads in Bangladesh; military juntas in Myanmar; and those seeking to abuse and oppress in

AFU: Es geht allenfalls einfacher!

- Alle möglichen Kombinationen für den Sperrcode durchprobieren («Brute Force», wie bei BFU, allenfalls «Rate Limit Bypass» eher möglich)   
- Erzwungenes Entsperren mit Fingerabdruck (Touch ID) oder das Smartphone vor das Gesicht halten (FaceID) 
- Smartphone im Gebrauch aus der Hand reißen («Phone Snatching») 
- Smartphone mit einem «vertrauenswürdigen» Computer verbinden («Pairing Record Attack»)

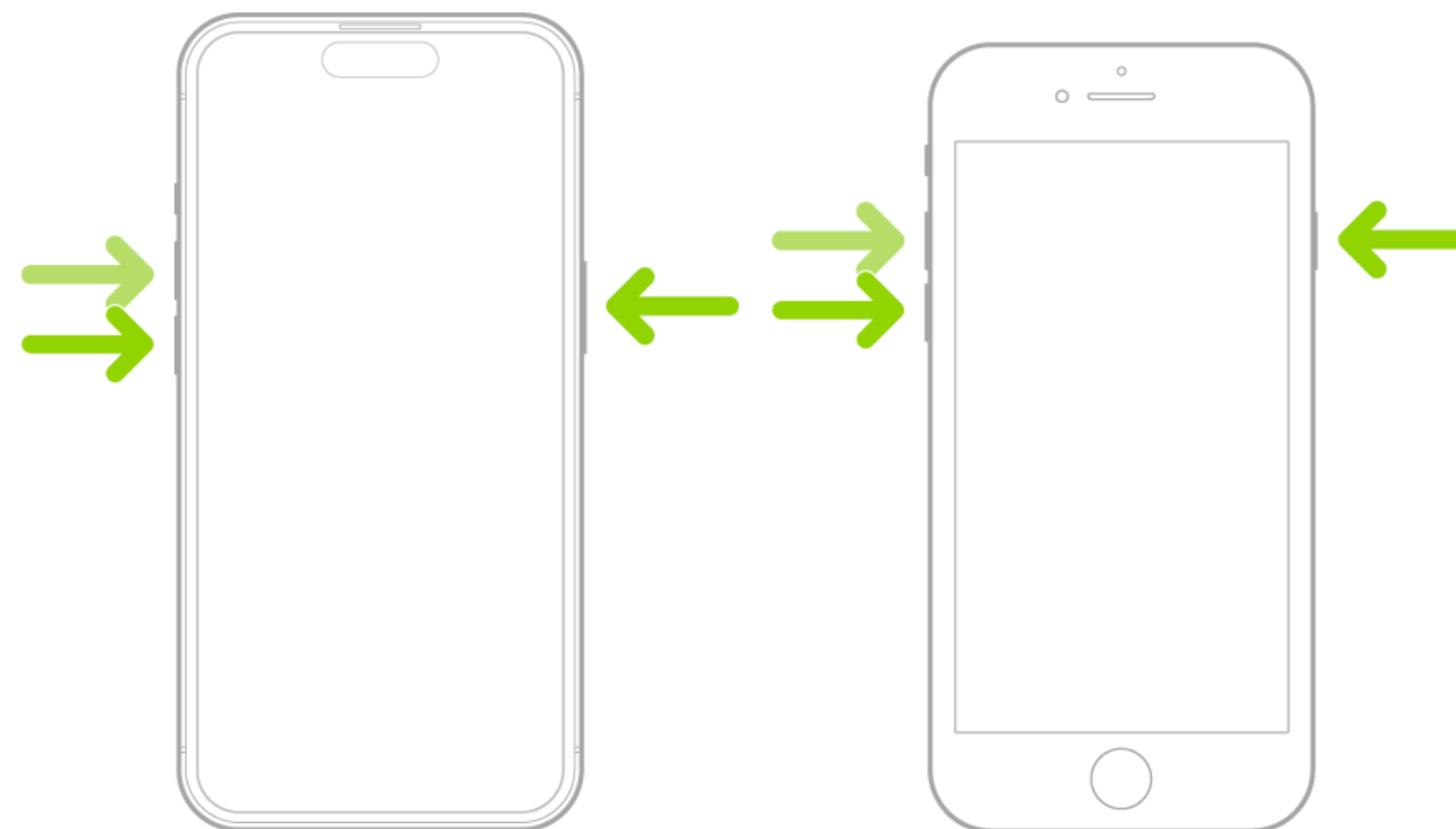
Gerät ausschalten oder neu starten



Neustart des iPhone erzwingen

Wenn dein iPhone nicht mehr reagiert und sich nicht [aus- und wieder einschalten lässt](#), kannst du versuchsweise einen Neustart zu erzwingen.

1. Drücke die Lautstärketaste „Lauter“ und lass sie schnell wieder los.
2. Drücke die Lautstärketaste „Leiser“ und lass sie schnell wieder los.
3. Drücke die Seitentaste und halte sie gedrückt.
4. Lass die Seitentaste los, wenn das Apple-Logo erscheint.



Wichtig: «Cop Button» deaktiviert Face ID und Touch ID, ist aber immer noch AFU



Mit Zugriff: Welche Nutzerdaten sind
für Behörden potenziell zugänglich?

Im Wesentlichen: Alle direkt sichtbaren
Nutzerdaten, nicht sichtbare Metadaten
und allenfalls gelöschte Daten 🔥

Mit wenig Aufwand: 95 % aller Daten

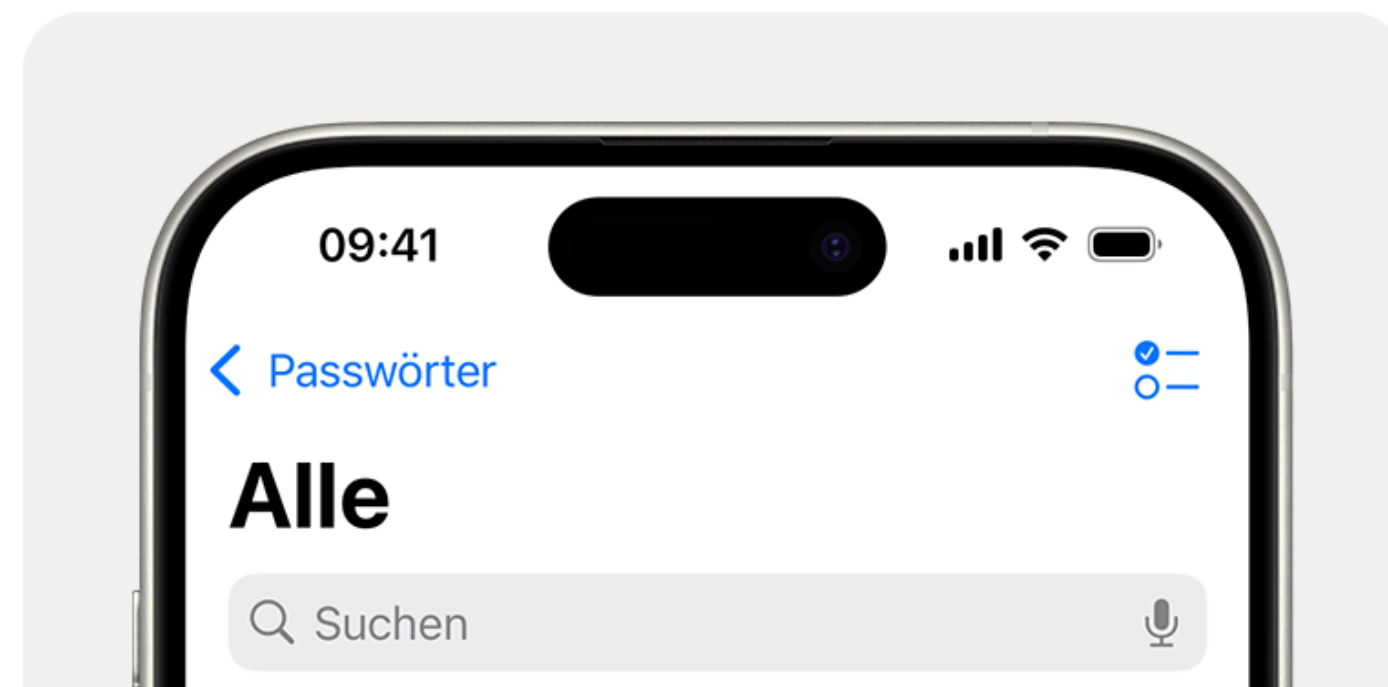
Gespeicherte Passwörter und Passkeys auf dem iPhone finden

Hier erfährst du, wie du deine gespeicherten Passwörter und Passkeys auf deinem iPhone oder iPad findest und bearbeitest.

Gespeicherte Passwörter und Passkeys unter „Passwörter“ anzeigen

Um die Passwörter-App zu verwenden, aktualisiere auf iOS 18.

1. Öffne die Passwörter-App.
2. Entsperre das Gerät mit Face ID oder Touch ID, oder gib deinen Code ein.



NSFileProtectionComplete: Der Klassenschlüssel wird mit einem Schlüssel geschützt, der aus dem Code oder Passwort des Benutzers und der UID des Geräts abgeleitet wird. Kurz nachdem Benutzer:innen ein Gerät sperren (10 Sekunden, wenn die Einstellung „Passwort erforderlich“ auf „Sofort“ festgelegt ist), wird der entschlüsselte Klassenschlüssel verworfen, damit auf alle Daten in dieser Klasse erst wieder

Ausserdem: Zugriff auf Nutzerdaten bei
(fast) allen verwendeten Cloud-Diensten,
allein schon über Smartphone-Apps

WhatsApp: Was «sieht» Forensik-Software?

- Alle direkt sichtbaren Nutzerdaten (Mitteilungen, Bilder, ...)
- Als gelöscht markierte, aber noch nicht überschriebene Inhalte in der SQLite-Datenbank («Freelist Carving»)
- Daten und Befehle, die vorläufig im «Write Ahead Log» (WAL) gespeichert werden, beispielsweise Löschbefehle für Daten
- Metadaten, beispielsweise wann Mitteilungen empfangen, gelesen oder gelöscht wurden
- Vorschaubilder («Thumbnails») von gelöschten Bildern und Videos

Blick auf Android: Heterogene Geräte-
und System-Landschaft, tendenziell
weniger sicher als modernes iPhone

[+ POLICY](#) [+ NEWS](#) [+ TECH](#)

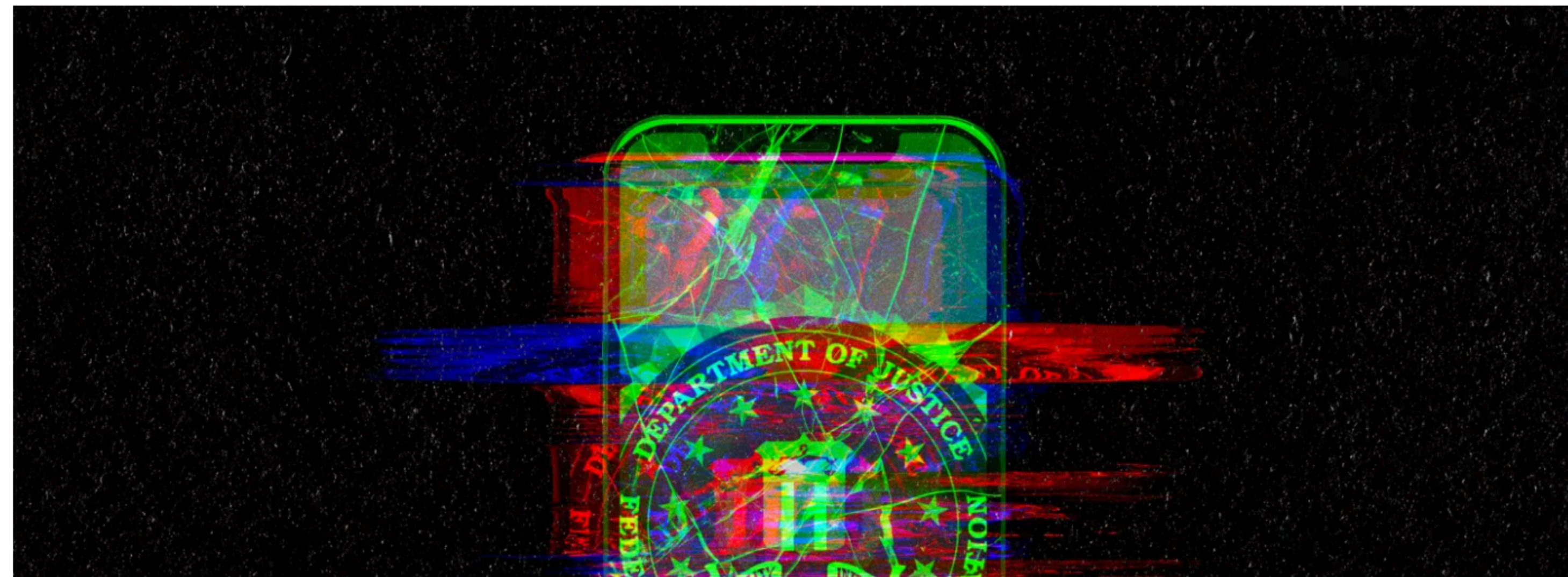
The FBI got into the Trump rally shooter's phone in just 40 minutes

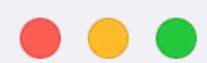
/ The bureau reportedly used an unreleased Cellebrite tool to open the phone.

by [+ Gaby Del Valle](#)

Jul 19, 2024 at 5:53 PM GMT+2

[Link](#) [Share](#) | [14 Comments \(All New\)](#)





Private



Reader Available



GrapheneOS

Features

Install

Build

Usage

FAQ

Releases

Source

History

Articles

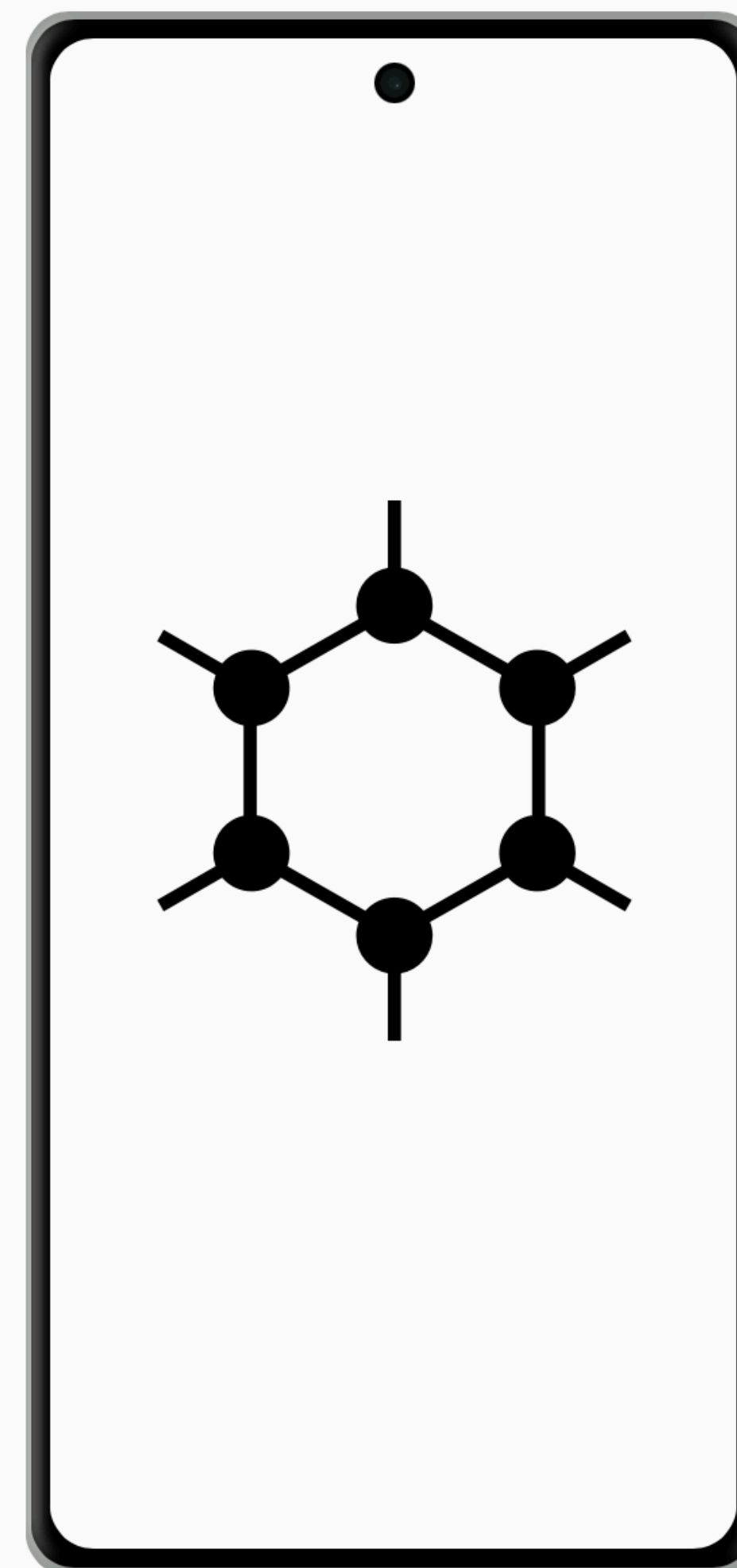
Donate

Contact

GrapheneOS

The private and secure mobile operating system with Android app compatibility. Developed as a non-profit open source project.

[Install GrapheneOS](#)



BFU > AFU, aber: Bei **1** aktuellen und gehärteten Betriebssystemen wie iOS oder GrapheneOS, mit **2** moderner Hardware und **3** einem langen Passcode bleibt der Zugriff anspruchsvoll



www.404media.co/leaked-docs-show-what-phones-cel



404

SIGN IN

SUBSCRIBE

Leaked Docs Show What Phones Cellebrite Can (and Can't) Unlock



JOSEPH COX · JUL 17, 2024 AT 1:31 PM

The leaked April 2024 documents, obtained and verified by 404 Media, show Cellebrite could not unlock a large chunk of modern iPhones.





www.404media.co/leaked-documents-show-what-phone



~~404~~

SIGN IN

SUBSCRIBE

Leaked Documents Show What Phones Secretive Tech 'Graykey' Can Unlock



JOSEPH COX · NOV 19, 2024 AT 9:06 AM

The documents provide never-been-seen insight into the current cat-and-mouse game between forensics companies and phone manufacturers Apple and Google.



Table 1: iPhones Support Matrix 7.69.1 Locked

Newly added

iPhone	SoC	≤11	12.0-12.5.x	13.1-13.7.x	14.0-14.8.x	15-15.8.x	16.0-16.7.x	17.0 - 17.0.3	17.1-17.3.1	17.4 - Newer
iPhone 5 iPhone 5C iPhone 5S iPhone 6 iPhone 6+	A6 A7 A8	BF	BF	N/A	N/A	N/A	N/A	N/A	N/A	N/A
iPhone 6S iPhone 6S+ iPhone SE gen 1 iPhone 7 iPhone 7+	A9 A10	BF	Supersonic BF	Supersonic BF	Supersonic BF	Supersonic BF	N/A	N/A	N/A	N/A
iPhone 8 iPhone 8+ iPhone X	A11	BF	Supersonic BF	Supersonic BF	Supersonic BF	Supersonic BF	AFU + IPR + Supersonic BF (1)(6)	N/A	N/A	N/A
iPhone XR iPhone XS max iPhone XS	A12	N/A	BF	Supersonic BF	Supersonic BF	Supersonic BF	AFU + IPR + Supersonic BF (1)	AFU + IPR + Supersonic B F (1)(4)	Supersonic BF (1)(4)	In Research
iPhone 11 iPhone 11 pro iPhone 11 pro max iPhone SE gen 2	A13	N/A	N/A	Supersonic BF	Supersonic BF	Supersonic BF	AFU + IPR + Supersonic BF (1)	AFU + IPR + Supersonic B F (1)(4)	Supersonic BF (1)(4)	In Research
iPhone 12 iPhone 12 pro iPhone 12 pro max iPhone 12 mini	A14	N/A	N/A	N/A	N/A	AFU + IPR	AFU + IPR	AFU + IPR	Coming soon	In Research
iPhone 13 iPhone 13 pro iPhone 13 pro max iPhone 13 mini iPhone SE gen 3	A15	N/A	N/A	N/A	N/A	AFU + IPR	AFU + IPR	AFU + IPR	Coming soon	In Research
iPhone 14 iPhone 14 Plus iPhone 14 pro iPhone 14 pro max	A16 A15	N/A	N/A	N/A	N/A	N/A	AFU + IPR	AFU + IPR	Coming soon	In Research
iPhone 15 iPhone 15 Pro iPhone Pro Max	A16 A17	N/A	N/A	N/A	N/A	N/A	N/A	In Research	In Research	In Research

Quelle: Cellebrite

Table 2: Android OS Access Support Matrix – Locked devices 7.69.1

Vendor (Chipset)		Section 1: COLD - turned off (Secure startup or FBE)		Section 2: HOT (AFU or FDE without secure startup)		Comments and exceptions
		BFU extractions (for FBE devices)	Brute-Force Password to get the user data (CE) decrypted	All Extractions (Even without BF)	Brute-Force password (not needed for extraction)	
Samsung (Exynos / MTK / Qualcomm)	Android 6					
	Android 7-14					Added BF support for QC S24, S24+, S24 Ultra
Huawei (Kirin / Qualcomm / MTK)						P40 family is supported for Brute-force only up to ~04-2021 SPL
Pixel	Pixel, Pixel XL					
	Pixel 3 - 5					Added AFU support for Android 14 Official and Pixel 8.
	Pixel 6 - 8					BF support for Pixel 3-5 extended to latest SPLs
Non-Samsung Qualcomm including Huawei, LG, Motorola, Xiaomi, Sony, OnePlus and many more						Added AFU, BFU & BF support for Snapdragon 8 Gen 3, 8 Gen 2, 6 Gen 1, 7+ Gen 2, 7s Gen 2, 4 Gen 2.



Fully Supported



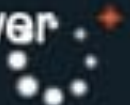
Partially Supported



Not Supported

Huawei Kirin temporarily disabled.

For Non-Samsung/Pixel, Qualcomm FBE devices, there may be a requirement for 24hr uptime of the device prior attempting to brute force the device. Affected chipsets: SM4350, SM6150 SM7150, SM8150 and newer



Anspruchsvoller physischer Zugriff auf das Smartphone:

Wo liegen die Daten denn sonst noch?

PRODUCT & PACKAGE SIZE



Bild: Pantasy / Retro 90s PC 85005 (aus Klemmbausteinen)

Manchmal: Daten liegen ganz oder teilweise auf Desktop-Computern und Notebooks der Nutzer:innen – und sind dort nicht wirksam geschützt

Einige Gründe:

- Keine standardmässige vollständige Systemverschlüsselung
- Häufig rund um die Uhr in Betrieb
- Einfach vor Ort in der Schweiz zugänglich 🔥





support.apple.com/de-ch/108353

Store

Mac

iPad

iPhone

Watch

AirPods

TV & Home

Entertainment

Zubehör

Support

Informationen zu verschlüsselten Backups auf dem iPhone, iPad oder iPod touch

Du kannst Backups des iPhone, iPad oder iPod touch auf deinem Computer mithilfe des Passwortschutzes und der Verschlüsselung schützen.

[Backups verschlüsseln](#) ⌵

[Überprüfen, ob deine Backups verschlüsselt sind](#) ⌵

[Verschlüsselung von Backups deaktivieren](#) ⌵

[Passwort des verschlüsselten Backups zurücksetzen](#) ⌵

Dein iPhone-, iPad- oder iPod touch-Backup verschlüsseln

Mit der Option „Lokales Backup verschlüsseln“ im Finder, in der App [Apple-Geräte](#) oder in [iTunes](#) kannst du deine Daten sperren und verschlüsseln. Verschlüsselte Backups können Daten enthalten, die in unverschlüsselten Backups nicht enthalten sind:

There is NO CLOUD, just



other people's computers

Fast immer: Nutzerdaten liegen ganz oder teilweise auf fremden Computern – und sind dort nicht wirksam geschützt

Grundsatz: Cloud-Dienste können auf alle Nutzerdaten zugreifen – und damit auch Sicherheitsbehörden

Ausnahme: Nutzerdaten sind geschützt durch Ende-zu-Ende-Verschlüsselung

Datenreichtum: Backup, E-Mail und Fotos

support.apple.com/de-ch/102651				
Standardmäßiger Datenschutz			Erweiterter Datenschutz	
Datenkategorie	Verschlüsselung	Speicherung von Schlüsseln	Verschlüsselung	Speicherung von Schlüsseln
iCloud Mail (1)	Bei der Übertragung und auf dem Server	Apple	Bei der Übertragung und auf dem Server	Apple
Kontakte (2)	Bei der Übertragung und auf dem Server	Apple	Bei der Übertragung und auf dem Server	Apple
Kalender (2)	Bei der Übertragung und auf dem Server	Apple	Bei der Übertragung und auf dem Server	Apple
iCloud-Backup (umfasst Geräte- und Nachrichten-Backup) (3)	Bei der Übertragung und auf dem Server	Apple	Ende-zu-Ende	Vertrauenswürdig Geräte
iCloud Drive (4)	Bei der Übertragung und auf dem Server	Apple	Ende-zu-Ende	Vertrauenswürdig Geräte



support.apple.com/de-ch/108756



Store

Mac

iPad

iPhone

Watch

AirPods

TV & Home

Entertainment

Zubehör

Support

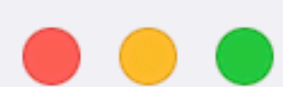


So aktivierst du den erweiterten Datenschutz für iCloud

Der erweiterte Datenschutz für iCloud bietet das höchste Maß an Datensicherheit in der Cloud und schützt den Großteil deiner iCloud-Daten mithilfe von Ende-zu-Ende-Verschlüsselung.

Informationen zum erweiterten Datenschutz für iCloud

Der erweiterte Datenschutz für iCloud ist eine optionale Einstellung, die das höchste Maß an Datensicherheit in der Cloud bietet. Wenn du den erweiterten Datenschutz aktivierst, wird der Großteil deiner iCloud-Daten – einschließlich iCloud-Backup, Fotos, Notizen und mehr – durch Ende-zu-Ende-Verschlüsselung geschützt. Keine andere Person kann auf deine Ende-zu-Ende verschlüsselten Daten zugreifen – nicht einmal Apple – und diese Daten bleiben selbst im Falle eines Datenmissbrauchs in der Cloud sicher. Bevor du den erweiterten Datenschutz aktivierst, kannst du mehr darüber erfahren, [wie deine Daten geschützt werden](#), wenn der standardmäßige Datenschutz verwendet und der erweiterte Datenschutz aktiviert wird.



support.apple.com/en-us/122234



Store

Mac

iPad

iPhone

Watch

Vision

AirPods

TV & Home

Entertainment

Accessories

Support



Apple can no longer offer Advanced Data Protection in the United Kingdom to new users

Here's what it means.

We are deeply disappointed that our customers in the UK will no longer have the option to enable Advanced Data Protection (ADP), especially given the continuing rise of data breaches and other threats to customer privacy. Apple remains committed to offering our users the highest level of security for their personal data and we are hopeful that we will be able to do so in the future in the United Kingdom.

[As we have said many times before](#), we have never built a backdoor or master key to any of our products or services and we never will.

- Withdrawing [Advanced Data Protection](#) from the UK will not affect the [15 iCloud data categories](#) that are end-to-end encrypted by default. Data like iCloud Keychain and

- Das Betriebssystem ist Android 9 oder höher.
- Das Paket „Google Mobile-Dienste“ (Version 241217000 oder höher) ist installiert.
- Auf deinem Gerät muss eine Displaysperre eingerichtet sein, z. B. eine PIN, ein Passwort

TECHNOLOGY

Arrested Man Learns ChatGPT Isn't His Lawyer So Much As It's Evidence

Astounding moron allegedly types out his whole crime so he can ask ChatGPT about it.

By Joe Patrice on October 03, 2025 1:05 pm



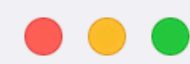
Police just added a new weapon to their arsenal: incredibly stupid people being way too comfortable confessing their secrets to the robot in their pocket.

When tech bro evangelists sell the world on the productivity accelerating power of the technological terrors they've



Abgesehen davon: Remote-Zugriff auf
Nutzerdaten auf Smartphones

Staatstrojaner: Neusprech «GovWare»

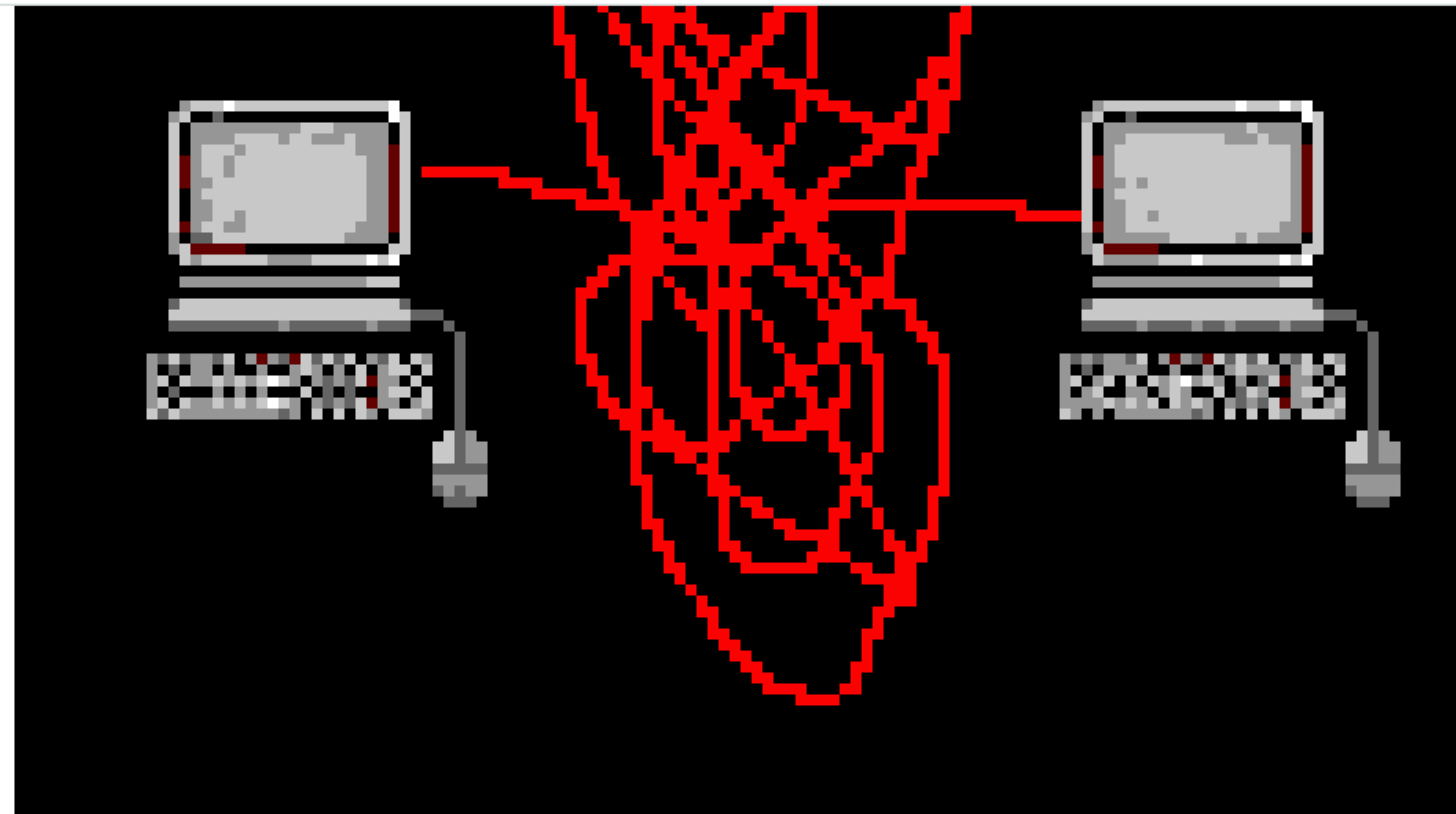


Anmelden

REPUBLIK



Folge 3: Surveillance fédérale ▾



Der Staat als Hacker

Die Bundesverwaltung lädt aus einer «Hackerzentrale» Staats-trojaner auf Handys von Verdächtigen. Die Kollateralschäden für die Cybersicherheit sind enorm. Die Serie zum Schweizer Überwachungsstaat, 3. und letzte Folge.

Von [Adrienne Fichter](#) (Text) und Erik Carter (Illustration), 18.01.2024



Teilen



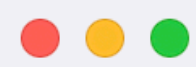
47 Beiträge

Funktionsweise: Schadsoftware zum
Zugriff auf Nutzerdaten wird über
gezielte Angriffe eingespielt

Gängige Varianten: Remote, zum Beispiel
per Browser oder Messaging-App, häufig
«Zero Click», oder vor Ort («Bad USB») 🔥

**Aufwendig für die Behörden – und
schädlich für die Allgemeinheit:**

Sicherheitslücken werden nicht behoben,
sondern aufgekauft und missbraucht



For our customers' protection, Apple doesn't disclose, discuss, or confirm security issues until an investigation has occurred and patches or releases are available. Recent releases are listed on the [Apple security releases](#) page.

Apple security documents reference vulnerabilities by [CVE-ID](#) when possible.

For more information about security, see the [Apple Product Security](#) page.

iOS 18.6.2 and iPadOS 18.6.2

Released August 20, 2025

ImageIO

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

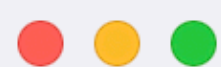
Impact: Processing a malicious image file may result in memory corruption. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals.

Description: An out-of-bounds write issue was addressed with improved bounds checking.

CVE-2025-43300: Apple

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. [Contact the vendor](#) for additional information.

Published Date: August 20, 2025



unit42.paloaltonetworks.com/landfall-is-new-commercial



Threat Research Center > Threat Research > Vulnerabilities

English ▾

VULNERABILITIES

LANDFALL: New Commercial-Grade Android Spyware in Exploit Chain Targeting Samsung Devices

🕒 21 min read

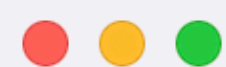
RELATED PRODUCTS



Advanced DNS Security



Advanced Threat Prevention



www.theregister.com/2025/11/07/landfall_spyware_samsu



SIGN IN / UP

The Register®



RESEARCH

Previously unknown Landfall spyware used in 0-day attacks on Samsung phones

8

'Precision espionage campaign' began months before the flaw was fixed

[Jessica Lyons](#)

Fri 7 Nov 2025 // 21:38 UTC



A previously unknown Android spyware family called LANDFALL exploited a zero-day in Samsung Galaxy devices for nearly a year, installing surveillance code capable of recording calls, tracking locations, and harvesting photos and logs before Samsung finally patched it in April.

The surveillance campaign likely began in July 2024 and abused [CVE-2025-21042](#), a critical bug in Samsung's image-processing library that affects Galaxy devices running Android versions 13, 14, 15, and 16, according to Palo Alto Networks Unit 42 researchers who discovered the commercial-grade spyware and [revealed details](#) of the espionage attacks in a Friday report.

"This was a precision espionage campaign, targeting specific Samsung Galaxy devices in the Middle East, with likely victims in Iraq, Iran, Turkey, and Morocco," Itay Cohen, a senior principal researcher at Unit 42, told *The Register*. "The use of zero-day exploits, custom infrastructure, and modular payload design all indicate an espionage-motivated operation."

<

2025

>

April

May

June

July

August

September

October

November

December

Disclaimer

- Please note that in some cases regular OS upgrades may cause delays to planned security updates. However, users can be rest assured the OS upgrades will include up-to-date security patches when delivered.
- While we are doing our best to deliver the security patches, the timing of the security patches may vary depending on the regions and models.
- Some patches to be received from chipset vendors (also known as OEM patches) may not be included in the update package of the month. They will be included in the next update package.

Acknowledgements

Dawuge: SVE-2025-0383, SVE-2024-1685
Sam of Honor Cyber Security Lab: SVE-2024-1695, SVE-2024-1920, SVE-2025-0276
Vincenzo Bonforte - @Bonfee1: SVE-2024-1795
WatchOut: SVE-2024-2341
localh0ster: SVE-2024-2368, SVE-2025-0037, SVE-2025-0255
Yuhui Cheng: SVE-2024-2403
Stealth Assassin: SVE-2024-2445
HBh25Y of shuffle team: SVE-2024-2455, SVE-2024-2456
Natalie Silvanovich: SVE-2025-0030

SMR-DEC-2025

SMR-NOV-2025

SMR-OCT-2025

Samsung Mobile Security and Cookies

Our site uses essential cookies only. You can read our [Privacy Policy](#) and [Cookie Policy](#).

Improper access control in Mdecservice prior to SMR Apr-2025 Release 1 allows local attackers to access arbitrary files with system privilege. The patch adds proper input validation.

Security UpdatesSecurity ReportingRewards ProgramSecurity Post

SVE-2024-1969(CVE-2025-21042): Out-of-bounds write in libimagecodec.quram.so

Severity: Critical
Affected versions: Android 13, 14, 15
Reported on: September 25, 2024
Disclosure status: Privately disclosed
Out-of-bounds write in libimagecodec.quram.so prior to SMR Apr-2025 Release 1 allows remote attackers to execute arbitrary code. The patch adds proper input validation.

Some SVE items included in the Samsung Android Security Update cannot be disclosed at this time.

Acknowledgements

Dawuge: SVE-2025-0383, SVE-2024-1685
Sam of Honor Cyber Security Lab: SVE-2024-1695, SVE-2024-1920, SVE-2025-0276
Vincenzo Bonforte - @Bonfee1: SVE-2024-1795
WatchOut: SVE-2024-2341
localh0ster: SVE-2024-2368, SVE-2025-0037, SVE-2025-0255
Yuhui Cheng: SVE-2024-2403
Stealth Assassin: SVE-2024-2445
HBh25Y of shuffle team: SVE-2024-2455, SVE-2024-2456
Natalie Silvanovich: SVE-2025-0030

Schweiz: 12 GovWare-Einsätze (2024)

Überwachungen;Besondere_technische_Geräte_IMSI_Catcher;1;Ja;BetmG: Artikel 19 Absatz 2 sowie 20 Absatz 2
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;StGB Art. 260ter Kriminelle Organisation
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;BetmG: Artikel 19 Absatz 2 sowie 20 Absatz 2
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;StGB Art. 260ter Kriminelle Organisation
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;BetmG: Artikel 19 Absatz 2 sowie 20 Absatz 2
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;BetmG: Artikel 19 Absatz 2 sowie 20 Absatz 2
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;BetmG: Artikel 19 Absatz 2 sowie 20 Absatz 2
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;BetmG: Artikel 19 Absatz 2 sowie 20 Absatz 2
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;StGB Art. 260ter Kriminelle Organisation
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;BetmG: Artikel 19 Absatz 2 sowie 20 Absatz 2
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;BetmG: Artikel 19 Absatz 2 sowie 20 Absatz 2
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;BetmG: Artikel 19 Absatz 2 sowie 20 Absatz 2
Überwachungen;Besondere_Informatikprogramme_GovWare;1;Ja;BetmG: Artikel 19 Absatz 2 sowie 20 Absatz 2

Auf den Punkt gebracht: Was muss die
Verteidigung über technische Fragen
beim Smartphone wissen?

Hohe Wahrscheinlichkeit für Zugriff auf Daten:

- Kein modernes Smartphone mit gehärtetem Betriebssystem
- PIN statt komplexer und vor allem langer Sperrcode

Erhöhte Wahrscheinlichkeit:

- Smartphone bereits in Gebrauch («After First Unlock»)
- Daten auf Datenträgern und Computern der Nutzer:innen in der Schweiz ohne wirksamen Schutz
- Daten ohne Ende-zu-Ende-Verschlüsselung bei Cloud-Diensten, insbesondere Backup, E-Mail und Fotos

Gretchenfrage: Wie viel finanziellen und zeitlichen Aufwand betreiben die Behörden im Einzelfall?

martinsteiger.ch 🙏