# Bedrohungen

- Datenspeicherspürhunde
- Phishing
- Funkzellenabfrage
- Verkehrsdatenüberwachung
- Forensik
- Persönliche-Überwachung
- Public-Charger
- Staatstrojaner
- Video-Audio-Überwachung
- Massenüberwachung
- Imsi-Catcher
- Shoulder-Surfing
- Stille-Sms
- Mobilfunk
- Logger

# Datenspeicherspürhunde

Im folgenden wird dieser Artikel unter der Creative Commons BY-NC-SA 4.0 von Netzpolitik.org wörtlich zitiert, da dieser das Thema ziemlich gut erklärt:

# Der unwiderstehliche Geruch von Festplatten

Bei Hausdurchsuchungen kommen immer öfter auch „Datenspeicher-Spürhunde“ zum Einsatz. Sie können Smartphones, Festplatten und sogar SIM-Karten riechen. Bei deren Ausbildung will sich die Polizei allerdings nicht in die Karten schauen lassen.

Von Polizeihunden, die nach Rauschgift oder Sprengstoff suchen, haben alle schon gehört. Auch von Hunden, die nach Banknoten schnüffeln, auf der Suche nach Steuerflüchtlingen. Am Ende der letzten Dekade kam dann eine neue Ausbildung dazu: Hunde, die Datenträger erschnüffeln – und das Land Sachsen war Vorreiter. Im Fall des massenhaften Kindesmissbrauchs auf einem Campingplatz in Lüdge kam Deutschlands bis dahin einziger „Datenspeicher-Spürhund“ zum Einsatz. In der Folge bildete die Polizei von Nordrhein-Westfalen ebenfalls solche Hunde aus und präsentierte „Odin“, „Jupp“ und „Ali Baba“ auch in sozialen Medien.

Auf der Transparenz-Plattform FragdenStaat gibt es gleich mehrere Anfragen zu Datenspeicher-Spürhunden. Dort hätte man also mehr dazu erfahren können, wie die Polizei Hunde trainiert, damit diese CDs, Festplatten, Speicherkarten, USB-Sticks, Smartphones und SIM-Karten finden. Denn ganz offenbar haben Speichermedien einen ganz eigenen Geruch, den Hunde erkennen, wenn sie auf diesen konditioniert werden. Allerdings hat die NRW-Polizei die Ausbildung der Hunde als „Verschlusssache“ eingestuft und großflächig geschwärzt, und so muss man sich stattdessen auf Medien wie zooroyal und deren Berichterstattung über die „Fellnasen“ verlassen.

In einem Bericht der Süddeutschen Zeitung heißt es, dass die Suche nach Datenträgern viel schwieriger sei als nach Drogen, die einfach stärker riechen würden als die handelsübliche Festplatte. Auch die Polizei Sachsen-Anhalt schreibt in einer Präsentation, dass die Datenträger kaum Geruchsmoleküle freisetzten.

Der sächsische Diensthundeführer sagte der Zeitung damals, dass der Hund die Chemikalien rieche, die zur Herstellung der Speichermedien verwendet werden. Er habe sogar den Eindruck, dass sein Hund Lithium-Ionen-Akkus schneller fände als Handys mit Chrom-Nickel-Batterien und gehe davon aus, dass „Artus“ Lithium riechen könne.

Weil die gesuchten Datenträger so wenig Geruch verströmen, verlange die „Spürarbeit“ eine „hohe, ausdauernde und körperlich anstrengende Leistung“ des Diensthundes, heißt es in den Unterlagen aus Sachsen-Anhalt. Deswegen setze diese Ausbildung „ein fokussiertes, sachliches Spürverhalten des DH [Diensthundes] voraus.“

# Belohnung: Beißwurst

Die Polizei NRW selbst verrät auf ihrer Webseite, wie die Suche vor sich geht: „Hört Hank [Hund] das Kommando »Spür!«, beginnt er zu suchen. Bleibt er bewegungslos stehen, weiß Peter Baumeister [Hundeführer]: Er hat etwas gefunden. Als Belohnung bekommt Hank dann sein Lieblingsspielzeug: eine Beißwurst.“

Demnach dauert die Zusatz-Ausbildung eines Spürhundes zum Datenspeicher-Spürhund 20 Tage, welche der Hund zusammen mit seinem Bezugsmenschen absolviert. Nach der Ausbildung darf sich der Mensch dann „Datenspeicherspürhundführer“ nennen. Ein Wort, wie es deutscher kaum klingen könnte.

# Phishing

Das Phishing mit E-Mails oder SMS ist zwar im Allgemeinen eher im Kontext von Enkeltricks oder anderem Scam bekannt, doch auch staatliche Akteure nutzen gerne Phishing, um Zielpersonen mit Malware zu infizieren.

Hierbei sind ein paar Sachen zu bedenken. One-Click-Malware, also jene, bei der User*innen proaktiv auf einen Link klicken, oder einen Download tätigen müssen, damit das Gerät infiziert werden kann, ist um einiges günstiger zu haben, als Zero-Click-Lösungen, bei denen Geräte, ohne weiteres Zutun der Nutzenden infiziert werden können.

Außerdem sind Phishingangriffe auch relativ schwierig zurück zu verfolgen. Fliegt das Phishing auf, bleibt trotzdem meist unklar, von wem der Angriff stammt, was eine ziemlich sichere Angriffsposition ermöglicht. Bei einer heimlichen Wohnraumverwanzung aufzufliegen ist deutlich riskanter und alarmiert die Betroffenen. Phishing hingegen landet bei uns allen ständig im Postfach und weckt kaum Misstrauen.

Hier ist ein Beispiel für, durch geschickte Wahl von Unicodezeichen, gefälschte Links. Erkennst du einen Unterschied in den Links? Welcher Link führt auf welche Seite?

**Beispiel 1**

- https://codeberg.org/esc-it/esc-it.org/releases/tag/@esc-it.org
- https://codeberg.org/esc-it/esc-it.org/releases/tag/@esc-it.org

Ausnahmsweise, nur zum Lernen, kannst du jetzt auf die beiden Links klicken, um zu sehen was passiert. Hat deine Vermutung gestimmt?

Der 1. Link führt nicht auf codeberg.org sondern auf esc-it.org. Durch das @ wird der Teil davor als Nutzername verwendet. Eigentlich sollte das nicht funktionieren wenn vor dem @ ein / ist, aber im 1. Link sind Unicode Zeichen, die kein "normales" Slash sind.

Manche Browser zeigen bei dem falschen Link sogar eine Warnung an, wie hier in Firefox und dessen Fork Librewolf:
Ein Pop-Up in Firefox warnt, dass wir dabei sind uns bei einer Webseite anzumelden die keine Anme

Chromium zeigt beispielsweise keine solche Warnung.

Auffällig an den Links ist, dass am Ende eine Domain steht (...@<esc-it.org>). Aber auch das ist kein eindeutiges Zeichen für Fakes und wird mit immer neuen Top-Level-Domains zunehmend schwer zu erkennen. Hier ein Beispiel mit einer ".zip"-Endung, sodass es sowohl eine .zip-Datei als

auch eine .zip-Domain sein könnte:

Achtung: Der erste Link führt auf eine Domain *(1312.zip)*, die nicht uns gehört. Das heißt wir wissen nicht was darauf geschieht. Daher besucht diesen Link bitte nicht einfach, wenn ich nicht genau wisst, was ihr tut.

**Beispiel 2**

- https://codeberg.org/esc-it/esc-it.org/releases/tag/@v1312.zip
- https://codeberg.org/esc-it/esc-it.org/releases/tag/v1312.zip

Auch hier führt der erste Link nicht auf eine Zip-Datei auf codeberg.org, der zweite Link aber schon. Hier erscheint auch keine Warnung, weil es die Domain bisher nicht gibt.

**Fazit**

- Klickt nicht auf komische Links
- Hinterfragt den Ursprung des Links. Kann das sein, dass mir diese "Adresse" genau diesen Link schickt.
  - Geht auf Nummer sicher und sucht die Seite über verifizierbare Wege. Speichert originale Links in euren Passwortmanagern, in Lesezeichen im Browser oder nutzt Suchmaschinen.
- Tippt die Links im Zweifel von Hand ab.
  - Das hilft aber nichts, wenn der Link per se ein Fake ist. [systeml1.org] wird Euch so oder so auf die falsche Fährte führen. Hierbei wieder der Verweis auf den Punkt oben drüber um die korrekte URL festzustellen.

# Funkzellenabfrage

Um dieses Kapitel zu verstehen ist es notwendig die grundlegenden Konzepte von Mobilfunkzellen (im Folgenden MFZ abgekürzt), insbesondere den Verbindungs- bzw Authentifizierungsprozess zwischen Handy und Mobilfunkzelle, zu verstehen. Wir haben versucht, das im Artikel Mobilfunk verständlich zu veranschaulichen.

Die Funkzellenabfrage ist eine in § 100g Abs. 3 StPO geregelte Maßnahme, derer sich Strafverfolgungsbehörden in ihren Ermittlungen bedienen können. Dabei Fragen die Behörden bei den Betreibern der in dem Fall interessanten MFZ bestimmte Daten zu deren Nutzung ab.

Karte, die symbolisch zeigt, wie mobilfunkzellen in einer Stadt verteilt sind

# Was wird bei Funkzellenabfragen abgefragt?

Bei Funkzellenabfragen werden folgende Daten im abgefragten Zeitraum und "Ort" (also ein bestimmtes Gebiet, das evtl von mehreren MFZ abgedeckt wird) erhoben:

- eingeloggte Rufnummern
- Zeitpunkte von:
  - Einwahl/Auswahl der Geräte
  - Aus- und eingehender Anrufe
  - Mailbox Gespräche
  - gesendete/empfangene SMS

Oftmals werden beispielweise bei Demos Funkzellenabfragen vor, während und nach der Demo gemacht. Dadurch kann beispielsweise ersichtlich werden, welche Geräte sich nur zum Zeitpunkt der Demo an diesem Ort aufgehalten haben und welche Geräte dort evtl "zu Hause" sind.

Welche Geräte zu Zeitpunkt X an welchem Ort, durch FZA

Außerdem können natürlich über Funkzellenabfragen auf einem größeren Gebiet Bewegungsprofile erstellt werden, in dem Ein- und Auswahlzeitpunkte einzelner Geräte bei den jeweiligen MFZ betrachtet werden:

Route von Gerät durch Stadt wird durch FZA ersichtlich

# Statistiken zu Funkzellenabfragen

Verfahren in denen Funkzellenabfragen durchgeführt wurden

Die Zahlen belaufen sich auf die durchgeführten Abfragen. In einer Abfrage können durchaus mehrere Hunderttausend Geräte betroffen sein. Das geht sogar soweit, dass in Berlin im Jahr 2016 statistisch jedes einzelne Handy alle 11 Tage in einer Funkzellenabfrage landete.

Mehr Details zu dieser Statistik

# Verkehrsdatenüberwachung

# Überwachung von Verkehrsdaten

Das ist meistens gemeint, wenn allgemein von TKÜ gesprochen wird. Hier zwingen die Behörden die Serviceanbieter dazu, eure Anschlüsse explizit zu überwachen und den Behörden sämtliche mitgeschnittenen Verkehrsdaten zu kommen zu lassen. Dafür ist ein richterlicher Beschluss notwendig.

Das ist möglich, weil normale Telefonverbindungen, also: Festnetz, Sprachanrufe, SMS und (last but still not missing) Mailboxgespräche lediglich **transportverschlüsselt** sind.

# Transportverschlüsselung

Bei der Transportverschlüsselung wird quasi jedem Teilnehmer in der Kette der gesamten Übertragung einer Nachricht das Recht gegeben die Nachricht zu öffnen und zu lesen.

Schreibt ihr beispielsweise eine normale Email, so geht die Email zunächst transportveschlüsselt an den Mailserver. Dazwischen kann niemand mitlesen. Der Mailserver jedoch kann die Mail öffnen und scannen. Das tun sie in der Regel auch, denn woher sollten eure Mailanbieter wissen was in den Spamordner gehört. Jetzt schickt euer Mailserver die Mail, wieder transportverschlüsselt, an den Mailserver des Empfängers der Mail. Auch dieser kann die Mail auspacken und scannen. Daraufhin schickt dieser Mailserver die Mail abermals transportverschlüsselt an den Empfänger.

Eine schematische Darstellung eines MITM-Angriffs durch die Polizei bei Transportverschlüsselung

Und so funktioniert das im Grunde auch mit Sprachanrufen und SMS.

Hieraus ist ersichtlich, das die Mailanbieter/Mobilfunkanbieter, die ja immer die Berechtigung haben euren Verkehr mitzulesen, der optimale Angriffspunkt für die Behörden sind. Dort können sie (mit richterlichem Beschluss) anklopfen und euren gesamten Datenverkehr verlangen.

Deshalb ist es so wichtig Ende-zu-Ende Verschlüsselung zu benutzen!

Statistiken zur TKÜ

Hier findest du eine detaillierte Erklärung zu dieser Statistik.

# Forensik

# Digitale Forensik

| Hilfe gesucht |
| --- |
| Wenn du dazu etwas beizutragen hast, schau gerne bei dem Issue vorbei und mach mit! |

# Physische Forensik

Bisher gehen wir hier nicht im Detail drauf ein. Generell sind klassische Forenskimethoden der Strafverfolgung zu beachten. Dazu gehören die Sicherstellung von:

- Faserspuren
- Schuhabdrücke
- Fingerabdrücke
- DNA
- ...

All diese Spuren können durchaus schwer zu vermeiden sein, besonders DNA und Faserspuren werden bei so ziemlich jeder Bewegung hinterlassen. Was das allerdings für das spezifische Threat Modeling bedeutet muss gesondert diskutiert werden. Die Analyse von diesen Dingen ist in aller Regel sowohl sehr Zeit als auch Kosten aufwendig. Trotzdem zeigen sich in einzelnen Fallbeispielen, dass verwirrte Cops das auch bei Bagatellen schon angeordnet haben, wie im Beispiel Adbusting Höcke

# Persönliche-Überwachung

**Hilfe gesucht**

Zu den verschiedenen Arten von verdeckten Ermittler*innen suchen wir nach weiteren Informationen sowie nach Statistiken zu deren Einsätzen. Falls du hierzu etwas beitragen kannst, schau doch gerne mal in die verlinkten Issues rein.

In den letzten Jahren haben sich Fälle von Personen bezogener Überwachung vermehrt. Immer häufiger werden Aktivist*innen Ziele von Zielfahnder*innen, V-Leuten oder anderen Spitzeln des deutschen Repressionsapparates.

Zu den Begrifflichkeiten und Unterschieden:

- Zielfahnder: Suchen und observieren Personen
- Tatbeobachter: Das ist die klassische Demo-Zifte. Sie lungern meist in BFE-Einheiten und sind oft bei Demos dabei um Straftaten zu beobachten. Zur besseren Dokumentation machen Sie teilweise während der Demo Bilder von den Personen, deren Kleidung, Rucksäcken oder Schuhen. Sie verfolgen vermeintliche Täter*innen, deren Festnahme teils direkt nach der Demo oder nach nur wenigen Stunden erfolgt. Sie sind vergleichsweise unauffällig, haben also keinen Knopf im Ohr, oder im Ärmel. Das Äußere wird dem entsprechenden Anlass angepasst, gerne auch selbst vermummt.
- Verdeckte Ermittler*innen (VE): Oftmals wenig inhaltliche Positionierung. Haben nur Zeit bei "spannenden Sachen".
- Zivilpolizei: Mit Westen und Knopf im Ohr, erkenntlich am Rand der Demo
- Vertrauens-/V-Personen: Sie werden gezielt vom Staat aus der Szene angeworben. Sie sitzen in Plena und wissen über Aktion/Leute und beteiligen sich rege am Szene-Leben

# Public-Charger

Öffentliche "Ladegeräte" finden sich beispielsweise in öffentlichen Verkehrsmitteln, Cafés, Bibliotheken, Flughäfen, Einkaufshäusern und co.

Unterschieden werden sollen hier natürlich zwischen einfache Steckdosen und USB-Ladebuchsen.

Das Schlimmste, was bei normalen Steckdosen passieren kann ist, dass dir dein eigenes Ladegerät kaputt geht. Abgesehen davon ist ja dein eigenes Ladegerät eh nur zum Aufladen gut und kann daher auch nicht wirklich mehr.

Bei USB-Ladebuchsen sieht es schon ein bisschen anders aus. Seit Jahren häufen sich Fälle von manipulierten Ladebuchsen, hinter denen sich nicht nur eine Spannungsquelle, sondern gleich ganze Mikroprozessoren verbergen, die versuchen auf das angeschlossene Gerät zuzugreifen. Dabei könnte Malware installiert werden, auf den Speicher zugegriffen werden und so weiter.

Netterweise sind mittlerweile sämtliche (mobilen) Betriebssysteme mit Schutzvorkehrungen ausgestattet und fragen die Nutzenden, ob dem angeschlossene "Gerät" Zugriff auf das Handy gegeben werden soll. Allein diese Frage sollte uns schon misstrauisch machen, denn:

**Achtung**

eine einfache USB-Buchse mit der klassischen 5V Spannungsversorgung wird von keinem Handy als "Gerät" erkannt, dem irgendwelche Rechte gegeben werden sollten!

Weiter kann dem vorgebeugt werden, wenn zum Aufladen nur USB-Kabel ohne "data lines" verwendet werden. Das sind solche Kabel mit denen keine Daten übertragen werden können. Das kann man in der Regel einfach am eigenen Rechner mal ausprobieren. Wenn mit dem USB Kabel nicht auf das Handy zugegriffen werden kann, dann hat dieses USB Kabel sehr wahrscheinlich nur 2 Drähte: Plus und Minus. Darüber können dann keine Daten übertragen werden.

**Achtung**

Besonders bei USB Ladebuchsen sei vor manipulierten Spannungsversorgungen gewarnt!

Anders als bei manipulierten Steckdosen, an denen ja noch euer eigenes Ladegerät steckt, kann hier eine manipulierte Spannungsversorgung das Gerät sehr direkt ernsthaft beschädigen.

Daher empfiehlt es sich diese Buchsen wo es auch geht zu meiden.

Falls sie doch einmal benutzt werden müssen, am besten:

- nur mit zwei-adrigen USB Kabeln benutzen
- Buchsen benutzen, bei denen ihr gesehen habt, dass schon vorher jemand ein Handy geladen hat, ohne es danach schreien von sich zu werfen.

# Staatstrojaner

# Quellen-TKÜ

Die Quellen-TKÜ ist quasi eine Online-Durchsuchung "light". Dabei wird zwar die selbe Software wie bei der Online-Durchsuchung eingesetzt, allerdings soll hier nur der live ein- und ausgehende Datenverkehr mitgeschnitten werden. Das Durchforsten von gespeicherten Inhalten ist hierbei nicht erlaubt und angeblich bei eingesetzter Software - durch entsprechende Modifikationen - auch nicht möglich.

Entstanden ist dieses Konstrukt, weil Online-Durchsuchungen einen sehr extremen Eingriff in die Privatsphäre sind, werden sie manchmal von Richter*innen auf Grund von "Unverhältnissmäßigkeit" nicht genehmigt. E2E-Verschlüsselung verhindert aber eine effektive TKÜ bei Serviceanbietern. Also wird diese "abgespeckte" Schadsoftware eingesetzt, da sie eher richterlich genehmigt wird. So können sämtliche Up- und Downloads (hier sind auch Chat-Nachrichten mit gemeint) jeweils vor der Verschlüsselung, oder nach der Entschlüsselung, auf den Endgeräten mitgelesen werden.

Statistiken Quellen-TKÜ

Hier findet ihr mehr Details zu der Statistik der **Quellen-TKÜ**

# Online-Durchsuchung

Wenn von Staatstrojanern die Rede ist, dann ist meist die Online-Durchsuchung gemeint. Hierbei werden betroffene Geräte mit Schadsoftware infiziert, sodass die Angreifer (i.d.R. Cops) vollen Zugriff auf das Gerät haben. Das bedeutet sie können sowohl live mitverfolgen was gerade auf dem Gerät gemacht wird, Kameras und Mikro's anschalten, Standorte abrufen, als auch gespeicherte Inhalte wie Nachrichten, Bilder, Kontakte, Kalender, Notizen einsehen und ausleiten. Die Vorteile davon liegen auf der Hand. Betroffene bemerken die Maßnahmen überhaupt nicht. Geräte müssen eventuell noch nicht einmal beschlagnahmt werden und Festplattenverschlüsselung wird somit "nutzlos" gemacht.

Statistiken Online-Durchsuchung

Statistiken Online-Durchsuchung

Hier findet ihr mehr Details zu den obigen beiden Statistiken zur **Onlinedurchsuchung**

Es ist daher mit Blick auf Online-Durchsuchung und Quellen-TKÜ zu beachten, dass die eingesetzten Softwares aus unterschiedlichen Quellen stammen. Der berühmte Staatstrojaner Pegasus der NSO-Group, oder Predator von Intellexa erfordern extrem teure Lizenzkosten.

Aus von der New York Times geleakten Predator Files ist beispielsweise zu erkennen, dass eine Lizenz zum Infizieren von 20 iOS oder Android Geräten, mit 12 monatiger Garantie, 13,6 Mio € (Euro) kosten soll. Die zu Verfügung gestellte Schadsoftware ist dabei "nur" eine 1-click-solution, bei der die Zielpersonen noch selber auf irgendeinen Link klicken müssen.

Einen Reboot von infizierten iPhones überlebt der Trojaner nicht, dafür müssen nochmal 2,4 Mio € gezahlt werden. Für Sim-Karten aus anderen Ländern, als dem agierenden, müssen 3,5 Mio € extra fließen.

Hier lässt sich also feststellen, dass eine solche Lösung sehr teuer ist. Allerdings haben deutsche (und andere) Behörden auch schon eigene Staatstrojaner gebaut, von denen aber zumindest bisher nicht bekannt wurde, dass sie remote infizieren können, sondern über Hardwarezugriff verfügen müssen.

Daher sollten Geräte auch physisch geschützt werden, denn die Behörden dürfen unter Umständen, wie bei der Wohnraumüberwachung auch, in eure Wohnung einbrechen und auf eurer Hardware heimlich Schadsoftware installieren. Um dem vorzubeugen ist es ratsam, Teile die zum Öffnen der Hardware bewegt werden müssen, so zu bearbeiten, dass ihr einen solchen Zugriff sofort bemerkt.

# Quellen-TKÜ+

Die Quellen-TKÜ+ stellt lediglich weiteres ein juristisches Konstrukt dar, auf das wir aber hier nicht eingehen wollen, da es bei einem Staatstrojaner bleibt. Falls ihr mehr darüber lesen wollt, gibt es dazu eine Stellungnahme des CCC.

**Zitat aus der Stellungnahme des CCC**

Die nur rechtlich definierte Trennung zwischen den „Payloads“ der heimlichen Schadsoftware, die nunmehr drei Trojaner-Varianten („Quellen-TKÜ“, „Quellen-TKÜ+“ und „Online-Durchsuchung“) hervorgebracht hat, ist technisch nicht begründbar […]
Durch die oben skizzierten Infektionswege und den zwingend damit einhergehenden tiefen Veränderungen in den Sicherheitsmechanismen der angegriffenen Systeme wird deutlich, dass eine technische Abgrenzung zwischen dem Staatstrojaner zur Festplatten-Durchsuchung („Online- Durchsuchung“) und dem Trojaner zum Abhören der laufenden Kommunikation („Quellen-TKÜ“) sowie der mittlerweile dritten Trojaner- Variante („Quellen-TKÜ+“ oder „Kleine Online-Durchsuchung“), die auch gespeicherte Inhalte und Umstände der Kommunikation erfassen darf, in der Praxis bei ehrlicher Betrachtung weder zuverlässig zu gewährleisten noch

überhaupt klar zu umreißen ist. Die „technischen Vorkehrungen“, die alle drei Staatstrojaner-Varianten unterscheiden sollen, könnte man zwar zu implementieren versuchen, allerdings scheitert offenbar das BKA seit mehr als einem Jahrzehnt daran, Trojaner-Varianten zu entwickeln oder zu kaufen, die alle grundrechtlich gebotenen Vorgaben sicher erfüllen.

Letztlich bleibt die Unterscheidung aller drei Trojaner-Varianten eine juristische und zudem theoretische, die mit den Realitäten der Trojaner- Branche und mit den technischen Notwendigkeiten beim erfolgreichen Infizieren eines informationstechnischen Geräts nicht zusammengehen.

Hierzu gab es auch einen früheren Fall, bei dem der CCC 2011 einen Staatstrojaner zerlegt hat und dabei zeigte, dass dieser natürlich technisch alles mit dem System machen konnte. Daraufhin, hat das Bundesverfassungsgericht das Gesetz 2016 auch für teilweise Verfassungswidrig erklärt.

# Video-Audio-Überwachung

## Videoüberwachung - öffentlicher Orte und Plätze

Insbesondere an Anlagen und Einrichtungen der Bahn. Es besteht ein eigener Nutzungsvertrag zwischen Bahn und Bundespolizei, der festlegt, dass die Infrastruktur der Videoüberwachung durch die Deutsche Bahn betrieben wird und die Bundespolizei diese nutzen darf.

Weiter sind oft Orte betroffen, wo es "gehäuft zu Drogenhandel, Diebstahl oder Gewalt kommt"

## "Intelligente Videoüberwachung"

Es gab einen Pilotversuch am Berliner Südkreuz 2019 und seit Juni 2023 in Hamburg auf dem Hansaplatz.

2023 implementiert der schweizer Bahnhof in Schaffhausen "intelligente" Kamerasysteme, um das Kaufverhalten von Kund*innen zu analysieren und Ladenmiete nach Kundenaufkommen aufzuschlüsseln.

Seit 2018 wird die Mannheimer Innenstadt mit KI-Technik vom Frauenhofer-Institut in München Überwacht. Von 68 Überwachungskameras der Polizei in Mannheim sind 10 mit "KI-Software" ausgestattet. Der Einsatz dieser Technik wurde im Dez. 2023 bis 2026 verlängert

Bisher sollen alle oben genannten Systeme keine direkte Identifikation von Individuen zulassen. Das heißt, dass die Systeme nur Situationsabhängig den gerade erkannten Personen einen *Identifier* zuweisen, der nur zur Verarbeitung der jeweiligen Videosequenz dienen soll. Personalien sollen so nicht festgestellt werden können.

In Rheinland-Pfalz gibt es seit 2023 "Handy-Blitzer", die Autofahrer*innen fotografieren und nach "Handy-am -Ohr" - Situationen analysieren.

In Frankreich werden zu Olympia 2024 massenhaft "intelligente" Verhaltensscanner eingesetzt werden.

# Videoüberwachung Demonstrationen

**Hilfe gesucht**

Bei den Ermittlungen zu den G20 Protesten wurde Videomaterial mittels Gesichtserkennung ausgewertet. Hier könnten Details dazu eingefügt werden.

Gesichtserkennung bei G20, nicht zum Identifizieren sondern zum Verfolgen

- Polizei mit Kameras
- Kamerawagen
- Insbesondere hier Datenauswertungen

# Video- Audioüberwachung - private Räume

Prinzipiell können private Räume verwanzt werden, auch wenn sich Verdächtige nur ab und zu darin aufhalten.

In der folgenden Statistik sind die Verfahren in denen Wohnraumüberwachung eingesetzt wurde aufgelistet. Die Statistik erfasst nur Verfahren, die geeignet sind den Schutzbereich des § 13 GG, die Unverletzlichkeit der Wohnung, zu berühren. Verfahren in denen andere Räume überwacht wurden sind demnach nicht erfasst.

Statistik Wohnraumüberwachung

# Massenüberwachung

## Chatkontrolle

Heiß diskutiert in 2023. Stand Okt. 2023 ist auch dieser Form der anlasslosen Massenüberwachung eine Absage erteilt worden. Vom Tisch ist aber auch dieses Thema nicht, da es höchstwarscheineich zu einem der großen Themen im EU-Wahlkampf Mitte 2024 wird.

## Vorratsdatenspeicherung

- anlasslose, präventive Speicherung sämtlicher Verkehrsdaten (keine Inhalte)
- EUGH-Urteil (Sep. 2022): rechtswidrig

## Quick-Freez

- BKA fordert "Quick-Freez"
  - "einfrieren" von Verkehrsdaten nach richterlichem Beschluss (einen Monat lang)
  - bisher politisch noch nicht umgesetzt

# Imsi-Catcher

Ein IMSI-Catcher simuliert eine kommerzielle Mobilfunkzelle (MFZ), um die Clients dazu zu bewegen, mit ihnen eine Verbindung aufzubauen. Generell gilt:

- Endgeräte loggen sich bei MFZ mit stärkstem Signal ein.
- Funkzelle fordert „Identity Request“
- Endgeräte authentifizieren sich mit IMSI + IMEI (und erhalten TMSI von der MFZ).

Dabei kann im Groben zwischen passiven und aktiven IMSI-Catchern unterschieden werden:

**Passive** IMSI-Catcher warten nur darauf, dass Clients versuchen sich mit ihren Identifier bei der MFZ zu authentifizieren. Damit können detaillierte Informationen darüber gesammelt werden, wer, oder viele Personen sich bspw. bei einer Demo aufhalten. Den Clients fällt der Schwindel auf Grund des GSM-Protokolls nicht auf.

**Aktive** IMSI-Catcher warten nicht nur auf die Synchronisationsanfrage des Clients. Sie geben dem Client auch eine TMSI (kann hier mit lokaler IP verglichen werden) und bauen sogar in seinem Namen eine legitime Verbindung zu einer echten MFZ her. Damit können vollwertige 'machine-in-the-middle-attacks' realisiert werden.

# Welche Sicherheitslücke wird hier ausgenutzt?

Das Problem liegt bei der Authentifizierung zwischen Telefon und der MFZ(Mobilfunkzelle). Das Telefon muss sich nämlich (wie unten dargestellt) gegenüber der MFZ mit seinen einmaligen/unverwechselbaren Identitäten (IMSI, IMEI) verifizieren, um zu beweisen, dass es das Recht hat, das Mobilfunknetz zu benutzen.

Die Funkzelle authentifiziert sich gegenüber dem Telefon jedoch **nicht**. Deshalb kann das Telefon auch nie sicher wissen, ob es gerade wirklich mit einer normalen, kommerziellen MFZ kommuniziert, oder nicht doch mit einem Klon der Behörden.

# Aktiver IMSI-Catcher - Systematik

IMSI-Catcher Schematik

# Warum ist die Kommunikation Telefon-Polizei unverschlüsselt?

Die Antwort findet sich in der oben beschriebene Schwachstelle im Kommunikationsprotokoll bei der Authentifizierung. Durch bestimmte Schritte ist es dem IMSI-Catcher möglich, das Telefon beim Authentifizierungsprozess auf einen alten Mobilfunkstandart (idR. 2G) herunter zu zwingen. Das ist allgemein möglich, um in Situationen, in denen moderne Standards (3G/4G) keinen Empfang bieten, die noch vorhandene 2G Infrastruktur nutzen zu können. Diese ist oft in der territoriale Abdeckung etwas resistenter als die moderneren. Der 2G-Standart wiederrum ist schon lange überholt und Sicherheitstechnisch in keinem Fall zu empfehlen. Von staatlichen Akteuren einmal abgesehen, ist es sogar privaten Menschen möglich, 2G-"verschlüsselte" Kommunikation sehr schnell zu entschlüsseln und mitzulesen/hören. Deshalb Kennzeichnen wir diese Kommunikation in seiner Praxis als "unverschlüsselt"

**Warum ist die Kommunikation Polizei-Mobilfunkzelle wiederum verschlüsselt?**

Um sogenanntem "eaves dropping" – also dem belauscht werden – entgegen zu wirken, akzeptieren die MFZ der neuen Standards nur Kommunikation, die mit ihrem jeweiligen Standard verschlüsselt wurden. Damit das Telefon also nicht merkt, das es eigentlich mit einer falschen MFZ verbunden ist, muss der IMSI-Catcher also auch eine real-funktionierende Verbindung zum Mobilfunknetz aufbauen. Dafür muss er die Verbindung zur MFZ wieder verschlüsseln.

# Praktische Gefahren

**Das heißt**

- Handy mit privater SIM & IMEI macht identifizierbar & ortbar
- "Anonyme" SIM-Karte und Handy ist nicht gleich anonym

Es ist zu beachten, dass dadurch potentiell Gefahr besteht, wenn ein "anonymes" Handy wiederverwendet wird. In Zusammenhang mit Funkzellenabfragen lassen sich unter Umständen Bewegungsprofile dieser Geräte herstellen und kontextualisieren.

Ein potentielles Beispielszenario könnte so aussehen: Ihr benutzt euer Aktionshandy auf mehreren Aktionen/Demos, gerne auch in verschiedenen Städten/Bundesländern. Bei diesen Demos landet ihr (eure IMSI+IMSI) mehrfach in Funkzellenabfragen. Damit kann erst einmal niemand etwas anfangen, außer zu sagen, dass dieses Gerät auf all diesen Veranstaltungen präsent war. Nun lauft

ihr aber auf weiteren Demos an IMSI-Catchern vorbei und werdet ggf. dabei kontrolliert oder gefilmt. Dadurch könnte natürlich über die Zeit eine Korrelation zwischen euch und dem Gerät hergestellt werden.

Hardware für professionelle IMSI-Catcher kommt in in Deutschland und Umgebung in der Regel von Rhode&Schwarz. Deren Geräte sind global, nicht nur bei Strafverfolgungsbehörden, bekannt und beliebt. Diese State-of-the-Art Technik ist auch dementsprechend teuer, Preise bewegen sich in 4-5 stelligen Bereichen.

Es lassen sich allerdings auch mit ~25€ "teuren" SDR-Dongles (Software Defined Radios) simple passive IMSI-Catcher realisieren. Diese sind allerdings nur dazu fähig, den existierenden Verkehr mitzulesen, jedoch nicht dazu, eine fake MFZ aufzusetzen und tatsächliche MITM Attacken auszuführen.

# Empfehlung

Lukas Arnold beschreibt in seinem Talk auf dem 37c3 (CCC-Congress 2023), wie es mit ihrem selbst gebauten Tool möglich sein sollte, fake base stations mit Hilfe eines iPhones zu erkennen.

# Quellen

- https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks
- SnoopSnitch-Talk (gehört in Empfehlungen): https://media.ccc.de/v/ber15-5-detecting_imsi-catchers_and_other_mobile_network_attacks

# Statistik zu IMSI-Catchern

IMSI-Catcher - Statista

# Shoulder-Surfing

Shoulder Surfing meint, wenn dir jemand heimlich über die Schulter schaut, um zu sehen, was du so auf deinem Handy, Laptop, Din A4 Block oder was auch immer tust bzw. tippst.

| **Achtung** |
| --- |
| Besonders beim Passwörter eintippen gilt besondere Vorsicht! |

Denn das bester Passwort hilft natürlich nichts, wenn es den Behörden in die Hände fällt.

Zu aller erst sei hier auf die immer mehr werdende Videoüberwachung hingewiesen. Gib keine Passwörter unter Kameras ein!

Wenn du selber schonmal versucht hast shoulder zu surfen, wird dir aufgefallen sein, dass es Orte und Situationen gibt, die dafür besonders gut geeignet sind.

In vollen Hörsälen beispielsweise kriegt man die Bildschirme und Tastaturen von mindestens 3 seiner Vorderpersonen praktisch vor die Nase gehalten.

Auch in öffentlichen Verkehrsmitteln sind besonders jene Sitze geeignet, die sich nicht direkt hinter der Zielperson, sondern schräg dahinter befinden. Ist der Bus extrem voll, fällt es noch nichtmal auf, wenn eine Person geradezu über deinem Handy hängt, während du tippst.

In solchen Situationen ist es wichtig sich wie im ehrlichen Thread-Modelling genau zu überlegen:

- besteht diese potentielle Gefahr wirklich, oder ist das übertrieben?
- ist es das Risiko wert, trotzdem mein Passwort einzutippen, oder kann ich warten/einen besseren Ort finden?

# Stille-Sms

Die Stille SMS ist nach GSM-Spezifikation 03.40 aus dem Jahr 1996 definiert: „Ein Kurzmitteilungstyp 0 bedeutet, dass das Endgerät (ME) den Empfang der Kurzmitteilung bestätigen muss, aber ihren Inhalt verwerfen kann.“

Das bedeutet, dass diese "leere" SMS an die entsprechende SIM zugestellt wird und das Telefon sofort eine Empfangsbestätigung an den Absender zurück sendet. Da das Telefon aber von vornherein weiß: "Ah, das steht eh nix drin, weg damit", ignoriert es diese SMS einfach, ohne der Benutzer*in überhaupt den Empfang dieser Nachricht mitzuteilen.

Dadurch entsteht bei den Mobilfunkbetreibern aber zurückverfolgbarer Datenverkehr, da die SMS (und später auch ihre Empfangsbestätigung) ja bis an ihr Ziel durch sämtliche dafür nötigen Mobilfunkzellen weitergeleitet wurden. Dieser Pfad, den die SMS dabei nimmt, kann dann von den Behörden ausgewertet werden und somit Standorte mit einer Genauigkeiten von bis zu wenigen Metern bestimmt werden.

auf mittel/osteuropäischer Karte Darstellung des Versands einer stillen SMS und dem Empfang ihrer

# Stille SMS - Anwendung

Stille SMS

Bemerkung: Die hier gezeigten Zahlen stammen von kleinen Anfragen der Fraktion Die Linke im Bundestag und beziehen sich dadurch auch nur auf die aufgeführten Bundesbehörden. Leider haben wir keine offiziellen Statistiken dazu aus dem Bundesjustizministerium, was auch die Landesbehörden mit einschließen würde.

Das Bundesamt für Verfassungsschutz gibt seit dem zweiten Halbjahr 2018 keine Zahlen mehr dazu raus.

# Mobilfunk

Für die Bedrohungen im Bereich Mobilfunk müssen zunächst einige Grundlagen erklärt werden. In diesem Artikel dreht es sich um die Frage, wie die Kommunikation eines einzelnen Handys mit dem Mobilfunknetz, in Form der Mobilfunkzelle [ugs.: Antennenmast]. Dabei tauchen die Begriffe IMSI und IMEI (und manchmal auch TMSI) häufiger auf, die hier ebenfalls kurz erläutert werden.

# Wem gehören Mobilfunkzellen?

Mobilfunkzellen (MFZ) werden von Mobilfunkanbietern betrieben. Dementsprechend kontrollieren die jeweiligen Mobilfunkanbieter auch den Datenverkehr durch diese MFZ hindurch. In dem unteren Bild symbolisieren die verschiedenen Farben, verschiedene Anbieter, wie z.B. Telekom, Vodafon, O2, etc.

Karte, die symbolisch zeigt, wie mobilfunkzellen in einer Stadt verteilt sind

# IMSI: SIM-Identifier

Jede SIM-Karte besitzt eine eindeutig identifizierbare Nummer, die International Mobile Subscriber Identity, kurz IMSI. Durch die Registrierungspflicht von SIM-Karten in den meisten europäischen Ländern lässt sich die SIM-Karte eindeutig einer Identität zuordnen. Das können die Repressionsbehörden einfach bei den Mobilfunkanbietern abfragen und machen es auch sehr regelmäßig:

Welche Nummern gehören Anna und Arthur ?

Welche Nummern gehören Anna und Arthur ?

Natürlich funktioniert diese Abfrage auch in die andere Richtung, von SIM-Karte zur Identität:

Wem gehört diese Nummer ? Natürlich funktioniert diese Abfrage auch in die andere Richtung, von SIM-Karte zur Identität:

Wem gehört diese Nummer ?

Quelle: Bestandsdatenauskunft 2022: Behörden fragen sekündlich, wem eine Nummer gehört

# IMEI: Geräte-Identifier

Auch Mobilfunkmodems (also der Chip im Handy der sich mit dem Mobilfunknetz verbinden kann), besitzen eine eindeutige Nummer, die International Mobile Equipment Identity, kurz IMEI. Diese IMEI sind in der Regel 15-Stellen lang und global einzigartig. Der Aufbau schaut wie folgt aus:

- die ersten 8 Ziffern sind, einfach gesagt, Typen spezifisch. Zum Beispiel haben alle Google Pixel 7a als erste 8 Stellen: 35917382
- die nächsten 8 Ziffern sind Seriennummern
- *die letzte Ziffer ist zur Fehlerkorrektur (error correction)*

picture of IMEI sets of different models from same and different vendors next to each other.

**Wie wird sichergestellt, dass diese Nummern einzigartig sind?**

Da viele verschiedene Firmen solche Mobilfunkmodems produzieren ist es notwendig, sich untereinander abzusprechen. Sonst würden bei den täglich abertausend produzierten Modems schnell Nummern multiple Male vergeben werden.

Darum kümmert sich die **GSMA** (Global System for Mobile Communications Association). Der Name spricht hier für sich selbst.

- Will ein Hersteller also ein neues Modell auf den Markt bringen, gehen sie zur GSMA und bitten um einen "Nummernraum", die 8 ersten Stellen. Nun dürfen sie alle produzierten Chips dieses Modells mit diesem Nummernraum benennen, also IMEIs vergeben.
- Die Seriennummern dienen zur Unterscheidung einzelner Geräte des selben Modells.
- Die Fehlerkorrektur ist ein bisschen schwarze Magie und kann hier wirklich vernachlässigt werden.

**EIR: (Equipment Identity Register)**

EIRs (Equipment Identity Register) sind im Grunde Datenbanken mit IMEIs. Meistens werden dort IMEIs gestohlener Handys in "blacklists" verwaltet (siehe weiter unten). Der Standard sieht aber auch "whitelists" vor. Das würde bedeuten, dass alle produzierten IMEIs erfasst werden und nur diese erfassten auch am Netzwerk teilhaben dürfen. Das wäre dann ein bedeutendes Sicherheitsrisiko, wenn ein Handy mit zurückverfolgbaren Zahlungsmethoden gekauft wird.

Beispiele für Modemhersteller: Qualcomm, Huawei, ZTE, Sierra Wireless, Netgear, Alcatel, TP-Link

Durch die IMEI ist also jedes mobilfunkfähige Gerät identifizierbar.

Wenn ein Gerät gleichzeitig mit mehreren SIM-Karten verwendet werden kann (egal ob bspw. 2 physische SIMs, oder 1 e-SIM & 1 physische SIM), hat es auch entsprechend viele IMEIs.

**Warnung**

Oft ist es aber ziemlich einfach eine Verbindung zwischen diesen beiden IMEIs herzustellen:

- Oft werden die Seriennummern einfach hochgezählt *(außer die error correction)*
- Wenn dauerhaft zwei IMEIs immer am selben Ort sind lässt sich das korrelieren
- Die Hersteller und Händler kennen die Korrelation der beiden IMEIs
- Sollte hier ein EIR im Spiel sein, sind diese beiden IMEIs im EIR auch miteinander verknüpft. Ist also eine der beiden IMEIs bekannt, ist aus dem EIR auch die Zweite ersichtlich.

Die IMEIs lassen sich nicht ohne Weiteres ändern. In vielen Ländern ist ihre Manipulation sogar strafbar und erfordert zudem spezielle Hardware, die am ehesten aus China bezogen werden kann.

# Probleme beim Kauf von Handys

Kauft Ihr also ein Handy im Laden und bezahlt mit Karte, liegt danach dem Laden die Verknüpfung eurer Karte und der IMEI(s) eures Handys vor. Kauft Ihr ein Gerät sogar direkt bei eurem Mobilfunkanbieter, kann sogar durch die oben gezeigten Abfragen wie "Welche Nummern gehören dieser Person?" bei den Anbietern direkt auch euer genaues Gerät bestimmt werden (also inklusive Seriennummer, IMEI, etc). Kauft Ihr also ein Handy im Laden und bezahlt mit Karte, liegt danach dem Laden die Verknüpfung eurer Karte und der IMEI(s) eures Handys vor. Kauft Ihr ein Gerät sogar direkt bei eurem Mobilfunkanbieter, kann sogar durch die oben gezeigten Abfragen wie "Welche Nummern gehören dieser Person?" bei den Anbietern direkt auch euer genaues Gerät bestimmt werden (also inklusive Seriennummer, IMEI, etc).

Als Konsequenz daraus ist es Behörden möglich, durch Abfragen bei Verkäufern und Geräteherstellern, die per Werk vergebenen IMEIs zu spezifischen Geräten zurück zu verfolgen.

Und damit besteht, wenn das Handy über die eigene Identität gekauft wurde, auch diese Zuordnung.

Uns ist allerdings bisher nicht bekannt ob und wie oft Behörden diese Zuordnung abfragen.

- Identifier eines Gerätes, nicht der SIM-Karte
- weltweit einzigartig
- wird an Mobilfunkanbieter übertragen, wenn mit Mobilfunknetz verbunden (siehe [Authentifizierung](./mobilfunk.md#authentifizierung))

# Authentifizierung

Schematische Darstellung des Authentifizierungsprozesses zwischen Sim und Mobilfunkzelle

- Erkennt das Handy das Signal einer MFZ, versucht es bei ihr mit einer Art "HALLO" anzuklopfen, um zu sehen, ob die MFZ überhaupt erreichbar ist und sagt ihr, das falls das der Fall ist, das es sich gerne ins Netz einloggen möchte.
- Wenn die MFZ diese Nachricht empfangen konnte, fragt sie zuerst einmal nach der Identität des Handys, um sicher zu gehen, dass es überhaupt das Recht hat, sich bei ihr einzuloggen.
- Daraufhin schickt das Handy die IMSI seiner SIM-Karte um zu beweisen, dass es das Recht hat sich zu verbinden. Gleichzeitig schickt es aber auch die IMEI seines Mobilfunkmodems (also des Handys) mit.
  - Eine Telekom MFZ würde also eine Vodafon Sim-Karte ablehnen und ihr sagen, dass sie kein Recht hat das Telekom-Netz zu benutzen.
- Damit ist die Authentifizieren quasi abgeschlossen und eine Verbindung kann aufgebaut werden. Was es mit der TMSI auf sich hat ist hier zweitrangig und deshalb übersichtshalber in den Details eingeklappt.
- Dem Standard nach können solche Verbindungen auch nur "verschlüsselt" aufgebaut werden. Warum das hier in Anführungszeichen steht, kannst du hier nachlesen.

**Was ist die TMSI?**

Würde nun einfach eine Verbindung aufgebaut werden, könnte jede*r in der Nähe mit geeigneter Hardware (bspw. Software Defined Radios ab 20€) sehen, welche Handys gerade mit welchen Sim-Karten im Netz eingeloggt und wie viel sie kommunizieren. Damit das nicht geschieht, geht das Prozedere noch um einen Schritt weiter: Die MFZ gibt dem Handy eine TMSI (Temporary Mobile Subscriber Identifier). Das Handy nutzt von nun an, aber auch nur in dieser Session, diese TMSI zur Identifikation. Loggt sich das Handy irgendwann aus dieser MFZ wieder aus und später wieder ein, beginnt das gesamte Prozedere von vorn und eine neue TMSI wird vergeben.

Falls du dich jetzt noch fragst, wofür das Handy sich nach der ersten Authentifizierung überhaupt noch weiter identifizieren muss: Versendete Pakete benötigen natürlich immer Empfänger (und Absender). Damit dein Handy also während einer Verbindung mit bspw. einer Webseite wieder gefunden werden kann, um dir die Inhalte zu präsentieren, muss "das Netz" natürlich wissen, welches Gerät du denn überhaupt bist.

Sowohl die IMSI als auch die IMEI werden bei der Authentifizierung mit dem Mobilfunknetz übertragen. Damit entstehen bei den Mobilfunkanbietern Tabellen (Datenbanken), die eine eindeutige Zuordnung zwischen IMSI und IMEI, also Handy und SIM-Karte, ermöglichen. Bei den Anbietern liegen diese Daten zwar nicht lange rum (zum Zeitpunkt des Schreibens dieses Artikels gibt es in Deutschland noch **keine** Vorratsdatenspeicherung). Dennoch sollte einem diese Gefahr

bewusst sein, wenn ein Handy verwendet wird welches vorher bereits mit einer anderen SIM-Karte verwendet wurde, welche wiederum Rückschlüsse auf die eigene Identität zulässt. Außerdem kann das Handy auch vorher mit einer anderen SIM in einer Funkzellenabfrage gelandet sein.

# Logger

Logger bezeichnen Geräte, mit denen etwas 'geloggt', also mitgeschnitten werden kann. Für uns hier sind zwei Arten von Logger relevant: Keylogger und Screenlogger.

# Keylogger

Keylogger sind Geräte, die im Grunde sämtliche Tasteneinschläge auf eurer Tastatur mitschneiden. Dafür sitzen sie zwischen Tastatur und Computer und sehen aus wie normale USB-Adapter:

Keylogger neben Tastatur

Keylogger zwischen Laptop und Tastatur

Sie können über Funk/WLAN/LTE in Echtzeit jeden einzelnen Tasteneinschlag zu einem Angreifer senden. Das Problem daran ist offensichtlich.

Diese Keylogger sind für sehr kleines Geld zu haben und einfach zu besorgen, sodass ihre Anwendung auch für Amateure sehr simpel ist!

Es gibt sogar Keylogger die wie ein ganz normales Kabel aussehen, siehe z.B. das O.MG Cable.

Fortgeschrittenere Angreifer (zB. Behörden) können auch Keylogger in den Tastaturen selbst verbauen, indem sie die Tastatur aufschrauben und eine kleine Keylogger-Platine an der Elektronik der Tastatur direkt verbauen. Oder sie tauschen die Tastatur einfach durch eine manipulierte aus. Das würde dann allein am USB-Port natürlich nicht auffallen.

# Screenlogger

Screenlogger funktionieren nach dem gleichen Prinzip wie Keylogger. Ein Adapter-ähnliches Gerät wird zwischen Display und PC gesteckt (je nach verwendetem Anschluss: VGA, HDMI, DisplayPort,...) und kann dann die gesamte Bildübertragung mitschneiden und über Funk/WLAN/LTE an den Angreifer senden.

| **Warnung** |
| --- |
| • vor öffentlich zugänglichen PC's |

- anderen PC's die nicht immer unter Beobachtung sind (das eigene Büro zB.)

*Es sei noch erwähnt, dass mit "Key-" bzw. "Screenlogger" auch Software-Logger gemeint sein können. Dass sind dann aber nichts anderes als Viren und beschreiben eine völlig andere Bedrohung als diese hier.*