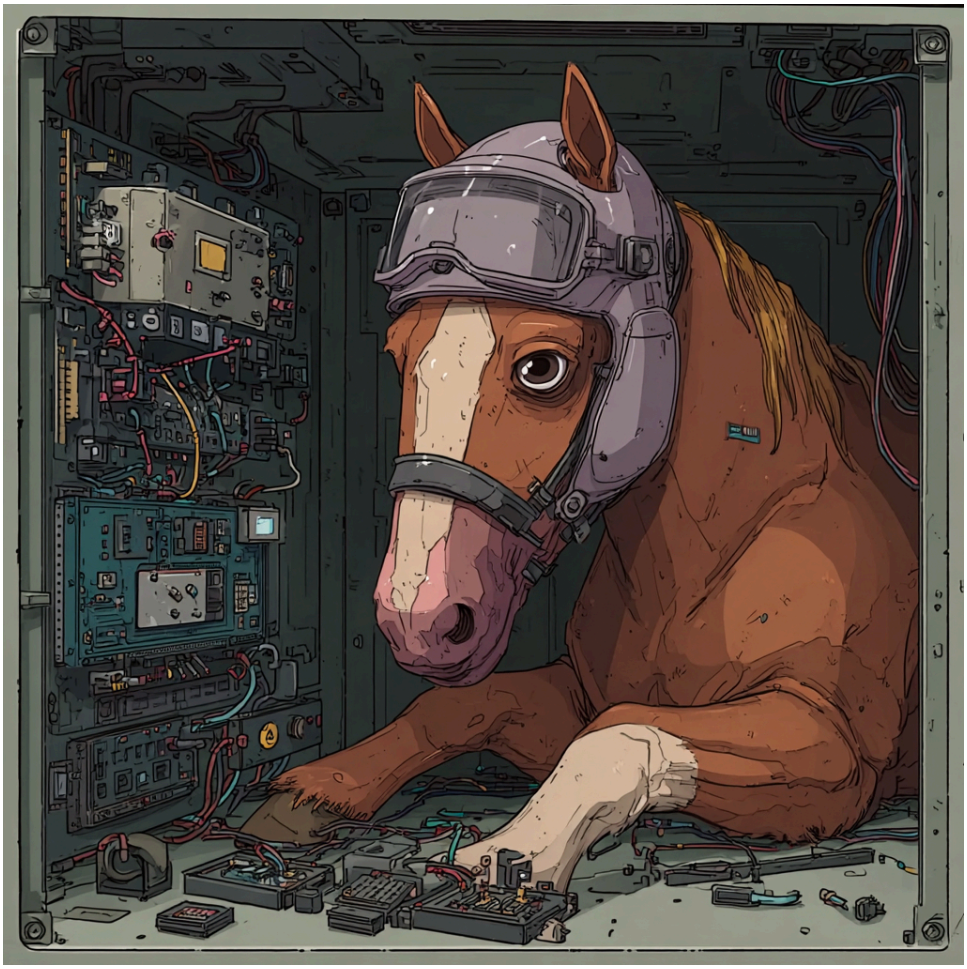
# Online-Durchsuchung, revisited [Update]



Imagine a horse sitting *inside* a computer—not in a server room, no, *inside* the actual hardware. It has made itself quite at home among the transistors and circuit boards, wearing an anti-static helmet and peering critically at a tiny monitor strapped to a RAM stick. It's casually chewing on a byte (low carb, of course) while calmly monitoring the data packets galloping past. Whenever an error occurs, it snorts in disapproval, kicks the motherboard with a hoof, and mutters, "Humans and their updates…" This is the horse that keeps your computer from crashing—whether you like it or not.

Lange nichts mehr von der „Online-Durchsuchung" gehört. Aber wir haben ja Stefan Krempl, der bei Heise zuverlässig liefert – mit allen Buzzwords („Quellen-TKÜ"), die schon hart an der Grenze zu soliden Fake News sind: „Strafverfolger setzen erneut mehr Staatstrojaner ein".

Nein, das tun sie gar nicht. Die Quelle, die sogar dreist

verlinkt ist, gibt das gar nicht her: „Übersicht Telekommunikationsüberwachung für 2023 (Maßnahmen nach § 100a StPO)“. Stand Juli 2025. Nochmal zum Mitschreiben: „Überwachung der Telekommunikation“. Was heißt das genau? IP-Adressen speichern? Hypertext Transfer Protocol Secure hacken? Router aushebeln?

Das verrät uns Krempl wie gewohnt nicht, weil er es gar nicht weiß. Ja ja, da sitzt jemand in einem Büro und beamt von fern eine Überwachungssoftware auf den Linux-Rechner eines Verdächtigen, der gerade Porn schaut. So macht das der Mossad bekanntlich auch, nur dass da noch Sprengstoff drin ist – man kann nie wissen, wofür man den brauchen könnte.

„Heimliche Eingriffe in IT-Systeme durch Ermittler“? Ist gar nicht gar nicht erlaubt, vgl. das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

„Gestattet sind präventive staatliche Eingriffe – vor allem die sogenannte Online-Durchsuchung – in dieses Grundrecht nur, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“, schrieb Krempl selbst. (Irgendwann ist der bestimmt die einzige Quelle zum Thema, die immer von sich selbst abschreibt und sich selbst zitiert.)

Diese „präventiven“ Eingriffe sind mitnichten das, was sich Klein-Fritzchen vorstellt. Ohne physischen Zugriff auf den Rechner geht das nicht, außer man schießt mit der Phishing-Schrotflinte auf einen Windows-Rechner und hofft, dass der Besitzer total bekloppt ist.

Fassen wir das mal seriös zusammen: Die Überwacher überwachen im Rahmen ihrer Möglichkeiten, vermutlich immer öfter wie

immer.

[Update] Jemand fragte nach *inject*. Das könnte von Krempl stammen, ist aber von netzpolitik.org, was ungefähr ein ähnliches hyperventilierendes Niveau ist.

*Eine Werbe-Broschüre von 2011 beschreibt einen beispielhaften Einsatz: „Ein Geheimdienst setzte FinFly ISP im Netzwerk des wichtigsten nationalen Internetdienstanbieters ein. Es genügte, dass das System nur die Log-in-Informationen der Zielperson in das Provider-Netz kannte, um eine Fernüberwachungslösung auf ihrem Computer zu installieren und sie von da an zu überwachen.“ (…) Erst vor zwei Wochen berichtete Amnesty International, wie Journalisten in Marokko über eine solche Netzwerk-Injektion mit dem Staatstrojaner der israelischen NSO Group infiziert wurden.*

– Die Israelische Spyware Pegasus ist für IPhone und Android (Voraussetzung: „fragt die App unter einem Vorwand nach Rechten“ usw. blabla. Ich sage allen Apps, die mich was fragen: NEIN! Widerstand ist zwecklos, du wirst gelöscht!)

– Es ist immer nötig, dass der Nutzer mitmacht. „…jeweils eine SMS auf seinem iPhone 6, die auf neue Hinweise zu Menschenrechtsverletzungen aufmerksam machte und einen Link zu einer Webseite enthielt, die angeblich neue Geheimnisse enthülle.“

Dumm klickt gut. Oder dass jemand anderes physischen Zugriff auf das Handy hat. (Analyse) „Aufgrund des hohen Preises pro Ziel (25.000 US-Dollar) ist nicht davon auszugehen, dass eine breite Masse an Benutzern mit Pegasus infiziert wurde.“

– „Es genügte, dass das System nur die Log-in-Informationen der Zielperson in das Provider-Netz kannte“. Noch Fragen?