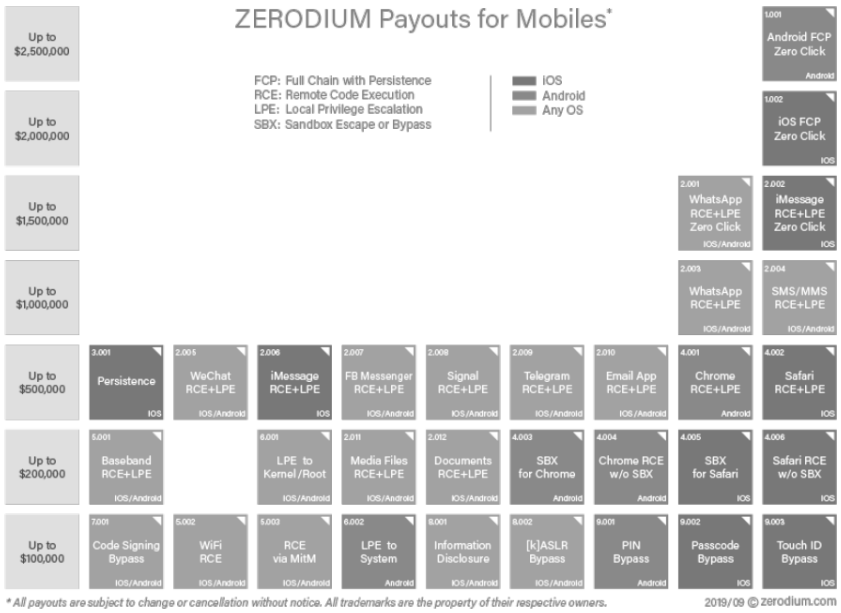
Mehr Unsicherheit durch Regierungsaufträge im privaten Spionagesektor

fb Im Sommer 2021 machte ein Bündnis von Journalist*innen und NGOs[1] den umfangreichen weltweiten Einsatz privater Spionagedienstleistungen zur illegitimen Verfolgung von Whistleblowern, Demokratieaktivist*innen, Journalist*innen, Regierungsmitgliedern und Anderen bekannt. Am Beispiel des „Pegasus“ genannten Tools der israelischen Firma „NSO Group“ *(vgl. ZEIT 2021)* wurde die Frage aufgeworfen, ob demokratische Gesellschaften durch dessen Einsatz einerseits die Datensicherheit für alle Nutzer*innen aktueller Technologie aufs Spiel setzen, andererseits demokratische Werte selbst unterlaufen *(vgl. Krack 2021; Marczak et al. 2020)*. Denn hierbei wird ein oft in einer Grauzone agierender Markt für geheimgehaltene Sicherheitslücken und Werkzeuge zu deren Ausbeutung genutzt. Pegasus ist ein Werkzeug, mit dem praktisch jeder Mensch mit Smartphone lokalisiert, überwacht und deren privateste Kommunikation sowie Präferenzen durch Eingriffe in sämtliche auf dem Gerät installierten Dienste einschließlich solcher, die nicht aktiv benutzt werden, abgegriffen werden können. Ermöglicht wird dies durch kontinuierliche Beschaffung geheimer Sicherheitslücken, die von Hacker*innen für viel Geld nur an die Käufer*in kommuniziert werden. Je nach individuellem Sicherheitsverhalten kann diese Komplettüberwachung mehr oder weniger perfekt realisiert werden – ganz schützen können sich die Nutzer*innen kaum *(vgl. Biermann 2021a, 2021b; Chawla 2021; Hegemann 2021; Kirchgaessner et al. 2021)*. Die in diesem Text argumentierte These lautet, dass der über Nationalstaatsgrenzen hinweg erfolgende Einkauf von Spionagedienstleistungen unter Ausnutzung von Sicherheitslücken und deren Geheimhaltung durch demokratische Regierungen zu einer globalen Verringerung von Datensicherheit führt.

Das früheste Beispiel für eine solche von Regierungen eingesetzte Cyberwaffe ist der Computerwurm W32.-Stuxnet, der 2010 entdeckt wurde, auf der Ausnutzung unveröffentlichter Sicherheitslücken aufbaute und die Sabotage von Industrieanlagen, vermutlich iranischer Atomanlagen, zum Ziel hatte *(vgl. Falliere et al. 2011)*. Als Verantwortliche für diese Schadsoftware werden US-amerikanische und israelische Sicherheitsorgane verdächtigt *(vgl. SPIEGEL 2013)*. Vergleichbar mit Pegasus: die Schadsoftware war so angelegt, dass sie prinzipiell auf jedem Windows-PC der Welt funktionierte und eine vom Hersteller Microsoft unbekannte Sicherheitslücke ausnutzte *(vgl. Beuth 2020)*. Pegasus wiederum wird nicht nur, wie anfangs kritisiert, in autokratischen Systemen zur Verfolgung von Demokratieaktivist*innen eingesetzt, sondern auch in der Bundesrepublik zumindest durch den BND und das BKA *(vgl. Biermann 2021a, 2021b)*. Die öffentliche Skandalisierung führte in den USA dazu, dass NSO Group auf eine Embargoliste gesetzt wurde, denn sie „developed and supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers“ *(ECR 2021)*. Die deutsche Bundesregierung dagegen sieht keinen Grund, die Zusammenarbeit mit dem Unternehmen in Frage zu stellen *(vgl. Biermann 2021a)*. Ein weiteres Beispiel ist der von der israelischen Spionagesoftwarefirma Candiru angebotene browserbasierte Zero-Click[2]-Angriffsvektor „Sherlock“, der vom Hersteller als „untraceable“ beworben wird und auf Windows-, iOS- und Android-Systemen funktionieren soll. Auch Candiru behauptet, seine Spionagetools ausschließlich an Regierungen zu verkaufen. Mit seiner Software ist es auch möglich, gefälschte Beweise auf den Geräten der Opfer zu platzieren, was in einzelnen Fällen von forensischen Spezialist*innen nachgewiesen werden konnte. Ebenso wie NSO Group steht auch Candiru auf der US-Embargoliste *(vgl. ECR 2021; Pandey 2021)*.[3]



Beispiel für Preisangebote für bislang unveröffentlichte Sicherheitslücken.

Quelle: https://zerodium.com/program.html

Den Softwareherstellern unbekannte Sicherheitslücken (Zero-Day-Exploits) stellen die gefährlichsten Instrumente dar, wenn es um das Knacken von IT-Security und die davon geschützten Prozesse, Daten oder Funktionen geht, weil Angriffe ausgeführt werden können, bevor Entwickler*innen Abwehrmaßnahmen überhaupt nur ersinnen können *(vgl. Zetter 2014: Chapter 1)*. Solange diese Lücken nicht geschlossen sind, können sie von Angreifer*innen genutzt werden, die das Wissen darüber von Zero-Day-Exploits-Märkten eingekauft oder selbst potenzielle Angriffsszenarien entworfen haben. Wenn nun demokratisch legitimierte Organe selbst solche Sicherheitslücken aufkaufen und geheim halten, vergrö-