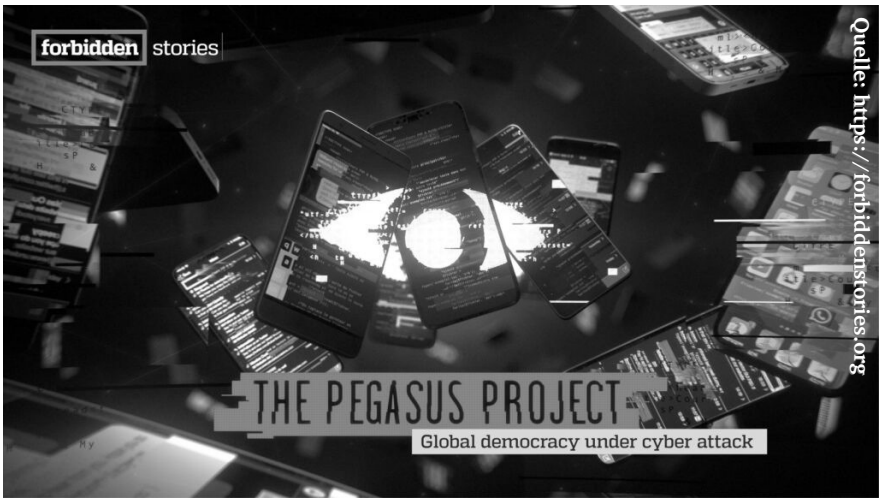
ßert sich für die Nutzer*innen der betroffenen Technologien mit jedem weiteren Tag nicht nur das Risiko von diesen Institutionen infiltriert zu werden, sondern auch Opfer von anderen Kriminellen zu werden, die sich finanzielle Vorteile aus ihren Attacken versprechen *(vgl. Chawla 2021; Hegemann 2021)*.

Die Preise, die für solche Zero-Day-Exploits (siehe Abbildung auf S. 3) erzielt werden, belaufen sich je nach Bedeutung der angreifbaren Sicherheitsarchitektur auf mehrere hundert bis zu mehrere Millionen US-Dollar *(vgl. Zerodium 2021)*. Neben Märkten im Darknet preisen auch einige Regierungsplattformen hohe Summen für die unterschiedlichsten noch unveröffentlichten Angriffsszenarien aus. Statt Hacker*innen und Andere, die Sicherheitslücken auf die Spur gekommen sind, dazu zu motivieren, Öffentlichkeit oder zumindest Softwarehersteller zu informieren, werden starke Anreize geschaffen, diese Information an die Höchstbietenden zu verkaufen. Auch der Einkauf solcher Zero-Day-Exploits oder kommerzieller Spionagesoftware durch demokratische Regierungen auf Märkten in einer legalen, teils auch offensichtlich illegalen, Grauzone verschafft diesen Legitimität und macht es unwahrscheinlicher, dass effektiv gegen den Missbrauch von Sicherheitslücken vorgegangen wird. So wird eine Industrie gefördert und aufgebaut, die sich auf das Eindringen in Sicherheitsarchitekturen millionenfach verbreiteter Geräte und den Einsatz von Schadsoftware spezialisiert *(vgl. Biermann 2021b; Hegemann 2021; Snowden 2021)*.

Was ist die Motivation für Sicherheitsorgane, solche IT-Securityprobleme nicht zu lösen, sondern Sicherheitslücken offen zu halten? Innenpolitiker*innen und Lobbyist*innen argumentieren, dass es ohne den Bruch von Sicherheitsarchitekturen schwerer oder gar unmöglich wäre, organisierte Kriminalität und Terrorismus effektiv zu bekämpfen. Individuelle Sicherheit und öffentliche Sicherheit werden somit als konträr präsentiert; der allgemeinen Sicherheit müssten die Interessen der Individuen untergeordnet werden. Dem widersprechen Datenschützer*innen, die meinen, dass die systematische Verbesserung von Datensicherheit einen größeren Nutzen in Aussicht stellt, da das Ausmaß von Cyberattacken auf einfache Leute, Unternehmen und Behörden, das auch auf solche Sicherheitslücken zurückgeführt werden kann, ausgeufert ist *(vgl. Keeper 2017)*. Statt den wachsenden Spionagesoftwaremarkt mit Einkäufen zu fördern, sollte der kommerzielle Handel mit Sicherheitslücken und diese ausnutzende Tools global verboten und so die Motivation für Unternehmen wie NSO Group, mit Cyberangriffen Profite zu machen, beendet werden *(vgl. Bamford 2016; Biermann 2021a; Krack 2021; Marczak et al. 2020; Snowden 2021)*.



Schadsoftware wie Pegasus, die neben Autokratien auch Länder wie die Bundesrepublik benutzen, stellt eine Gefahr für alle Nutzer*innen von Smartphones dar, weil diese dem Wohlwollen oder der Willkür aller, die darauf Zugriff erlangen, ausgesetzt werden. Außerdem führen derartige Geschäftsmodelle dazu, dass Hacker*innen motiviert werden, Sicherheitslücken nicht zu veröffentlichen, sondern an die Meistbietenden zu verkaufen. Die Nutzung von Märkten, deren Geschäftsmodell auf dem Profit aus Zero-Day-Exploits oder Spionagesoftware basiert, durch demokratische Sicherheitsorgane legitimiert diese Branche und behindert die Schließung von Schwachstellen in weitverbreiteten Technologien. Eine internationale Politik[4], die mehr Sicherheit bewirken will, sollte den Handel mit Angriffsvektoren und Schadsoftware unterbinden, den transparenten Umgang mit Sicherheitslücken fördern und Hacker*innen, die dabei behilflich sind, unterstützen[5]. Wie genau dies umgesetzt werden kann, bleibt zu ergründen. Ein Ansatz könnte sein, Studien zur Wirkung von OpenSource-Technologien und damit verbundene Communitys auf Instrumente und Mechanismen zu untersuchen, die hier wirksam werden könnten.

Fußnoten

1 - Auf die geleakten Pegasus-Daten hatten zuerst Forbidden Stories und Amnesty International Zugriff, die ein internationales Konsortium von 80 Journalist*innen aus 17 Ländern einbezogen; in der BRD gehören dazu ZEIT, Süddeutscher Zeitung, NDR und WDR *(vgl. Biermann 2021; Kirchgaessner et al. 2021; ZEIT 2021)*.

2 - „Zero-Click"-Angriffe sind solche, die ein Einschleusen von Schadsoftware ohne Benutzer*inneninteraktion ermöglichen, wo also nicht einmal ein Link angeklickt werden muss, sondern Sicherheitslücken einer Anwendung genutzt werden, um über diese im Hintergrund das Programm herunterzuladen und zu installieren *(vgl. Becker 2021)*.

3 - Ein weiteres Beispiel ist das – der NSO Group angeschlossene – Spionageunternehmen „Circles", das Schwachstellen im globalen Telekommunikationsnetzwerk ausnutzt, um Anrufe, Textnachrichten und Informationen über Standorte der Opfer weltweit abzufangen. Dabei hinterlässt seine Technologie im Gegensatz zu Pegasus keine auf den Geräten erkennbaren Spuren *(vgl. Marczak u. a. 2020)*.

4 - Marczak et al. *(2020)* führen im „Citizen Lab Research Report No. 133" eine Reihe von Empfehlungen für konkrete technische und politische Maßnahmen auf, die zum Schutz der Telekommunikationsnetzwerke international vorgenommen werden sollten.

5 - Interessant könnten dabei communitybasierte Geschäftsmodelle wie „HackerOne" sein, welches eine Plattform für Hacker*innen sein möchte, die „Gutes" tun wollen, und eine Schnittstelle zu Hard- und Softwareherstellern bildet, um IT-Security zu testen, Schwachstellen zu finden und Lösungen anzubieten *(siehe https://www.hackerone.com)*. 2016 rief das US-amerikanische Verteidigungsministerium in Kooperation mit HackerOne zu einem Wettbewerb „Hack the Pentagon" auf *(vgl. DoD 2016)*.

Literaturangaben zu den im Text referenzierten Veröffentlichungen finden sich in der Onlinefassung des Artikels auf der Internetseite des grünen blatts.