PROJEKTSKIZZE ZUM SECURITY-LAB / AMNESTY TECH

Danke für Ihr Interesse am Schutz der Menschenrechte im digitalen Zeitalter.
Lesezeit 4 Min.

AMNESTY INTERNATIONAL

DAS SECURITY LAB VON AMNESTY TECH

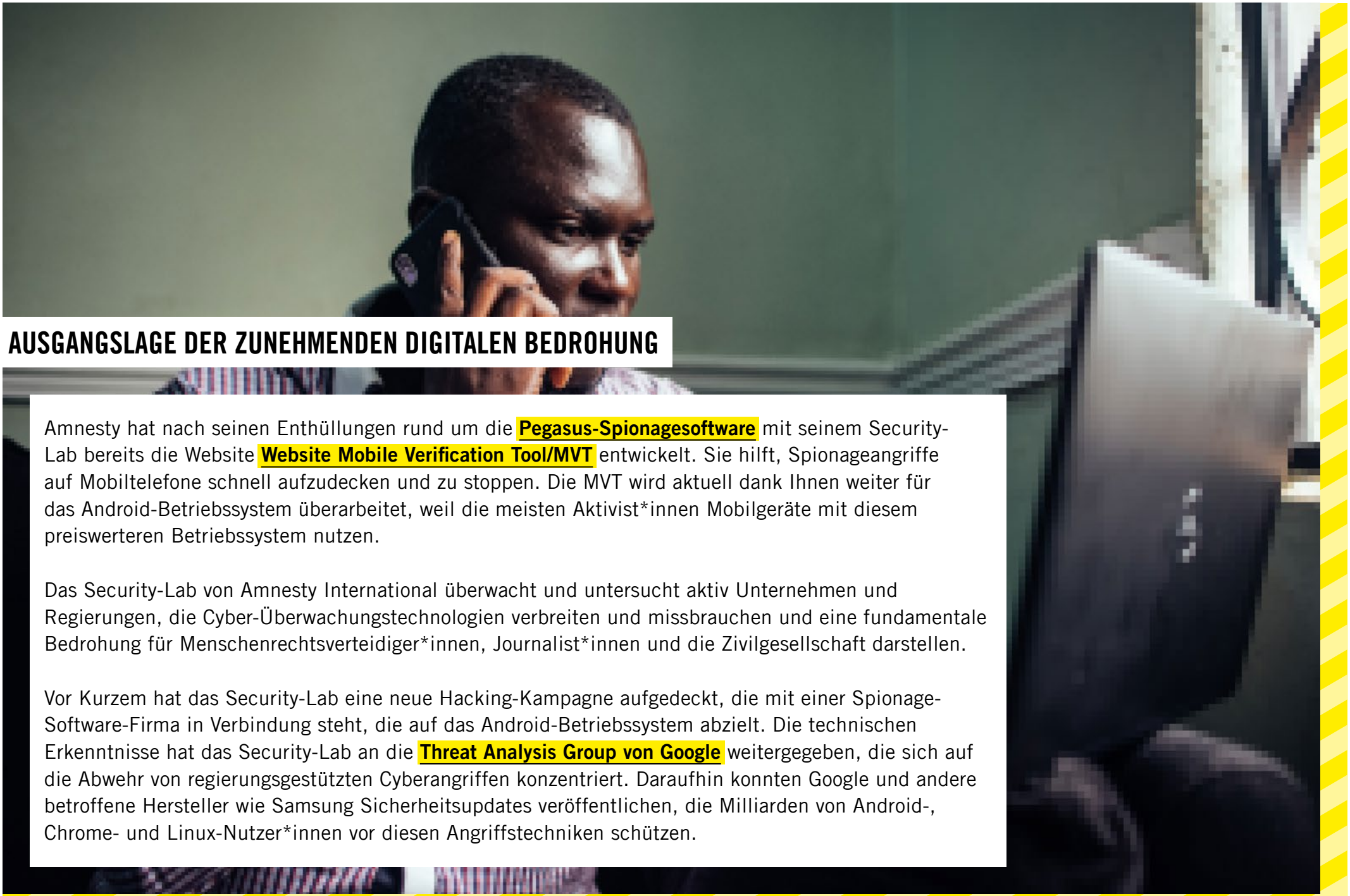
Liebe Leser*in,

herzlichen Dank für Ihre Tatkraft, Entschlossenheit und Ihren Pioniergeist. Denn Sie wollen mit Amnesty neue Bereiche betreten, um den Schutz der Menschenwürde in unserem Alltag zu verankern.

Heute geht es um den Schutz der Würde und Privatsphäre von Human Rights Defenders im digitalen Zeitalter. Denn unterdrückerische Staaten wie Weißrussland oder Indonesien ruhen nicht, digitale Wege zu finden und auszuweiten, um mutige Menschenrechtsaktivist*innen seelisch zu zerstören, mundtot zu machen und aus der Öffentlichkeit zu verdrängen.

Dazu hat das Security-Lab von Amnesty bereits eine Software entwickelt, die digitale Spionageangriffe gegen Human Rights Defenders aufdeckt. Darüber hinaus schützt die sehr spezifische Lobby- und Kampagnenarbeit vom Security-Lab die Persönlichkeitsrechte von Menschenrechtsverteidiger* innen ganzheitlich.

Diesen notwendigen Schutz für die Aktivist*innen wollen wir gern mit Ihnen gemeinsam ausbauen. Denn wir trauen Ihnen den Mut für derart innovative und gleichzeitig notwendige Schutzmaßnahmen zu. Entsprechen erhalten Sie heute den passenden Projektantrag zum Security-Lab von Amnesty, das weiter unter Hochdruck arbeitet.



AUSGANGSLAGE DER ZUNEHMENDEN DIGITALEN BEDROHUNG

Amnesty hat nach seinen Enthüllungen rund um die **Pegasus-Spionagesoftware** mit seinem Security-Lab bereits die Website **Website Mobile Verification Tool/MVT** entwickelt. Sie hilft, Spionageangriffe auf Mobiltelefone schnell aufzudecken und zu stoppen. Die MVT wird aktuell dank Ihnen weiter für das Android-Betriebssystem überarbeitet, weil die meisten Aktivist*innen Mobilgeräte mit diesem preiswerteren Betriebssystem nutzen.

Das Security-Lab von Amnesty International überwacht und untersucht aktiv Unternehmen und Regierungen, die Cyber-Überwachungstechnologien verbreiten und missbrauchen und eine fundamentale Bedrohung für Menschenrechtsverteidiger*innen, Journalist*innen und die Zivilgesellschaft darstellen.

Vor Kurzem hat das Security-Lab eine neue Hacking-Kampagne aufgedeckt, die mit einer Spionage-Software-Firma in Verbindung steht, die auf das Android-Betriebssystem abzielt. Die technischen Erkenntnisse hat das Security-Lab an die **Threat Analysis Group von Google** weitergegeben, die sich auf die Abwehr von regierungsgestützten Cyberangriffen konzentriert. Daraufhin konnten Google und andere betroffene Hersteller wie Samsung Sicherheitsupdates veröffentlichen, die Milliarden von Android-, Chrome- und Linux-Nutzer*innen vor diesen Angriffstechniken schützen.

Dank der Erkenntnisse des Security-Labs konnte Google im Dezember 2022 eine neue **Zero-Day-Exploit**-Kette aufdecken, die zum Hacken von Android-Geräten verwendet wird. Mit Zero-Day-Exploits wird die Ausnutzung einer Schwachstelle bezeichnet, die nur der Person bekannt ist, die diese Schwachstelle entdeckt hat. Die Nutzer*innen und insbesondere die Produktionsunternehmen erlangen in der Regel erst dann Kenntnis von der Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle aufbauen. Das Produktionsunternehmen hat somit keine Zeit, seine Nutzer*innen vor den ersten Angriffen zu schützen. Über Zero-Day-Exploits können sogar vollständig nachgerüstete mobile Endgeräte angegriffen werden.

Die neu entdeckte Spyware-Kampagne ist seit mindestens 2020 aktiv und zielt auf Mobile- und Desktop-Geräte ab. Die Spyware und die Zero-Day-Exploits wurden über ein umfangreiches Netzwerk von mehr als 1.000 bösartigen Domains verbreitet, darunter auch Domains, die Medien-Websites in mehreren Ländern vortäuschen.

LÖSUNGSANSATZ VON AMNESTY

Amnesty hat Einzelheiten zu den Domains und der Infrastruktur, die mit dem Angriff auf GitHub in Verbindung gebracht werden, veröffentlicht, um die Zivilgesellschaft bei der Untersuchung und Reaktion auf diese Angriffe zu unterstützen.

Das Security-Lab hat weitere Aktivitäten im Zusammenhang mit dieser Spyware-Kampagne in Indonesien, Weißrussland, den Vereinigten Arabischen Emiraten und Italien festgestellt. Diese Länder stellen wahrscheinlich nur eine kleine Teilmenge der gesamten Angriffskampagne dar, weil die Angriffsinfrastruktur sehr umfangreich ist.

Die Vision von Amnesty ist ein lebendiger und wachsender städtischer Raum, der frei von unrechtmäßiger Überwachung ist.

Die Ziele für 2023 sind:

1. Politik: Weitere politische Impulse für ein weltweites Moratorium über Ausfuhr, Verkauf, Weitergabe und Einsatz von Überwachungstechnologien, gestützt durch Kampagnenarbeit. Fortschritte bei der Gewährleistung eines menschenrechtskonformen Rechtsrahmens.

2. Forschung: Gute Berichterstattung über neue, mit Partner*innen erbrachte Forschungsergebnisse in einflussreichen Medien. Untersuchungen und Studien in Nord- und Südamerika, insbesondere zu geschlechtsspezifischen Auswirkungen der Überwachung.

3. Zurüstung Zivilgesellschaft: Zweites Digital-Fellowship-Programm als Training von zivilgesellschaftlichen Organisationen, Einzelpersonen und Amnesty-Mitarbeiter*innen für ihre eigenständigen forensischen Untersuchungen von rechtswidriger Überwachung.

4. Ausbau der Kapazitäten: Kapazitäten für Lobbyarbeit und technische Herausforderungen zum einen und Strukturen für Zusammenarbeit mit Sektionen, Regionalbüros und anderen Teilen der Amnesty-Bewegung zum anderen.

KOSTEN- UND FINANZIERUNGSPLAN 2023

KOSTENPLAN
SECURITY LAB

Personalkosten	
Fixe Personalkosten	305.000 Euro
Sonstige Personalkosten	5.000 Euro
Reisekosten	10.000 Euro
Strukturelle Aufwendungen	
Miete	5.000 Euro
Hardware	8.000 Euro
Porti, Telefon, sonstige Kosten	2.000 Euro
Gesamtkosten	**335.000 Euro**

FINANZIERUNGSPLAN
SECURITY LAB

Noch offen	20.000 Euro
Spende Stiftung Menschenrechte in Aussicht gestellt	35.000 Euro
Eigenmittel Amnesty International Deutschland liegt vor	192.000 Euro
Internationales Sekretariat Amnesty London liegt vor	88.000 Euro
Gesamteinnahmen	**335.000 Euro**

Deshalb bitten wir Sie, sich mit einem vier- bis fünfstelligen Betrag für den Schutz der Human Rights Defenders im digitalen Zeitalter einzusetzen.

Liebe Leser*in,
Ihre Unterstützung für den digitalen Schutz von Human Rights Defenders ist hochwillkommen und sehr wertvoll.

Wie sagt Ihnen die Stoßrichtung vom Security-Lab mit seiner ganz praktischen Hilfe wie auch rechtlichen Lobby- und Kampagnenarbeit zu?

Wir freuen uns, Menschen mit Pioniergeist wie Sie an unserer Seite zu haben.
Für Fragen stehe ich Ihnen gern zur Verfügung.

Herzlich
Ihre

Alexandra Ripken

AMNESTY INTERNATIONAL Deutschland e. V.
Zinnowitzer Straße 8 . 10115 Berlin
T: +49 171 5568796 . E: alexandra.ripken@amnesty.de

AMNESTY INTERNATIONAL