

DIE UNIVERSELLE BIOMETRISCH-DIGITALE MARKIERUNG ALLER ERDENBÜRGER WIRD WAHR | VON NORBERT HÄRING

Posted on 15. November 2023

*Ein Kommentar von **Norbert Häring**.*

Zur gleichen Zeit, in der bekannt wird, dass Hacker die Identitätsdaten der meisten Inder aus der größten staatlichen Identitätsdatenbank der Welt zum Kauf anbieten, einigen sich EU-Parlament und -Rat darauf, so etwas auch für uns einzuführen, Gleichzeitig preist Washington die ukrainische Version als Exportmodell an und Bill Gates will jedem neugeborenen Kind in Kenia so eine biometrisch-digitale Markierung auf Lebenszeit aufdrängen. Das hat System [<1>](#).

Anfang Oktober machte die IT-Sicherheitsfirma Resecurity bekannt [<2>](#), das Hacker nach eigenen Angaben die biometrischen Identitätsdaten von über 800 Millionen Indern aus der staatlichen Datenbank Aadhaar gestohlen haben und relativ günstig zum Kauf anbieten. Nachforschungen von Sicherheitsexperten zeigen, dass die Behauptung zumindest im Kern stimmt, wenn auch die Anzahl der Betroffenen nicht zu verifizieren ist. Resecurity erwarb 400.000 Datensätze und verifizierte deren Authentizität. Die Betroffenen waren von der unbekannten Organisation, deren Daten gestohlen wurden, nicht von dem Diebstahl informiert worden und wussten von nichts. Die Daten sollen neben der Aadhaar-Nummer den Namen und den Namen des Vaters, die Adresse, Passnummer, Alter und Geschlecht beinhalten.

Nach Angaben von Rescurity können etwaige Käufer mit diesen Daten Online-Bankkonten der Betroffenen plündern und Steuerrückerstattungsbetrug zu deren Lasten begehen.

Der Vorfall zeigt die riesigen Probleme für den Schutz der Bürgerrechte, die mit einer solchen Datenbank verbunden sind, deren Daten für alle nur denkbaren Identifikationszwecke verwendet werden. Die Versicherungen, das System sei sicher, haben sich nicht zum ersten Mal als grob falsch herausgestellt. Das Sicherheitsniveau wird von der Plattform mit Zugang zu den Daten bestimmt, die das wenigste Know How hat und den schlampigsten Umgang mit den Daten pflegt. In diesem Fall ist das Einfallstor für den Datendiebstahl unbekannt. In anderen, ebenfalls sehr großen Fällen in diesem Jahr soll das Einfallstor die Datenbank von Covid-Tests des Indian Council of Medical Research (ICMR) gewesen sein, die mit den Aadhaar-Nummern der Getesteten verbunden ist, sowie eine Datenbank zur Identifizierung von Prepaid-

Telefonkunden.

Wenn die gleiche Datenbank von sehr vielen Behörden und Anbietern für alle möglichen Zwecke genutzt wird, multipliziert sich dadurch nicht nur das Risiko von Datenverlust, sondern auch der Schaden für die Betroffenen. Wenn dann auch noch die für die biometrische Identifikation genutzten Daten gestohlen werden, im Fall Aadhaar Fingerabdrücke und Iris-Scans, steht dem umfassenden Identitätsdiebstahl nichts mehr im Wege. Da Lesegeräte für biometrische Daten überall genutzt werden, um die Identität zu prüfen, können Kriminelle relativ leicht an solche Daten kommen. Da man seine biometrischen Merkmale nicht wie ein Passwort ändern kann, ist das verheerend für die Betroffenen.

Die indische Regierung behauptet, es sei freiwillig, sich in der Datenbank registrieren zu lassen. Das ist etwa so wahr, wie die Covid-Impfung für Beschäftigte im deutschen Gesundheitssystem „freiwillig“ war. Alle möglichen staatlichen Leistungen setzen eine Registrierung voraus und so viele private Anbieter nutzen das System, dass eine Nichtregistrierung für Menschen, die nicht autark auf dem Land leben, mit sehr großen Nachteilen verbunden ist.

Europas Aadhaar heißt Digital Identity Wallet

Völlig unbeirrt von diesen hier ohnehin so gut wie nicht berichteten Vorkommnissen im Vorreiter Indien, gaben EU-Rat und EU-Parlament am 8.11. die Einigung [<3>](#) auf eine Verordnung bekannt, die von allen EU-Ländern verlangt Digital Identity Wallets, digitale Identitäts-Brieftaschen, nach einheitlichem Format anzubieten. Natürlich, wie in Indien völlig freiwillig für die Bürger und nur zu deren Nutzen, damit sie sich bei Behörden und privaten Anbietern überall leicht und schnell mit den immer gleichen Identifikationsdaten anmelden können. Natürlich soll diese Datenbank 100% sicher sein, die Daten unmöglich gehackt werden können und auf keinen Fall von Behörden zu Überwachungszwecken missbraucht werden. Wer es glaubt, wird selig.

Es ist nicht bekannt, dass es große Unzufriedenheit in der Bevölkerung damit gegeben hätte, dass sie nicht über eine derartige, vom Staat kontrollierte digitale Identität verfügen. Hier wird im Interesse der global agierenden US-Konzerne wie Microsoft und Google und der Überwachungsagenda Washingtons und der

anderen beteiligten Regierungen gezielt (siehe „Mehr“ unten) ein weltumspannendes System errichtet, das alle Menschen unentrinnbar an das computerisiert überwachte Netz anbindet. Damit sollen immer mehr und schließlich alle ihre Aktivitäten überwachbar und steuerbar werden. Vorangetrieben wird das maßgeblich von Weltwirtschaftsforum, Gates-Stiftung und Rockefeller-Stiftung, mit Unterstützung Washingtons und von Washington kontrollierter internationaler Organisationen.

Bei all diesen staatlichen Identitätsdatenbanken in Indien [<4>](#), Europa und Afrika, weiß man, oder darf getrost davon ausgehen, dass die großen US-IT-Konzerne ihre Finger im Spiel haben und der Geheimdienst NSA Zugang hat.

Ukraines Dija als Exportmodell, Kenia als Importeur

Auch in der Ukraine gibt es eine mit offizieller US-Unterstützung eingeführte, umfassend genutzte staatliche Identitätsdatenbank namens Dija (engl. Übertragung aus dem Kyrillischen: „Diia“). Diese wird, ebenso wie das indische Vorbild, systematisch anderen Ländern zu Nachahmung angetragen und ihnen in modularer Form zur Verfügung gestellt. Der zuständige Digitalisierungsminister, Mykhailo Fedorov, ist ein Young Global Leader des Weltwirtschaftsforums. Das Branchenmagazin Biometric Update berichtet [<5>](#):

„Rund 70 Prozent der Bürgerinnen und Bürger verfügen inzwischen über die digitale ID, die zur Speicherung von biometrischen Pässen, Steuer-IDs und Führerscheinen, für den Zugang zu öffentlichen Dienstleistungen und sogar für den Austausch militärischer Informationen genutzt wird: Nutzer können über die App die geografische Position feindlicher Panzer übermitteln. Diia wurde 2019 ins Leben gerufen. Seit Russland 2022 eine Invasion des Landes startete, hat die App neue Dienste hinzugefügt. Dazu gehört die Ausstellung eines digitalen „Evakuierungsdokuments“, das Identitätsinformationen enthält, um die Abfertigung an Kontrollpunkten zu beschleunigen, und das es Bürgern, deren Häuser im Krieg beschädigt wurden, ermöglicht, eine Entschädigung zu beantragen. Das Diia-Projekt, das in Zusammenarbeit mit USAID, der Eurasia Foundation und Partnern aus dem Privatsektor ins Leben gerufen wurde, stößt auch in anderen Ländern, die von den Erfahrungen der Ukraine lernen, auf Interesse. Im Januar dieses Jahres kündigte USAID an, Partnerländer zu unterstützen, die sich von Diia

inspirieren lassen.“

Folgendes hat, passend dazu, vor Kurzem die Kenyan Post berichtet [<6>](#) (übersetzt):

„Die Bill and Melinda Gates Foundation hat mit der kenianischen Regierung eine Vereinbarung getroffen, um sie bei der geplanten Einführung des digitalen Identifikationsdokuments (ID) mit dem Namen Maisha Namba zu beraten. Maisha Namba wird der Personalausweis der dritten Generation mit einer eindeutigen Nummer sein, die jedem Kenianer bei der Geburt zugewiesen wird und von der Geburt bis zum Tod gilt. Der Geschäftsführer der Stiftung, Mark Suzman, sagte einer lokalen Zeitung: „Wir haben eine Reihe spezifischer Investitionshilfen für die digitale Identität, die wir breiteren Plattformen zur Verfügung stellen.“ Der Milliardär hat sich mit [Regierungschef] Ruto mehrfach getroffen, seit dieser an die Macht gekommen ist, wobei die meisten dieser Begegnungen geheim gehalten wurden. Berichten zufolge wird das Abkommen die Regierung mit wichtigen technischen Experten und Partnern zusammenbringen, die professionelle Beratung anbieten werden, um eine reibungslose Einführung zu gewährleisten.“

Wie Sie den folgenden Beispielen entnehmen können, werden die biometrisch-digitalen Identitätsdatenbanken nach indischem Vorbild in viele andere Länder exportiert, darunter Nigeria, Äthiopien und Kasachstan. Aber auch weitere, unten nicht aufgeführte asiatische Länder wie Pakistan und Thailand sind dabei. Es fehlt nicht mehr viel, dann können die US-Dienste von ihren Computern in Langley und Fort Meade aus mitverfolgen und speichern, was fast jeder beliebige Erdenbürger (außerhalb Chinas) so macht.

Quellen

<1> <https://norberthaering.de/macht-kontrolle/washington-diia/>

<2>

<https://www.resecurity.com/blog/article/pii-belonging-to-indian-citizens-including-their-aadhaar-ids-offered-for-sale-on-the-dark-web?s=08>

<3>

<https://www.consilium.europa.eu/en/press/press-releases/2023/11/08/european-digital-identity-council-and-parliament-reach-a-provisional-agreement-on-eid/>

<4> <https://norberthaering.de/macht-kontrolle/indien-ueberwachungsstaat-biz-augustin-carstens/>

<5>

<https://www.biometricupdate.com/202310/ukraines-digital-identity-app-growing-and-becoming-an-inspiration-for-other-countries>

<6>

<https://kenyan-post.com/2023/10/bill-gates-lands-a-lucrative-deal-just-after-meeting-ruto-see-what-he-will-be-doing-for-the-president-and-his-government/>

+++

Dank an den Autor für das Recht zur Veröffentlichung des Beitrags.

+++

Dieser Beitrag erschien zuerst am 10. November 2023 bei norberthaering.de

+++

Bildquelle: [Trismegist san](#) / shutterstock