Bedenkliche Zertifikate

Corona-Selbsttests von Aldi: Online-Zertifikate wertlos

Geht es nach dem Test-Hersteller Aesku, könnten online ausgestellte Negativbescheinigungen der Türöffner für öffentliches Leben werden. Doch die zugehörige Web-App war nicht nur anfällig für Betrug, c't fand auch ein veritables Datenleck.

Von Jan Mahn

Als Bonus zu den Corona-Selbsttests des Herstellers Aesku, die bei Aldi an der Kasse erhältlich sind, gibt es auch eine Online-Funktion. Wer sich getestet hat, kann sich über einen QR-Code auf der Packung bis zu fünf Negativ-Zertifikate ausstellen lassen. Die Idee von Aesku: Solche vom Hersteller ausgegebenen Zertifikate sollen der Schlüssel für Friseur- und Restaurantbesuche sowie Veranstaltungen werden. Doch unsere Untersuchung zeigt, dass nicht nur die Grundidee fragwürdig ist. Fehler in der technischen Umsetzung machten die Zertifikate faktisch wertlos und verursachten darüber hinaus ein Datenleck.

Die erste Schwachstelle des Zertifikatesystems von Aesku: Auf der 5er-Packung der Selbsttests befindet sich von außen sichtbar ein QR-Code, über den man auf der Website ichtestemichselbst.de bis zu fünf Negativ-Bescheinigungen abrufen kann. Dazu muss man nur anklicken, dass man sich selbst negativ getestet hat. Anschließend hinterlegt man die eigene Personalausweis- oder Führerscheinnummer und bekommt die PDF-Datei mit dem Zertifikat.

Dabei verwendete Aesku in der Download-URL als einziges variables Element das Erstellungsdatum des Zertifikats in Form eines Unix-Timestamps, also der Anzahl der Sekunden, die seit Neujahr 1970 vergangen sind. Indem wir die Sekunden rückwärts zählten, gelang es uns per Skript, fremde Zertifikate herunterzuladen. Nach nur wenigen Stunden hatten wir so über hundert PDF-Dateien heruntergeladen.

So gelangten wir an etliche Personalausweis- und Führerscheinnummern – weil die Nutzer in das Freitextfeld alles Mögliche eingeben konnten, waren auch Namen darunter.

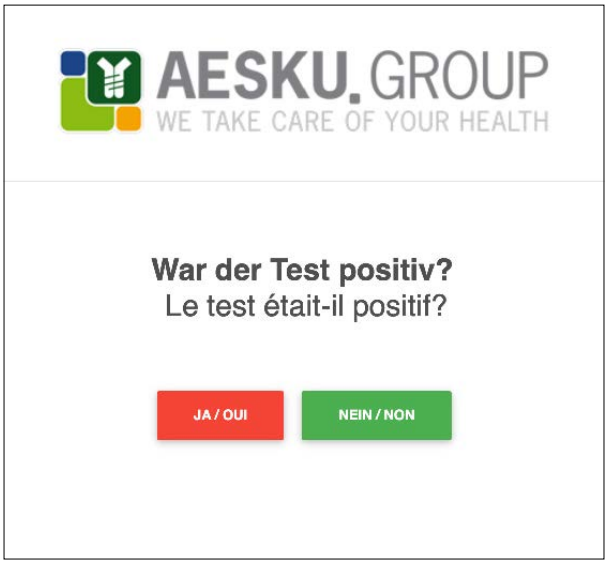
Zertifikate vermehren

Doch damit noch nicht genug. Eine Untersuchung der PDF-Zertifikate, die man auf dem Smartphone speichern oder ausgedruckt etwa zum Friseur mitnehmen soll, offenbarte ein weiteres Problem: Der darin verwendete QR-Code, über den man die Gültigkeit online prüfen kann, enthält auch den Code, der sonst nur auf der Packung aufgedruckt ist. Wer also das Zertifikat in die Hand bekommt, kann das Kontingent an Online-Zertifizierungen für die 5er-Schachtel aufbrauchen und sich bis zu vier weitere Zertifikate ausstellen.

Nach unserem Hinweis dichtete das Unternehmen das Datenleck zunächst ab und ersetzte den Unix-Timestamp durch eine 32 Bit lange ID, offenbar ein Hash, der nicht mehr zu erraten ist. Den Fall stufte der externe Datenschutzbeauftragte des Herstellers als meldepflichtigen Vorfall im Sinne der DSGVO ein und informierte den zuständigen Landesdatenschutzbeauftragten.

Die notdürftigen Reparaturen ändern aber nichts daran, dass man weiterhin von den Packungen etwa im Laden oder über die Zertifikate an die Packungs-ID herankommt, außerdem bietet die Online-Selbstzertifizierung keinerlei Schutz vor Missbrauch. Wie der Hersteller selbst schreibt, basiert das Verfahren auf Vertrauen. Die hemdsärmelig entwickelte Online-Vergabe der Zertifikate von Aesku trägt aber nicht gerade zur Vertrauensbildung bei. Technisch fanden wir ein System auf dem Stand eines frühen Prototypen vor.

Von den Online-Pannen nicht betroffen ist die Offline-Funktionalität der Tests. Für die reine Selbstkontrolle angewandt, können die durchaus ihren Zweck erfüllen. Als Eintrittskarte zum öffentlichen Leben taugte das Verfahren aber nicht. Vier Tage nach unserem Hinweis entschied sich Aesku dann um und stellte die Funktion zum Generieren von Online-Zertifikaten ab. *(jam@ct.de)* c't



Die Online-Zertifikatserstellung bei Aesku basiert auf Vertrauen. Wenn man sich selbst getestet hat, wird man gebeten, die Frage nach dem Testergebnis wahrheitsgemäß zu beantworten.