OZG

Verpasste Chance für mehr IT-Sicherheit?

[19.05.2022] Den Security-by-Design-Ansatz hat das OZG nicht beschrieben, eine Verordnung zur Sicherung der eingesetzten IT trat erst 2022 in Kraft. Dabei verarbeitet gerade die Verwaltung besonders sensible Daten. Behörden sollten die Bürgerkommunikation deshalb von sich aus durchgängig verschlüsseln. Ein Kommentar von FTAPI-COO Ari Albertini.

Noch bis Ende 2022 haben deutsche Behörden Zeit, die Anforderungen des Onlinezugangsgesetzes (OZG) fristgerecht umzusetzen. In sechs Monaten müssten also quasi alle Verwaltungsleistungen digitalisiert sein. Erlassen wurde das Gesetz bereits im Jahr 2017. Zu diesem Zeitpunkt wurden auch die rund 600 Leistungen definiert, die den Bürgerinnen und Bürgern zukünftig digital angeboten werden sollen. Das ehrgeizige Ziel ist eine moderne Verwaltung, die sowohl durchgängig digitalisiert als auch nutzerfreundlich im Sinne der Bürgerinnen und Bürger ist. Eine moderne Verwaltung ist allerdings nicht automatisch eine sichere Verwaltung. Denn was Bund und Länder zwar bedacht, nicht aber in den Mittelpunkt des Transformationsvorhabens gestellt haben, ist das Thema Sicherheit. Dabei wäre die OZG-Einführung ein guter Zeitpunkt gewesen, um mit der flächendeckenden Verschlüsselungspflicht eines der größten Einfallstore vor Cyber-Kriminellen zu verschließen.

IT-Sicherheit erst im Nachklapp

Das Gesetz zur Verbesserung des Online-Zugangs zu Verwaltungsleistungen wurde 2017 erlassen, eine entsprechende Verordnung zur Sicherheit der eingesetzten IT-Komponenten trat jedoch erst im Januar 2022 in Kraft. Zu diesem Zeitpunkt war die Entwicklung zahlreicher Lösungen allerdings bereits in vollem Gange. Aufgrund der nachträglichen Verordnung müssen verschiedene Technologieanbieter ihre Produkte nun entsprechend nachrüsten. Dass Ansätze wie Security by Design, also das Mitdenken der Sicherheit schon bei der Entwicklung von Lösungen, beim OZG nicht zur Anwendung kamen, wird von Experten zum Teil stark kritisiert. Dabei empfiehlt sogar das Bundesamt für Sicherheit in der Informationstechnik (BSI) im jährlichen Bericht zur Lage der IT-Sicherheit in Deutschland, Anforderungen an die Informationssicherheit bereits bei der Entwicklung eines Produkts zu berücksichtigen. Umso mehr gilt das für Bereiche, in denen personenbezogene und damit äußerst sensible Daten übermittelt und verarbeitet werden und ein entsprechender Schutz einen besonderen Stellenwert hat. Mit ebensolche Daten arbeiten die digitalisierten Verwaltungsleistungen.

Bürgerkommunikation per se verschlüsseln

Ob eine Verschlüsselung gesetzlich gefordert wird oder nicht, Behörden sollten alle Kanäle, die für die Bürgerkommunikation wichtig sind, absichern. Denn seien es Personalausweise, Geburtsurkunden oder Führungszeugnisse – gelangen diese Unterlagen in die falschen Händen, kann das großen Schaden verursachen. Aus diesem Grund sollten Länder und Kommunen solche OZG-Lösungen auswählen, die eine durchgängige Verschlüsselung erlauben. Das gilt sowohl für die Übertragung von Daten und Dokumenten als auch für die alltägliche Behördenkommunikation. Die Bürgerinnen und Bürger können sich dann sicher sein, dass der Schutz ihrer Daten ernst genommen wird und sie den Komfort des digitalen Amts guten Gewissens nutzen können.

()

Stichwörter: IT-Sicherheit, OZG, FTAPI Software