DATABUND

Bundesverband der mittelständischen IT- Dienstleister und Softwarehersteller für den öffentlichen Sektor e. V.

Stellungnahme zur BSI Richtlinie “BSI TR-03172-3 Onlinedienst”

Aus Sicht des DATABUND e.V. ist das Bemühen um eine sichere Infrastruktur bei Online-Diensten angesichts der Bedrohungen, denen diese mittlerweile ausgesetzt sind, zu begrüßen. Unsichere Dienste führen dazu, dass das Vertrauen in E-Government-Anwendungen schwindet und damit ein wichtiger Eckpfeiler für eine Digitale Verwaltung gefährdet wird.

Allerdings sind wir über den Ansatz der BSI TR-03172-3 verwundert. Die BSI Grundschutzmethodik ist ein seit Jahren etablierter und erprobter Standard, der auch bei Online-Diensten im Portalverbund angewandt werden sollte. Im vorgenannten Papier werden Methoden aus den Grundschutzkatalogen entnommen, zu einem scheinbaren “Sicherheitskonzept” zusammengesetzt und pauschale Anforderungen gestellt. Diese Anforderungen sind an vielen Stellen teils allgemein, unklar oder interpretationsfähig bis schwammig formuliert, teils fordern sie technische Vorgehensweisen oder Verfahren, die kaum oder nur mit erheblichem Aufwand umzusetzen sind. Dies gefährdet die effiziente, erfolgreiche und sichere Umsetzung von Online-Diensten.

Ein unbedingt diskussionsbedürftiger Punkt ist unter anderem eine an verschiedenen Stellen pauschal geforderte Verschlüsselung, die Aspekte realistischen Schlüsselmanagements und realistischer Schutzziele außer Acht lässt; die Forderung nach Deaktivierung der Autovervollständigung, was etablierten und von zahlreichen internationalen Experten bestätigten Sicherheitspraktiken widerspricht; pauschale Anforderungen hinsichtlich Absicherung gegen missbräuchliche Nutzung durch die Administration und vieles mehr.

Im Entwurf der vorliegenden Richtlinie finden sich leider sehr viele solcher undifferenzierter Anforderungen, die teilweise der BSI Grundschutzmethodik widersprechen.

Das Papier sollte daher nicht in dieser Form veröffentlicht werden, da

- durch eine undifferenzierte Forderung von Sicherheitsmethoden der Aufwand unverhältnismäßig steigt und die Umsetzungskosten und Umsetzungsdauer von Online-Diensten steigt;
- bestimmte Anforderungen wenig praktikabel oder gar undurchführbar sind, da sie die Realität der Software-Entwicklung nicht berücksichtigen;

- durch pauschale, undifferenzierte Anforderungen viele Unklarheiten entstehen (“es muss verschlüsselt werden”), die dann in den einzelnen Umsetzungsprojekten aufwändig geklärt werden müssen und zu Konflikten führen;
- durch viele Referenzierungen im Dokument eine völlig unklare Anforderungslage entsteht;
- die Richtlinie vermutlich pauschal und unreflektiert als Anforderungsdokument herangezogen wird, wie das in der Vergangenheit bei Technischen Richtlinien leider häufig zu beobachten war;
- das Papier eine scheinbar einfache Lösung für ein komplexes Problem bietet, aber die Grundschutzmethodik selbst und damit ein bewährtes Vorgehensmodell außer Acht lässt. Insbesondere widerspricht sich das Papier in sich selbst, da es einerseits die Grundschutzmethodik fordert, andererseits aber konkrete Methoden ohne vorherige Schutzbedarfsbetrachtung vorschreibt.

Statt dessen sollte in einer Richtlinie Handlungsempfehlungen gegeben werden, wie die Grundschutzmethodik effizient und zielgerichtet auf Online-Dienste des Portalverbundes angewendet werden kann.

Berlin, den 15.12.2023

Der DATABUND-Vorstand