Antworten der Referenten Katharina Raabe-Stuppnig und Armin Simon auf Fragen der Teilnehmer, die während der Live-Sendung aus Zeitgründen nicht beantwortet werden konnten:

(chronologisch aufgeführt; alle Fragen im Original-Wortlaut)

Frage 1:

Bereits schon mehrfach diskutiert: Frage an Sie Herr Simon: Eine Cloud-Anwendung, die unbedingt eine Data-in-Motion-Verschlüsselung erfordert (da ständig "live" Modifikationen an den Daten vorgenommen werden). Sprich externes Key Mgm ist nicht möglich. Dies ist und bleibt also ein Problem, wenn die Daten bei einem US-Konzern liegen, richtig?

Nachdem US-Konzerne, gemäß FISA 702, Daten herausgeben, muss das „Zero Knowledge"-Prinzip umgesetzt werden.

Verschlüsselung ist ein probates Mittel, wenn die Schlüssel ausschließlich unter der Kontrolle des Datenexporteurs oder einer vom Exporteur vertrauenswürdigen Stelle im EWR sind. Es muss dabei sichergestellt werden, dass der US-Konzern keinen Zugang zu den Daten im Klartext hat. Genau ein solches Szenario wurde in einem Urteil in Frankreich als ausreichend festgestellt: https://www.conseil-etat.fr/en/news/the-urgent-applications-judge-does-not-suspend-the-partnership-between-the-ministry-of-health-and-doctolib-for-the-management-of-covid-19-vaccinati

THALES bietet Verschlüsselungsmöglichkeiten, die dies gewährleisten.

Frage 2:

Gibt es zu diesem Verschlüsselungszusammenhang ein White-Paper oder etwas zum Einlesen, denn in unserer Org. gibt es keine Fachleute dafür. Als DSB muss ich solche techn. Info nachweisen, um gehört zu werden.

Ja – steht auf der Thales-Webseite zur Verfügung:
https://cpl.thalesgroup.com/de/resources/encryption/securing-access-to-data-in-a-post-schrems-ii-era-white-paper

Frage 3:

SGX wurde doch auch schon erfolgreich angegriffen, oder nicht?

Ja, es gab nicht nur bei SGX, sondern bei den Implementierungen aller Prozessoranbieter Schwachstellen, Sicherheitspatches und weiterentwickelte Versionen, welche Lücken geschlossen haben. Ein weiteres Beispiel dafür, dass Sicherheit ein relativer Zustand der

Gefahrenfreiheit ist. Man kann zwar prinzipiell „sicher“ sein, ein Restrisiko, so klein es auch sein mag, bleibt bestehen.

Solche Schutzmaßnahmen werden den Forderungen des EDSA nach Verschlüsselung und vom Provider getrennten Schlüsselmanagement gerecht und sind somit ein probates Mittel, „Compliance“ zu erreichen

Frage 4:

Besten Dank für die gute Diskussion! Es wurde gerade über MS Teams, DSGVO-Konformität und DSFA gesprochen. Gibt es Erfahrungen Ihrerseits mit den Aufsichtsbehörden für den Fall, dass der Verantwortliche Untersuchungen (DSFA) durchgeführt hat, TOM soweit wie möglich eingestellt hat? Wäre dann MS Teams (o.ä. Tools) immer noch nicht nutzbar? Soweit ich erinnere, darf auch eine wirtschaftliche Betrachtung und Anwenderfreundlichkeit etc. einfließen, wenn alternative (angeblich DSGVO-konforme) Tools gesucht werden.

Nein. Eine aktuelle Entscheidung der österreichischen Datenschutzbehörde hat gezeigt, dass die Ausführungen des EuGH im Rahmen von Schrems II sehr klar in die Datenschutzpraxis übertragen werden. In besagtem Fall wurden die ergänzenden Maßnahmen von Google als nicht effektiv angesehen, da keine Schließung der Rechtsschutzlücken in Bezug auf Zugriffs- und Überwachungsmöglichkeiten von US-Nachrichtendiensten gewährleistet war. Es ist davon auszugehen, dass die deutschen Datenschutzbehörden in vergleichbarer Weise agieren werden. Im Fall von Kontrollen sind natürlich DSFA und TOMs ein guter Anfang, jedoch – leider – für eine Schrems-II-Konformität in der Regel nicht ausreichend (weil, siehe oben, nicht „effektiv“) und somit verbunden mit erheblichem Restrisiko.

Frage 5:

Habe ich richtig verstanden, dass die DKE nicht geeignet ist das nötige Datenschutzniveau herzustellen?

Nein, DKE (Double Key Encryption) ist eine sehr gute Möglichkeit, Dokumente mit einem 2. Schlüssel so zu verschlüsseln, dass Microsoft die Dokumente nicht lesen kann und somit das „Zero Knowledge“-Prinzip hergestellt wird. Es ist jedoch darauf zu achten, dass die Schlüssel nicht in der Software liegen. Weitere Details finden Sie hier:
https://cpl.thalesgroup.com/cloud-security/encryption/double-key-encryption