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

(chronologisch aufgeführt; alle Fragen im Original-Wortlaut)

Frage 1:

Meines Wissens sagt beispielsweise AWS, man "bekenne" sich per AGB zu den Standardvertragsklauseln - erfüllt das die Vorgaben, da kein unterschriebenes Papier vorliegt?

Antwort von Herrn Simon:

Auch wenn wir hier keine Rechtsberatung bieten, lässt sich die Frage eindeutig beantworten. Die Standardvertragsklauseln erfordern eindeutig TOMs (Technische und Organisatorische Massnahmen) „… zur Gewährleistung des im Wesentlichen gleichwertigen Schutzniveau..." (wie im EWR). Diese TOMs müssen in Anhang II konkret beschrieben werden und lassen sich nicht durch AGBs regeln. AWS drückt möglicherweise damit aus, dass sie sich dazu bekennen, diese Vereinbarung mit Ihnen abzuschließen.

Frage 2:

Wenn die Schlüssel extern gehalten werden müssen, dann kann ich die Cloud nur als Storage nutzen. Denn um mit den Daten in der Cloud zu arbeiten, muss ich die Daten(-Streams) in dem Service / dem Node entschlüsseln. Dafür braucht es die Schlüssel zumindest in den Speicher laden.

Antwort von Herrn Simon:

Diese Frage wurde im weiteren Verlauf des Webcast beantwortet.

Frage 3:

Wie stellt sich das Thema Datenschutz bei Cloud-Telefonanlagen dar? Selbst wenn die Sprach-Daten (Echtzeit-Kommunikation) verschlüsselt werden, so gibt es ja immer noch die Verbindungsdaten, welche der (ggfs. amerikanische) SIP-Provider zur Rechnungslegung erfassen muss. Und genau diese Daten offenbaren eben, wer wann mit wem wie lange telefoniert und genau das führt ggfs. zu Sanktionen seitens Amerika. (Ähnliches gibt/gab es ja aktuell in Kanada im Zuge dieser Trucker-Demos).

Antwort von Herrn Simon:

Wie im Webcast erläutert, ist die große Herausforderung, „Segregation of Duties“ zu erreichen. Wir haben bereits Projekte durchgeführt, in denen Telefonnummer durch Tokenisierung pseudonymisiert und somit DSGVO-konform wurden.

Frage 4:

Es ist kaum vorstellbar, dass Verschlüsselung in der Hand des Kunden funktioniert. Außer wenn es um reine Speicherung von Daten in der Cloud geht.

Bei vielen Online Dienstleistern (z.B. bei Videokonferenzsystemen wie Zoom, Cisco, Adobe; multifunktionale Anwendungssysteme wie M365 mit einer vielzahl von Programmen, ZEN Desk, Atlassian Confluence und Jira, sowie viele weitere) bei denen explizit die personenbezogenen Daten mit den Anwendungen verarbeitet werden (Stichwort SAAS). Denn das hilft keine Verschlüsselung des Data at Rest und auch keine Transportverschlüsselung. Wie also soll eine Komplettverschlüsselung in der Hand des Verantwortlichen (also des Auftraggebers nach DSGVO Art. 4 Nr.7) funktionieren? Sobald Daten technisch bearbeitet werden müssen sie entschlüsselt werden!

Der EDSA hat das in seinen Empfehlungen 01/2021 v. 18.06.2022 in den Szenarien Nr. 6 und 7 dargestellt!

Letztlich werden doch technische Lösung vorgestellt, die ebenfalls von vorne herein nicht funktionieren können, weil es zu komplex ist dies zu implementieren.

Falls es doch einen Lösung gibt: Wie teuer würde so eine Lösung werden? Teurer als die Anwendung selbst?

Das wird sich kein Unternehmen, und v.a. keine öffentliche Einrichtung (Behörden, Schulen, Hochschulen, usw.) leisten können.

Antwort von Herrn Simon:

Auf viele dieser Punkte wurde im Laufe des Webcasts eingegangen. In der DSGVO wird an einigen Stellen auf den Einsatz von Verschlüsselung hingewiesen. Beim Einsatz von Verschlüsselung erreicht man Funktionstrennung durch die Schlüsselgewalt beim Verantwortlichen. Genau darauf bezieht sich der EDSA immer wieder in seinen Empfehlungen.

Die THALES-Lösungen sind absolut marktführend und bei tausenden Kunden weltweit verbreitet. Die modernen Systeme zur Verschlüsselung und insbesondere zum Key-Management haben die Komplexität deutlich reduziert und leicht beherrschbar gemacht. Bzgl. der Kosten lässt sich anmerken, dass diese idR bei 1 - 5 % der Cloud-Gebühren liegen.

Frage 5:

Zu Teams: Wie können die Verbindungsdaten - also wan wer mit wem kommuniziert hat - der DSGVO entsprechend gesichert werden? Denn diese Daten sind ja wiederum für das Billing erforderlich.

Antwort von Herrn Simon:

siehe Frage 3

Frage 6:

Kann die native Hyperscaler Verschlüsslung modular gewählt werden und ist das kommerziell ein Unterschied zu den Service Kosten der Hyperscaler?

Antwort von Herrn Simon:

Die Verschlüsselung der Hyperscaler ist ein sehr weites Feld. Ebenso die Lizenzierungspolitik. Somit lässt sich die Frage nicht einfach beantworten. Es lässt sich allerdings feststellen, dass es eine Vielzahl von Verschlüsselungsoptionen bei den Hyperscalern gibt und es sehr empfehlenswert ist, darauf zurückzugreifen. Allein schon um sich gegen Zugriffe von Dritten zu erwehren. Zur Erfüllung der Forderungen des EDSA genügen diese Maßnahmen allerdings nicht, solange das Schlüsselmaterial im Zugriff des Anbieters liegt. (erwähnter Use Case 6 in den Empfehlungen des EDSA)

Frage 7:

Was hilft denn eine technisch hochwertige Verschlüsselung und Schlüsselhoheit, wenn Geheimdienste wie z.B. die NSA technisch in der Lage sind, Verschlüsselungen zu "knacken" (auch im Kontext Quanten-Computing interessant)? Ist die EU da nicht sehr blauäuig und realitätsfremd?

Antwort von Herrn Simon:

Um es nochmal unmissverständlich auszusprechen – die NSA kann sauber implementierte Verschlüsselung nicht knacken. Dass dies möglich sein wird, ist nicht vor Ende des Jahrzehnts zu erwarten. Darüber hinaus bezieht sich die erwartete Quantenüberlegenheit auf mathematische Probleme, welche bei asymmetrischer Verschlüsselung zu Einsatz kommen. Für dieses Problem gibt es bereits Ansätze zur Postquantenkryptografie (PQC). Viele der aufgezeigten Lösungsansätze beziehen sich allerdings auf symmetrische Verschlüsselung wie AES. Die EU ist keinesfalls blauäugig.

Frage 8:

Was ist aber z.b. mit den Inhalten in Chats, die keine eigenen Dokumente sind. Auch hier können personenbezogene Daten vorkommen?

Antwort von Herrn Simon:

Wenn sich das auf M365 bezieht, siehe Fragen 9 und 10. Bei anderen Anbietern gibt es verschiedene Möglichkeiten, welche spezifisch betrachtet werden sollten.

Frage 9:

Hallo, mir stellt sich hier die Frage wie ein externes Key-Management in Lösungen wie MS-Teams oder bei den Postfächern umgesetzt werden kann?

Antwort von Herrn Simon:

Wie im Webcast aufgezeigt, ist externes Key Management bei M365 Lösungen derzeit „nur“ für mit MIP geschützte Dokumente mittels DKE möglich.

Frage 10:

Wäre daher das Conlusio, dass in Europa derzeit SaaS-Systeme wie z.B. MS-Teams gar nicht genutzt werden dürften?

Antwort von Herrn Simon:

Für bestehende Systeme hat man bis 27.12.2022 Zeit, die neuen SCCs abzuschließen. Wenn keine entsprechenden TOMs möglich sind, steht in den Empfehlungen des EDSA unmissverständlich „In den Fällen, in denen keine zusätzliche Maßnahme geeignet ist, müssen Sie die Übermittlung vermeiden, aussetzen oder beenden, um das Schutzniveau der personenbezogenen Daten nicht zu gefährden.“

Frage 11:

Ist es empfohlen, "Confidential Computing" zur Verschlüsselung der Daten "in memory" einzusetzen?

Antwort von Herrn Wolff:

Auf der einen Seite scheint Data-at-Rest- und Data-in-Motion-Verschlüsselung, nach aktuellem Stand, ein zur Gewährleistung des geforderten „im Wesentlichen gleichwertigen Schutzniveaus wie im EWR“ ausreichend zu sein, wenn die Schlüssel nicht beim Cloud-Anbieter liegen. In Frankreich wurde, in der erwähnten Klage zu Impfkampagne, entsprechend geurteilt.
Auf der anderen Seite empfiehlt der EDSA „Künftige technische, rechtliche oder organisatorische Entwicklungen können dazu führen, dass neue zusätzliche Maßnahmen entstehen, die Sie in Betracht ziehen sollte“. Aus unserer Sicht ist Data-in-Use eine solche Entwicklung und sollte somit in Betracht gezogen werden.

Frage 12:

Es wäre gut, wenn die beiden Referenten, mal darauf eingehen würden, dass bei allen IT-Anwendungen immer alle Aktivitäten aller Benutzer ständig registriert und geloggt werden. Genau diese Daten sind jedoch für SAAS Anwendungen sehr relevant. Denn es werden nicht nur Einzeldokumente gespeichert, die vorher klassifiziert werden können. Sondern es wird z.B. in einer Hochschule von tausenden Beschäftigten ständig interagiert.

All das sind personenbezogene Daten. In M365 werden über die Analyse Werkzeuge für die Administratoren in den Admin Dashboards all diese Aktivitäten sichtbar. Und jede/r einzelne Benutzer*in kann dies ebenfalls in MyAnalytics nachvollzogen werden.

Wie bitte schön soll denn die Verschlüsselungslösung von Thales hier helfen.

Wenn die beiden Referenten ehrlich sind müssten sie zugeben dass dies nicht möglich ist.

Das Urteil in Frankreich bezieht sich wiederum nur auf die Szenarien des EDSA zur Cloudspeicher!!!

Antwort von Herrn Simon:

Wie im Webcast erläutert, ist die große Herausforderung, „Segregation of Duties" zu erreichen. Dies erstreckt sich auch auf den Zugriff auf die Metadaten (z. B. Aktivitätslogging). Diese Trennung ist bei SaaS nur möglich, wenn der Anbieter entsprechende Schnittstellen vorgesehen hat. Bei M365 ist dies aktuell „nur" für Dokumente vorgesehen, welche sich mittels Microsoft Information Protection schützen lassen. In der Tat helfen für andere Daten in M365 Verschlüsselungslösungen in der vorgestellten Form nicht.
Das Urteil in Frankreich beschreibt keineswegs nur Cloud-Speicher. Die Doctolib-Anwendungen werden bei AWS gehostet.

Frage 13:

Als öffentliche Stelle muss man ja auf prinzipiell sicher sein und nicht verhältnismäßig sicher sein. Also muss ich ja den höchsten technisch machbaren Stand erreichen?!

Antwort von Herrn Simon:

Sicherheit ist ein relativer Zustand der Gefahrenfreiheit. Somit kann man zwar prinzipiell „sicher" sein – ein Restrisiko, so klein es auch sein mag, bleibt dennoch bestehen. Den höchsten technisch machbaren Stand zu erreichen, ist idR nicht sinnvoll. Vielmehr gilt es, ein angemessenes Schutzniveau zu erreichen. Genau darauf zielen die TOMs ab.

Frage 14:

Aber wenn der Betreiber verpflichtet ist zum liefern der Daten an die US-Behörden, dann wird es einen Weg geben die Daten zur Verfügung zu stellen. In der Vergangenheit haben Betreiber von Diensten auf Druck von US-Behörden, Daten herauszugeben, ihren Dienst eingestellt, weil sie ansonsten Hintertüren hätten einbauen müssen.

Antwort von Herrn Simon:

Aktuell müssen US-Unternehmen gemäß CLOUD Act Daten herausgeben. Um dies zu unterbinden, wird vom Europäischen Datenschutzausschuss Verschlüsselung und getrennte Aufbewahrung der Schlüssel empfohlen. In dem erwähnten Urteil zur COVID-Impfkampagne in Frankreich wurden diese Schutzmaßnahmen als ausreichend bewertet, um den Datenschutz gerecht zu werden. Aus unserer Sicht ist dies nachvollziehbar, weil gezieltes

Ausspähen deutlich erschwert wird und sich der Angriff auf die Systeme für massenhafte Datenabfrage nicht eignen. Als nächster Schritt empfiehlt sich eine Data-in-Use-Verschlüsselung mit getrenntem Key Management für ein weiter gesteigertes Schutzniveau.

Frage 15:

Wo setzt man mit SCC an, bzw. ordnungsgemäßer Umsetzung - eine Microsoft wird mit einem KMU (500 Mitarbeiter) keine individuellen Vertragsgestaltungen durchführen.

Antwort von Herrn Simon:

Vom Grundsatz her hat Microsoft bereits die neuen SCCs als Basis für die Nutzung von Microsoft-Diensten begrüßt. Die SCCs sehen konkrete TOMs (technische und organisatorische Schutzmaßnahmen) „zur Gewährleistung des im Wesentlichen gleichwertigen Schutzniveau“ (wie im EWR) vor. Als Kunde wird man wohl darauf bestehen müssen, damit die Dienste konform betrieben werden können.

Frage 16:

Welche Voraussetzungen müssen erfüllt sein um die PIIs zu finden und zu klassifizieren? Müssen Sie strukturiert sein? Wo dürfen die Daten liegen?

Antwort von Herrn Simon:

Ein Modul der THALES-CipherTrust-Plattform ist Data Discovery, welches man optional buchen kann. Die Data Discovery Engine ist sehr leistungsfähig und findet PIIs (und andere gesuchte Daten) sowohl in unstrukturierten, als auch in strukturierten Daten. Sie geht sogar so weit, dass Bilddateien analysiert werden können. So würden z. B. auch Fotos von Ausweisdokumenten als DSGVO-relevante Daten entdeckt werden. Wo die Daten gespeichert sind, ist dabei nicht relevant. Aber natürlich braucht die Engine Zugriff auf die Systeme, egal ob in der Cloud oder on-p1remise.

Frage 17:

Bei SAP und Arvato handelt es sich um Microsoft Tochter, dann ist doch diese Tochterunternehmen unnter Hoheit von Microsoft und damit kann wiederum die Daten an die US Koncern weiter laufen oder ?

Antwort von Herrn Simon:

Microsoft hält gemäß des Heise-Artikels weder an SAP, noch an Arvato, noch am geplanten Joint Venture Anteile. Dieser Ansatz zielt darauf ab, dass der Vertragspartner kein US-Unternehmen ist, daher unter europäisches Recht fällt und weder Microsoft, noch US-Behörden Zugriff auf die Daten haben. Microsoft will sich auf die Rolle des Softwarelieferanten beschränken.

https://www.heise.de/news/SAP-und-Arvato-versprechen-souveraene-Microsoft-Cloud-fuer-Behoerden-6346760.html