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

Frage 1:

Da hat wohl niemand das DSG (Datenschutzgesetz) Schweiz wirklich gelesen. Einfache Zusammenfassung: https://www.vischer.com/know-how/blog/die-dsgvo-und-die-schweiz-10-mythen-und-missverstaendnisse-38502/ sowie https://www.humanrights.ch/de/ipf/menschenrechte/innere-sicherheit/schweizer-nachrichtendienstgesetz

Antwort von Frau Raabe-Stuppnig:

Ich verstehe die „Frage" in Zusammenhang mit unserem Vortrag leider nicht. Für die Schweiz besteht ein Angemessenheitsbeschluss, es bedarf also keiner SCC. Ich habe mir auch die Links angesehen und habe leider keine Überschneidungen mit unserem Vortrag gefunden. Vielleicht kann diese Frage nochmals spezifiziert werden?

Frage 2:

Wie steht es aktuell mit dem „Datenschutz" bzw. mit der Weitergabe der pesonenbezogenen Daten in Zusammenhang mit COVID 19 – und insbesondere auch mit der entsprechenden Zweckwidmung?

Antwort von Frau Raabe-Stuppnig:

Gesundheitsdaten unterliegen einem besonders strengen Schutz. Abgesehen davon, dass es sich um Daten „besonderer Kategorien" nach Art 9 DSGVO handelt (für die ein noch strengeres Verarbeitungsverbot mit Rechtfertigungsvorbehalt besteht), bestehen auch weitere Sondervorschriften zur Wahrung der Sicherheit der Daten. In den Anfangszeiten von COVID-19 hatte man das Gefühl, dass der datenschutzrechtliche Umgang mit Gesundheitsdaten heruntergeschraubt wurde. Das ist in dieser Allgemeinheit aber nicht der Fall. Nur dann, wenn die Datenverarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich ist (Art 9 Abs 2 lit i DSGVO), ist sie gerechtfertigt. Darüber hinaus ist der Zweckbindungsgrundsatz gemäß Art 5 Abs. 1 lit b DSGVO zu beachten. Eine Verwendung der Gesundheitsdaten für andere Zwecke als der Gesundheitsvorsorge, der Eindämmung des Virus und der Heilbehandlung ist daher unzulässig. Weiters ist auf den Grundsatz der Speicherbegrenzung gemäß Art 5 Abs 1 lit e DSGVO hinzuweisen. Die Daten sind zu löschen, sobald sie zur Zweckerreichung nicht mehr erforderlich sind.

Das Urteilsbeispiel, das im Vortragsteil von Armin Simon vorgetragen wurde, hing mit Gesundheitsdaten zusammen. In diesem Urteil wurde die Wichtigkeit von Verschlüsselungen iSd „Zero Knowlege“-Prinzips betont.

Frage 3:

Bezüglich „Hold your own key“: Heisst das, das ich nicht die Dienste zum Credentials Management der Cloud Anbieter nutzen sollte. z.B. AWS KMS oder Azure Key Vault?

Antwort von Herrn Simon:

Die Dienste AWS KMS und Azure Key Vault verhindern nicht, dass die Cloud-Anbieter auf Ihre Daten zugreifen können. Das EDPB (European Data Protection Board) fordert daher zusätzliche Schutzmaßnahmen. Das bedeutet, allein diese Dienste helfen nicht dabei, Schrems-II-konform zu sein.

Seit dem Schrems-II-Urteil ist jedoch viel Bewegung in die Lösungen der Cloud-Anbieter gekommen:

- Microsoft hat mit DKE (Double Key Encryption) mit THALES eine Möglichkeit geschaffen, mittels eines zweiten zusätzlichen Keys mit MIP (Microsoft Information Protection) geschützte Daten so zu verschlüsseln, dass auch Microsoft nicht mehr an die Daten kommt.
  https://cpl.thalesgroup.com/de/cloud-security/encryption/double-key-encryption
- GCP (Google Cloud Platform) ermöglicht inzwischen für viele ihrer Dienste EKM (External Key Management) unter Einbindung des THALES Cipher Trust Managers.
  https://cpl.thalesgroup.com/de/encryption/data-protection-on-demand/services/key-broker-google-cloud-ekm
- AWS entwickelt derzeit gemeinsam mit THALES eine Lösung, welche Schrems-II-Konformität ermöglichen wird. AWS nennt diese Lösung xKS (eXternal Key Storage). Wie erwähnt, ist ein Tech Preview ab Q1 2022 geplant

Frage 4:

Hallo zusammen. Problem: die globalen Anbieter lassen kaum mit sich verhandeln. D.h. auch die verbesserten Regelungen mit SDK und erweiterten Maßnahmen sind deren Regelungen. Es gibt kaum Möglichkeiten eigene Maßnahmen TOM zu etablieren. de facto sind das AGB keine Verträge. Beispiele, M365, AWS, Zoom, Adobe, Cisco, etc.

Antwort von Herrn Simon:

Die Verhandlungen unserer Kunden mit den globalen Anbietern erleben auch wir, immer wieder, als größere Herausforderung.
An vielen Stellen haben sich die Anbieter allerdings inzwischen geöffnet (siehe auch Antwort zu Frage 3). Häufig ist das Wissen über die Lösungsintegration von technischen Maßnahmen

innerhalb der Anbieter nicht überall bekannt. Gerne unterstützen wir und zeigen konkret auf, welche TOMs bei welchen Anbietern möglich sind.

Frage 5:

Szenario: SAP bietet uns ein Applikations-Hosting in MS-Azure an
Alleiniger Vertragspartner für uns ist SAP
Microsoft ist also Subdienstleister von SAP
=> Reicht für DSGVO Konformität die Verschlüsselung von „Data in Rest/Transition“ in Azure aus, wenn SAP den Schlüssel besitzt Danke

Antwort von Frau Raabe-Stuppnig:

Wenn ein Sub in einem Drittstaat herangezogen wird, kann das die Datenschutz-Compliance ebenso gefährden. Es sollte die Vorlage der SCC, die zwischen dem Auftragsverarbeiter und dem Sub abzuschließen sind, zu Dokumentationszwecken verlangt werden. Nur wenn aus diesen SCC hervorgeht, dass der Datenschutzstandard gewahrt bleibt, dürfen die Subs „freigegeben“ werden. Die Haftung trifft (auch) den Verantwortlichen. Vertragliche Regelungen mit dem Auftragsverarbeiter sind insofern sinnvoll, als sie (zumindest) ein Regressrecht absichern können.

Antwort von Herrn Simon:

In den uns bekannten Installationen gab es verschiedene Datenschutzherausforderungen. Als Lösung wurde THALES Transparent Encryption für SAP HANA auf MS Azure geschaffen (siehe Link weiter unten). Darüber hinaus ist eine THALES-Integration für SAP Custodian und THALES Tokenisation for SAP angekündigt (beides für Q1 2022).
https://cpl.thalesgroup.com/sites/default/files/content/solution_briefs/field_document/2021-03/ciphertrust-sap-hana-in-azure-sb.pdf

Frage 6:

Helfen diese neuen SCC bei Datentransfer in die USA? Sind die dann rechtssicher, trotz FISA etc.?

Antwort von Frau Raabe-Stuppnig:

Der Abschluss der SCC ist unbedingt erforderlich, aber nur dann ausreichend, wenn gleichzeitig in den TOMs (technische und organisatorische Maßnahmen) ausreichende „ergänzende Maßnahmen“ vereinbart werden, die ein faktisches Einhalten der SCC ermöglichen. Nur die vertragliche Zusicherung laut SCC, das Datenschutzniveau zu gewährleisten, ist nicht mehr ausreichend, weil FISA diesen Vertrag „overruled“. D.h. es muss insb. mit technischen Maßnahmen sichergestellt werden, dass der Vertrag über die Wahrung des Datenschutzniveaus auch faktisch eingehalten werden kann. Beispielsweise über Verschlüsselung, bei der der Schlüssel nicht beim Auftragsverarbeiter, sondern beim Verantwortlichen oder einem Treuhänder liegt. Wenn die NSA dann Daten „absaugt“, sind

sie verschlüsselt, ohne dass eine Möglichkeit vorliegt, auf die Herausgabe des Schlüssels zu bestehen. Das erfüllt das „Zero Knowlege“-Prinzip und wahrt die Datenschutz-Compliance.

Frage 7:

Starke Verschlüsselung=Anonymisierung, nicht Pseudonymisierung, oder?

Antwort von Herrn Simon:

Das ist richtig. Der erwähnte Punkt Pseudonymisierung zielt auch eher auf die Möglichkeit der Tokenisierung. Bei der THALES-Tokenisierungslösung wird der Originalwert durch einen anderen nicht ableitbaren Wert im gleichen Format ersetzt und dadurch pseudonymisiert. Diese Lösung bietet sich zB für Datenbanken an. Häufig wird Tokenisierung auch genutzt, um die Anzahl der zu auditierenden Systeme zu verringern.

Frage 8:

Welche MS 365 Pläne und zusätzlichen Dienste von MS müsste ich buchen, so dass nur ich als Verantwortlicher und nicht die MS als Provider den Schlüssel hat?

Antwort von Herrn Simon:

M365 bietet an verschiedenen Stellen die Möglichkeit der Verschlüsselung, aber leider keine generelle Schnittstelle, um die Schlüssel alleinig in der Kundenhoheit zu belassen.

Nur an einer speziellen Stelle hat MS die Möglichkeit der Verschlüsselung unter Zuhilfenahme eines zweiten Schlüssels geschaffen (DKE für MIP siehe auch Antwort zu Frage 3). Nachdem wir keine M- Lizensierungsspezialisten sind, können wir nur unverbindlich mitteilen, dass die Nutzung von MIP eine E5 Lizenz erfordert. Möglicherweise ist der Service allerdings auch einzeln erhältlich.

Frage 9:

„Key at Customer“ funktioniert mMn nur für IaaS / PaaS aber nicht für SaaS. Sobald der Dienstleister selber Datenverarbeitung durchführen soll, muss er an die unverschlüsselten Daten herankommen. MWn gibt es noch niemanden der technische Lösungen für dieses Problem hat.

Antwort von Herrn Simon:

Der Gedanke ist grundsätzlich richtig. In dem Moment, in dem Daten verarbeitet werden, müssen sie unverschlüsselt sein*. Das ist allerdings unabhängig davon, auf welchem Level verschlüsselt wird.
Wenn auf Applikationslevel verschlüsselt werden soll, muss die Applikation eine entsprechende sauber implementierte Schnittstelle bieten. Dann kann auch der THALES Cipher Trust Manager (CTM) die Hoheit über die Verschlüsselung gewährleisten.

Das European Data Protection Board (EDPB) fordert allerdings „nur“ die Verschlüsselung der gespeicherten Daten und die vollständige Kontrolle über das Schlüsselmaterial. Dies ist auch für uns nachvollziehbar. Es geht tatsächlich darum, ein angemessenes Schutzniveau zu erreichen. Im Vortrag hatte ich das Beispiel der Steuer-CDs bei den Schweizer Banken genannt. Die Verschlüsselung der Daten, bei getrennter unkopierbarer Aufbewahrung des Schlüsselmaterials, hätte diesen Datenabfluss verhindert. Angriffe auf Prozessorebene eignen sich nicht für massenhaften Datenabfluss und machen das gezielte Abfragen von Daten nahezu unmöglich. Somit ist es nachvollziehbar ausreichend um Schrems-II-konform zu werden.
*THALES bietet auch Lösungen für Confidential Computing, welche spezielle CPU-Fähigkeiten zum Schutz während der Datenverarbeitung nutzen (z.B. in Verbindung mit Google Ubiquitous Data Encryption).
https://cpl.thalesgroup.com/blog/encryption/google-ubiquitous-data-encryption-ekm

Frage 10:

Datenverschlüsselung ist nur „Data at rest“ und „Data at transport“ möglich, bei „Data at use“ ist das in aller Regel nicht möglich. Viele Cloud-Dienste bieten daher keine komplette Verschlüsselung mittels „Bring your own Key“ an. Sind diese Dienste daher nicht konform nutzbar?

Antwort von Herrn Simon:

Bei den „Bring your own Key”-Lösungen der Provider werden i.d.R. Schlüssel auf Kundenseite generiert und anschließend zum Provider hochgeladen. Dies verhindert nicht den Zugriff und die Herausgabe von Daten. Somit sind diese Lösungen nicht Schrems-II-konform.
Seit dem Schrems-II-Urteil ist jedoch viel Bewegung in die Lösungen der Cloud-Anbieter gekommen (siehe auch Antwort zu Frage 3).

Frage 11:

Wie würden Sie die Möglichkeit einschätzen, dass Schulen in der Lage sind dafür zu sorgen, dass die bekannten amerikanischen Anbieter von Lernplattformen keinerlei Zugriff auf die (personenbezogenen) Daten von Schülern, die diese Lernmanegment-Plattform nutzen, erhalten? Wären die vorgestellten Verschlüsselungssysteme anwendbar? Falls ja, welche Kosten würden für Schulen entstehen?

Antwort von Herrn Simon:

Nach unserem Verständnis handelt es sich bei Lernplattformen um Software-as-a-Service. Wenn diese Software eine Möglichkeit der Datenverschlüsselung und eine Schnittstelle für externes Key Management bietet, sollte es möglich sein, das „Zero knowledge“-Prinzip umzusetzen. In bestimmten Fällen lässt sich auch an anderer Stelle mit Verschlüsselung ansetzen. So hat in einem Projekt IBM als Cloud-Anbieter THALES die Möglichkeit gegeben, Verschlüsselung auf Infrastrukturebene mit externem Key Management umzusetzen.

Es gibt also vielerlei Optionen. Um die Frage nach den Kosten zu beantworten, brauchen wir genauere Hintergründe zur eingesetzten Lösung.

Frage 12:

Ein Key Management ist zwar eine gute Idee. Aber: Allerdings soll diese Verschlüsselung auf der Ebene von Daten ablaufen. Bei komplexen integrierten Systemen wie M365 mit all den vielen Einzelprogrammen ist es kaum möglich eine Kenntnis über die unzähligen Daten zu erhalten, diese zu klassifizieren und dann gezielt zu verschlüsseln. Sofern man nur eine Cloud-Plattform wie AWS für seine eigene Anwendung nutzt ist dies vmtl. besser möglich. Es ist also eine Frage wieviele Personen im eigenen Unternehmen, Behörde, Bildungseinrichtung man für Daten und Keymanagement einsetzen will.

Antwort von Herrn Simon:

Die allermeisten Cloud-Lösungen bieten Verschlüsselung und diese wird auch grundsätzlich angewendet. Momentan ist es insbesondere bei M365 so, dass die Schlüsselhoheit und somit die Verfügungsgewalt über die Daten beim Cloud-Anbieter liegt. Wie schon in der Antwort zu Frage 3 angeführt, ist dort Bewegung reingekommen und es gibt einige bessere Optionen.
Bezüglich der Anzahl der einzusetzenden Personen lässt sich feststellen, dass der Automatisierungsgrad insbesondere bei Verschlüsselung und Key-Life-Cycle Management inzwischen sehr hoch ist. Ohne dies wäre es kaum möglich, Verschlüsselung in so großem Stil sinnvoll einzusetzen.

Frage 13:

Wenn Hersteller Features angesprochen werden, dann bitte richtig erklären. Customer Key bedeutet, MS verwendet 2 Schlüssel, einer vom Kunden und einen MS Service Key. Der Rest war sehr gut. Vielen Dank

Antwort von Herrn Simon:

Vielen Dank für diesen Kommentar. Offensichtlich war ich an dieser Stelle nicht präzise genug.
Microsoft 365 bietet eine zusätzliche Verschlüsselungsebene für Inhalte. Diese Inhalte werden mit Customer Key verschlüsselt. Diese Schlüssel können durch den Kunden generiert und in den Azure Key Vault hochgeladen werden. THALES bietet für das Encryption Key Lifecycle Management den THALES Cloud Key Manager.

https://azuremarketplace.microsoft.com/de-de/marketplace/apps/thales-vormetric.ciphertrust-cckm-171?tab=overview

Allerdings kann Customer Key und Dienstverschlüsselung nicht verhindern, dass Microsoft-Mitarbeiter auf Ihre Daten zugreifen können.

https://docs.microsoft.com/de-de/microsoft-365/compliance/customer-key-overview?view=o365-worldwide
Im 2. Abschnitt steht dort: „Die Dienstverschlüsselung soll nicht verhindern, dass Microsoft-Mitarbeiter auf Ihre Daten zugreifen.“

Damit wird die Forderung des EDPB, nach getrennter vom Provider unabhängiger Aufbewahrung des Schlüsselmaterials zur Vermeidung von Datenzugriffen, nicht erfüllt.