Wahlweise als Inhouse-Seminar oder Webinar buchbar

Datenschutz und Verschlüsselung in der Public Cloud – die aktuelle Lage

Zielgruppe:	Cloud Use Case Owner, Cloud Manager, IT-Leiter, IT-Projektleiter, IT-Provider-Manager, Beauftragte für IT-Outsourcing, Beauftragte für Datenschutz, Informationssicherheit und IT-Risiko-Management, IT-Revision, IT-Betrieb und Rechtsabteilung
Dauer:	Empfohlen als 1,5-tägiges Vor-Ort-Seminar oder als Webinar in Teilen
Preis:	EUR 1.100,- p. P. zzgl. MwSt., zzgl. Reisekosten bei Durchführung vor Ort. Mindestteilnehmerzahl 4 Personen. Im Preis sind die Vorbereitung und die Durchführung des Seminars bzw. Webinars inkl. Unterlagen enthalten. Bei kleineren oder größeren Gruppen Preis auf Anfrage.

Beschreibung

Wie beeinflusst der neue Angemessenheitsbeschluss der EU für einen sicheren und vertrauenswürdigen Datenverkehr zwischen der EU und den USA den Datenaustausch mit US-amerikanischen Cloud-Providern? Ist mit dem im Juli 2023 veröffentlichten Datenschutzrahmen EU-USA die Datenschutzkonformität im Sinne der EU-DSGVO nun dauerhaft gewährleistet? Welche organisatorischen, technischen und vertraglichen Lösungsansätze bieten die US-amerikanische Hyperscaler wie AWS, Google Cloud oder Microsoft Azure/M365 grundsätzlich an? Was tolerieren die Datenschutz-Aufsichtsbehörden in Deutschland angesichts der vielfachen De-facto-Monopollösungen dieser Anbieter und wie ist die aktuelle Lage hinsichtlich Standard-AVVs der Anbieter?

Datenverschlüsselung kann wirksamen Schutz bei der Nutzung cloudbasierter Ressourcen und Services bieten. Vor allem im Kontext der Angebote der großen US-amerikanischen Hyperscaler, aber reicht es aus? Die Experten von IT-Security@Work (ISW) und microfin erläutern in diesem Partner-Seminar/Webinar die aktuelle Rechtslage, räumen zugleich mit den vielerorts verbreiteten (Fehl-) Interpretationen auf und geben eine grundlegende Übersicht zu den Möglichkeiten der Verschlüsselung in der Nutzung, dem Transport und der Speicherung der Daten. Sie und Ihr Team haben die Möglichkeit, Ihre konkreten Cloud-Use-Cases und -Vorhaben mit uns zu diskutieren. Und Sie erfahren, was zu tun ist, falls vor dem Europäischen Gerichtshof auch gegen die Rechtmäßigkeit dieses Datenschutzrahmens EU-USA geklagt wird.

Stimmen Sie Ihren individuellen Bedarf in einem persönlichen Gespräch mit uns ab

Irina Shapiro

T +49 6172 / 177 630
E anfrage@microfin.de

Inhalte Teil 1 – Fokus Datenschutz:

Datenschutz gestern, heute und morgen

- Eine ganz kurze Geschichte des europäischen Datenschutzes
- Gibt es einen Unterschied zwischen Datenschutz und Datenschutz in der Cloud?
- DSGVO vs. CLOUD-Act, FISA, PATRIOT-Act und andere US-amerikanische Rechtssätze
- Datenaustausch mit den USA: Was die Datenschutz-Aufsichtsbehörden aktuell erwarten
- Was sind erweiterte Garantien bezogen auf die Informationssicherheit und Technik?

Cloud-Sourcing mit den großen Hyperscalern

- Möglichkeiten zur Annäherung an eine datenschutzkonforme Nutzung der Cloud
- Verschlüsselung: Allzweckwaffe oder doch nur ein Feigenblatt?
- Erläuterung der Verschlüsselungsoptionen, Möglichkeiten, Option Customer Lockbox (Zugriff nur bei explizierter Freigabe)
- Angemessenheitsbeschluss der EU für einen sicheren und vertrauenswürdigen Datenverkehr zwischen der EU und den USA und der Datenaustausch mit US-amerikanischen Cloud-Providern
- Technische Restriktionen der „Reaktionen“ und was daher noch notwendig ist

Aktuelle Entwicklungen im Spannungsfeld Datenschutz und Cloud

- Angemessenheitsbeschluss der EU für einen sicheren und vertrauenswürdigen Datenverkehr zwischen der EU und den USA

IT-Security@Work GmbH (ISW)
Robert-Bosch-Straße 18
63303 Dreieich
www.isw-online.de

microfin Unternehmensberatung GmbH
Rathausplatz 12
61348 Bad Homburg
www.microfin.de

- Einschätzungen der Datenschützer zum Einsatz von Video-Tools (z. B. Microsoft Teams)
- Fragebogen des Hamburgischen Landesdatenschutzbeauftragten und mögliche Antworten darauf
- Ausnahmegenehmigung für Teams durch den Hessischen Landesdatenschutzbeauftragten (bis 2021), aktuelle Diskussion zu AVV für Microsoft Cloud-Dienste (2022-2023)
- Modellhafte Verantwortungsteilung in einem Unternehmen (z.B. IT, Einkauf, ISB, Betriebsrat etc.) – typische Probleme und Lösungsansätze

Vision: Die Europäische Cloud: GAIA-X; European Cloud User Coalition; IPCEI-CIS; branchenspezifisch: European Cloud: „Bafin-konforme Anbieter" und Visionen von IT-Providern

Standards und Zertifikate sowie spezifische Muster-Checklisten zum Datenschutz in der Cloud

Back-up der Daten in der Cloud: Eine Angelegenheit des Kunden

Folgen und Bußgeld bei Verstößen gegen den Datenschutz in der Cloud

Inhalte Teil 2 – Fokus Verschlüsselung:

Einführung Verschlüsselung
- Was ist ein Schlüssel, was ist ein Zertifikat und wie sieht ein Zertifikatsantrag aus?
- Was ist symmetrische, asymmetrische und Hybridverschlüsselung?
- Warum muss ich verschlüsseln? Welche Anforderungen stellen Datenschutz und Kunden in diesem Zusammenhang? Warum setzt man die Verschlüsselung außerhalb der Cloud?

Unterschied zwischen Transport-, In-Nutzung- und Speicher-Verschlüsselung
- Data at Rest: auf dem Device, über das SAN/LAN, von der Datenbank und von der Applikation (Ort der Verschlüsselung, Performance, Sicherheits- und Schutzniveau, Funktionseinschränkungen)
- Data in Transit (Verschlüsselung Payload, Verschlüsselung Kanal, REST-Nutzung von Standardmechanismen
- Data in Use (Funktionsweise)

Funktionsweise eines Hardware-Sicherheits-Moduls (HSM)
- Aufgaben und Funktionen eines HSMs (Schlüsselerstellung, Verwaltung, Zertifikatserstellung, Partitionierung, Verfügbarkeit und Key Backup)
- Physisches HSM vs. virtuelles HSM, HSM as a Service (Anbieter)

Architekturmodell der Cloud in Verbindung mit Verschlüsselung
- Wo greift welche Verschlüsselung?
- Funktionsweise, Zielsetzung von Bring your own key (BYOK) vs. Hold your own key (HYOK) in der Cloud

Praxisbeispiel (1) Microsoft Azure: Was ist der „Availability Key" von Microsoft? Welche Möglichkeiten gibt es, um den Zugriff durch Microsoft auf die Kundendaten abzustellen?

Praxisbeispiele (2) Microsoft Azure: Wie kann ich sicherstellen, dass MS-Office-Daten, MS Exchange und Teams-Daten verschlüsselt werden?
- Welche Optionen werden angeboten und für welchen Dienst (OneDrive, SharePoint, Exchange etc.)?
- Welchen Sinn machen die Optionen „Sicherheitssicht" und „Betriebssicht"?

Kann ich auf Verschlüsselungsangebote der Cloud Service Provider vertrauen? Welcher Cloud Service Provider bietet welche Möglichkeiten bei der Verschlüsselung?
- Vor- und Nachteile
- Probleme bei Optionen, die ein Cloud Service Provider anbietet

Bei Bedarf: Technische Kryptographie (Open SSL, XCA)

IT-Security@Work GmbH (ISW)
Robert-Bosch-Straße 18
63303 Dreieich
www.isw-online.de

microfin Unternehmensberatung GmbH
Rathausplatz 12
61348 Bad Homburg
www.microfin.de