Online-Zahlungsdienste: Wann ist „sicher“ sicher genug?

Banken und Finanzdienstleister müssen ihre Transaktionsdienste ab September 2019 durch Verschlüsselung und Zwei-Faktor-Authentifizierung absichern. Doch um sensible Daten zuverlässig zu schützen, sollten Unternehmen mehr tun als das.

10.05.2019 – München: Online bezahlen war noch nie so einfach: Die EU-Richtlinie PSD2 („Payment Services Directive 2“) mischt bereits seit Anfang 2018 die Payment-Branche auf. Sie erlaubt Unternehmen, auf Daten von Kreditinstituten zuzugreifen und begünstigt so die Entstehung neuer Finanz- und Zahlungsdienste, zum Beispiel Zahlungsauslöse- und Kontoinformationsdienste. Ab 14. September 2019 sind Banken und Unternehmen EU-weit dazu verpflichtet, diese Dienste durch Zwei-Faktor-Authentifizierung und verschlüsselte Übertragung abzusichern – doch reicht das aus, um dem hohen Schutzbedarf sensibler Kundendaten zu genügen? IT-Sicherheitsexperte Dr. Hubert Jäger von der TÜV SÜD-Tochter Uniscon rät Banken, Finanzdienstleistern und Unternehmen zu zusätzlichen Maßnahmen.

Ein Schritt in die richtige Richtung?

„Starke Kundenauthentifizierung und Verschlüsselung bei der Datenübertragung sind Schritte in die richtige Richtung und helfen, Daten gegen Angriffe von außen abzusichern. Doch sensible Daten müssen auch bei der Verarbeitung zuverlässig geschützt sein – und zwar auch gegen Angriffe von innen“, betont Jäger. Dies zu gewährleisten ist nicht einfach: Werden Kundendaten im eigenen Rechenzentrum verarbeitet, muss der Anbieter seine Mitarbeiter durch geeignete Maßnahmen vom Zugriff auf sensible Informationen zuverlässig ausschließen. Bei der Nutzung von Cloud-Diensten wird es noch schwieriger, hinreichenden Datenschutz zu gewährleisten – es ist ein offenes Geheimnis, dass die meisten Cloud-Anbieter technisch die Möglichkeit haben, auf die Daten in ihren Rechenzentren zuzugreifen.

„Viele Infrastrukturen können nicht das hohe Sicherheitsniveau bieten, dass die DSGVO für die Verarbeitung schutzbedürftiger Daten voraussetzt“, sagt Jäger und verweist auf Artikel 25 und 32 der Datenschutzgrundverordnung. Gerade die dort aufgeführten Forderungen nach `Datenschutz durch Technikgestaltung‘[1] – „Privacy by Design“ – und Schutzmaßnahmen nach dem `Stand der Technik‘[2] stellen Unternehmen vor eine echte Herausforderung.

Zero-Trust-Technologie als Chance

Eine Alternative zu klassischen Cloud- und Serverinfrastrukturen sind betreibersichere Clouds, die etwa in Form der „Versiegelten Cloud“ der Deutschen Telekom oder Uniscons „Sealed Platform“ seit einiger Zeit im kommerziellen Einsatz sind. Jäger: „Viele Cloud-Anbieter setzen auf eine Kombination von organisatorischen und technischen Maßnahmen, um unerwünschte Zugriffe auszuschließen. Gerade organisatorische Schutzmaßnahmen lassen sich aber mit verhältnismäßig geringem Aufwand umgehen – ein nicht zu unterschätzendes Restrisiko bleibt hier also bestehen. Betreibersichere Infrastrukturen hingegen schließen durch rein technische Maßnahmen jeglichen unbefugten Datenzugriff aus – auch den Betreiber der Infrastruktur selbst.“ Sogar privilegierter Zugriff im Rechenzentrum oder durch den Admin ist technisch ausgeschlossen – und auch ein Zugriff durch in- oder ausländische Behörden ist so unmöglich[3]. Auf diese Weise können sensible Daten nicht nur sicher übertragen und gespeichert

[1] https://dsgvo-gesetz.de/art-25-dsgvo/
[2] https://dsgvo-gesetz.de/art-32-dsgvo/
[3] https://www.uniscon.com/de/pressemitteilungen/usa-versus-eu-was-passiert-mit-den-daten/

werden, sondern sind auch bei ihrer Verarbeitung in der Cloud geschützt – und zwar sowohl gegen externe als auch interne Angreifer.

Bei der Entwicklung dieser einzigartigen Zero-Trust-Technologie haben die Softwareingenieure grundlegende Datenschutz- und IT-Sicherheitsgrundsätze von Anfang an berücksichtigt. Durch diesen konsequenten Privacy by Design-Ansatz erreichen betreibersichere Infrastrukturen ein höheres Sicherheitsniveau als andere Cloud-Lösungen und bieten so eine ideale Basis für sämtliche digitalen Geschäftsmodelle, bei denen hochsensible Daten erhoben, gespeichert und verarbeitet werden. Das umfasst Finanz- und Payment-Services, aber auch alle anderen Dienste oder Anwendungen, bei denen Compliance höchste Priorität hat.

Weiterführende Informationen und druckfähiges Bildmaterial erhalten Sie auf Anfrage bei presse@uniscon.de.

Uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die Uniscon GmbH ist ein Unternehmen der TÜV SÜD Gruppe. Als Teil der Digitalisierungsstrategie von TÜV SÜD bietet Uniscon hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund ist Uniscon in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zu Partnern und Produkt: www.uniscon.com

Pressekontakt

Uniscon GmbH, Claudia Seidl
Ridlerstr. 57
80339 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Julia Fehrle
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20