



FACT SHEET

Was CISOs über TLS-Terminierung wissen sollten



Was CISOs über TLS-Terminierung wissen sollten

Sie stehen an der Sicherheitskontrolle im Flughafen. Ihr Rucksack verschwindet im Röntgengerät. Als er wieder auftaucht, nimmt ein Beamter ihn kommentarlos vom Band, öffnet ihn und beginnt, Ihr Hab und Gut zu fotografieren. Medikamente, Ausweispapiere, Kontoauszüge und andere persönliche Dinge wandern nacheinander vor die Linse seiner Kamera. In der zweiten Reihe steht ein unbekannter Mann im Anzug und schwarzer Sonnenbrille, beobachtet die Szene und bekommt am Ende die Kamera ausgehändigt, mit der er in ein Hinterzimmer verschwindet.

Was im analogen Leben wie ein massiver Eingriff in die Privatsphäre wirkt, ist im digitalen Raum tägliche Praxis – meist unbemerkt. Immer dann, wenn Organisationen auf nicht-europäische Applikationsschutz-Anbieter setzen, müssen Nutzerinnen und Nutzer faktisch akzeptieren, dass Dritte tiefen Einblick in ihre Datenströme erhalten. HTTPS ist der Standard für den Schutz sensibler Informationen im Internet, gleichzeitig nutzen Angreifer dieselbe Verschlüsselung als Tarnkappe für Angriffe. Um diese Bedrohungen zu erkennen und abzuwehren, heben Applikationsschutz-Anbieter die Verschlüsselung mittels TLS-Terminierung kurzzeitig auf, prüfen den „digitalen Rucksack“ und sehen dadurch sowohl schädliche Zugriffe als auch besonders sensible Daten.

Entscheidend ist, wem Sie diesen hochkritischen Prozess anvertrauen – Resilienz, Vertraulichkeit und Compliance hängen maßgeblich vom beauftragten Provider ab.



Schutzdienstleister heben die TLS-Verschlüsselung kurzzeitig auf, um den Datenverkehr zu prüfen, Angriffe zu erkennen und nur legitime Anfragen an die Unternehmensserver weiterzuleiten. Die hierbei erforderliche TLS-Terminierung entlarvt schädliche Zugriffe, macht allerdings auch sensible Daten für den Dienstleister zugänglich.

Kernrisiken und Anforderungen im Überblick

- **DSGVO-Verstöße:** Die Entschlüsselung sensibler personenbezogener Daten birgt rechtliche Risiken. Nur Anbieter mit Sitz in der EU können volle DSGVO-Konformität und Schutz vor Zugriffen nicht-europäischer Behörden gewährleisten.
- **Unautorisierter Zugriff auf sensible Geschäftsdaten:** Überwachungsgesetze wie FISA 702 und der CLOUD Act erlauben US-Behörden Zugriff auf Daten bei US-Anbietern, selbst wenn die Daten physisch in Europa gespeichert sind. Dies birgt Risiken für Vertraulichkeit und Compliance.
- **Gefährdung der digitalen Lieferkette:** Geopolitische Spannungen schaffen das Risiko, dass US-Regierung und Anbieter den Zugang zu Cloud-Diensten kurzfristig sperren („US Kill Switch“) – etwa zur Durchsetzung von Embargos, Sanktionen oder Strafzöllen.

Was bedeutet das für CISOs

TLS-Terminierung ist unabdingbar für umfassende Sicherheitsanalysen. Ihre Umsetzung erfordert jedoch sorgfältige rechtliche und technische Kontrolle, um Datenschutz und Vertraulichkeit nicht zu gefährden. CISOs sollten sich bei der Auswahl des geeigneten Providers für Applikationsschutz folgende Fragen stellen:

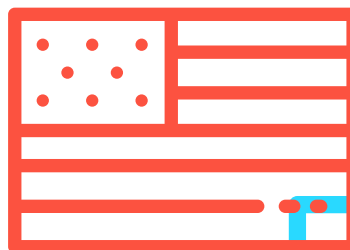
- Erfolgt die TLS-Terminierung ausschließlich durch einen EU/EWR-basierten Provider?
- Besteht in meiner digitalen Lieferkette eine Verbindung zu Nicht-EU-Anbietern oder US-Konzernstrukturen – auch hinsichtlich Subunternehmern?
- Habe ich vollständigen Einblick in alle Datenzugriffe sowie die technische Durchführung der Traffic-Kontrolle?
- Sind Lieferketten transparent dokumentiert und existieren klare Exit-Strategien, inklusive Kontrolle über Datenlokation und Schlüsselmaterial sowie definierte Prozesse für Behördenanfragen?



Was bedeutet das für den User?

Diese Risiken betreffen aber nicht nur abstrakte Datenströme, sondern ganz konkrete Menschen: User, Patientinnen, Bürger, Kundinnen. Schon heute gibt es Staaten, die Einreise, Aufenthalt oder Visumvergabe an politische Äußerungen, finanzielle Situation oder Gesundheitszustand knüpfen. Menschen können an Grenzen abgewiesen werden, weil ihre Daten irgendwo ausgewertet, verknüpft oder falsch interpretiert wurden.

Wer sensible Kommunikations- und Personendaten über Provider verarbeitet, die ausländischen Überwachungsgesetzen unterliegen, setzt seine Nutzer potenziell genau diesem Risiko aus – insbesondere im KRITIS-Umfeld (Energie, Gesundheit, Finanzen, Verwaltung). Die Frage ist daher nicht nur: Welche Risiken gehe ich als Organisation ein? Sondern auch: Welche Risiken mute ich meinen Kunden, Patientinnen und Bürgern zu?



Round-up

TLS-Terminierung ist mehr als eine technische Notwendigkeit – sie ist ein strategisches Instrument zur Stärkung von Resilienz, Compliance und digitaler Souveränität. Durch die Wahl eines europäischen Providers für Applikationsschutz können Organisationen aus hochregulierten Branchen wie der Finanzindustrie, dem Gesundheitswesen, KRITIS oder der öffentlichen Hand ihre Position in diesen Bereichen schnell und nachhaltig stärken.

TLS-Terminierung bei Myra

Die Schutzlösungen von Myra bauen auf einer rechtssicheren und datenschutzkonformen TLS-Terminierung auf. Die Services richten sich speziell an Organisationen aus hochregulierten Branchen, die besonderen Wert auf Compliance, Servicequalität und solide Lieferketten legen.

- Unternehmenssitz und Management in Deutschland – keine Betroffenheit von CLOUD Act oder FISA 702, klarer EU-Rechtsrahmen
- TLS-Terminierung und Traffic-Verarbeitung ausschließlich auf dedizierter Infrastruktur in deutschen Rechenzentren – Daten und Schlüssel bleiben im EU-Raum
- Zertifizierte Sicherheits- und Compliance-Strukturen für nachweislich DSGVO-konforme Verarbeitung in hochregulierten Branchen
- Vollständig protokollierte, auditierbare Prozesse und hohe Verfügbarkeitsstandards für maximale Transparenz gegenüber Aufsicht, Prüfern und Kunden
- Europäische Sicherheitsplattform „Made in Germany“ ohne versteckte Hyperscaler-Abhängigkeiten – ein starker Baustein für eine souveräne, resiliente Lieferkette



Made in Germany

Myra schützt, was zählt. In der digitalen Welt.

Sie wollen mehr darüber erfahren, wie Sie mit unseren souveränen Lösungen Ihre digitale Unabhängigkeit stärken, Ihre Kosten minimieren und Ihre Webanwendungen vor böartigen Angriffen schützen? Unser Expertenteam berät Sie gerne individuell und erarbeitet eine maßgeschneiderte Lösung für Ihr Unternehmen. Vereinbaren Sie am besten noch heute ein unverbindliches Beratungsgespräch.

**Starten Sie jetzt Ihre Souveränitäts-Initiative:
mit Cybersecurity „Made in Germany“**

Myra Security GmbH

☎ +49 89 414141 - 345

🌐 www.myrasecurity.com

@ info@myrasecurity.com