TÜV TRUST IT
TÜV AUSTRIA Group

Sicherheit und Wert von Informationen

Neue Anforderungen für SWIFT-Anwender: Das SWIFT Assessment

Im Umfeld großer Unternehmen und Finanzsysteme spielt die Sicherheit der IT-Infrastrukturen sowie angrenzender Prozesse eine besonders wichtige Rolle – insbesondere aufgrund der stetig zunehmenden Komplexität von Cyberangriffen auf diesem Gebiet. SWIFT-Anwender sollten beachten, dass das SWIFTNet zwar einen sicheren Zahlungsverkehr ermöglicht, jedoch nicht die Sicherheit der lokalen Umgebung angeschlossener Unternehmen gewährleistet.

Hier greift das von der Society for Worldwide Interbank Financial Telecommunication (SWIFT) eingeführte „Customer Security Programme“ (CSP), welches eine Reihe von Sicherheitskontrollen enthält. Ergänzend hierzu werden obligatorische sowie empfohlene Kontrollen im „SWIFT Customer Security Controls Framework“ (CSCF) beschrieben, sodass SWIFT-Anwender die Möglichkeit haben, alle Anforderungen zur Sicherung ihrer SWIFT-Infrastruktur und zur Abwehr von Cyberangriffen leicht nachzuvollziehen.

Sorgen Sie rechtzeitig vor

Bislang wurde die konkrete Umsetzung dieser Anforderungen in Form von Self Assessments geprüft und musste lediglich gegenüber SWIFT bestätigt werden.

CSCF Aktualisierungsprozess

Das CSCF wurde seit seiner Einführung im Jahr 2018 stetig weiterentwickelt, wobei entsprechend der Bedrohungslage regelmäßig neue empfohlene Advisory Controls aufgenommen wurden und bereits eingeführte Advisory Controls zu verpflichtenden Mandatory Controls aufstiegen.

Mit diesem Vorgehen strebt die SWIFT-Organisation eine kontinuierliche Verbesserung von SWIFT-Infrastrukturen an. Der Fokus liegt insbesondere auf folgenden Zielen:

1. Secure Your Environment – eigene Umgebung sichern
2. Know & Limit Access – Zugriff kennen und einschränken
3. Detect & Respond – erkennen und reagieren

Neu ab 2021:

Forderung der SWIFT nach einem unabhängigen Assessment über die Einhaltung der vorgegebenen Kontrollen.

Unsere Empfehlung:

Bereiten Sie sich bereits jetzt auf die neuen Anforderungen vor und lassen Sie die Einhaltung der Kontrollen anhand eines unabhängigen CSCF-Assessments überprüfen.

Unser Angebot

Die TÜV TRUST IT bietet hierzu eine Reihe von Leistungen an, um Sie optimal bei der Umsetzung der neuen Anforderungen zu unterstützen:

1. Umsetzung des SWIFT CSP

Gemeinsam mit Ihnen analysieren wir alle vorgegebenen Sicherheitskontrollen und unterstützen Sie bei der anforderungsgerechten Umsetzung. In diesem Rahmen steht Ihnen folgendes Angebot zur Verfügung:

- Durchführung eines Scoping-Workshops zur Validierung des SWIFT-Geltungsbereiches und des daraus abgeleiteten Architekturtyps
- Übergreifende Zuordnung von Sicherheitsmaßnahmen aus dem Informationssicherheits-Managementsystem (ISMS), falls vorhanden
- Durchführung von Workshops (typ. ½ Tag) zu folgenden Themen:
  - Feststellung des Erfüllungsgrades der SWIFT-Sicherheitskontrollen auf Vorgaben- und Umsetzungsebene (Operationalisierung der Vorgaben)

TÜV TRUST IT
TÜV AUSTRIA Group

Sicherheit und Wert von Informationen

- Ableitung von konkreten Maßnahmen zur Herstellung der Compliance zum SWIFT CSP auf Vorgaben- und Umsetzungsebene

Bei der Umsetzung der Maßnahmen unterstützen die Experten der TÜV TRUST IT Sie als SWIFT-Anwender gerne durch eine regelmäßige Überwachung, z. B. in Form von Jour Fixe Terminen inkl. begleitendem Reporting.

2. SWIFT Assessment

Die Mitarbeiter der TÜV TRUST IT bringen eine langjährige bestätigte Expertise im Bereich der Cyber Security in unseren Service ein und stehen Ihnen als SWIFT-Kunde beim SWIFT Customer Security Programme sowie folgenden Themenbereichen gerne zur Seite:

- Durchführung der SWIFT-konformen unabhängigen CSCF-Bewertungen/Assesments für die SWIFT-Architekturen A1, A2, A3, A4 und B
- Analyse der vorhandenen Infrastruktur und Sicherheitslösungen
- Beurteilung Ihrer Kontrollziele und konkrete Empfehlungen zu deren Optimierung
- Umsetzung von Maßnahmen durch technische Lösungen, Produkte und Consulting Services

Empfehlung: Nutzen Sie jetzt die Gelegenheit, mithilfe des SWIFT-Assessment über eine gesamtheitliche Lösung für die Cybersecurity Ihres Unternehmens nachzudenken – für mehr Sicherheit in Ihrem Unternehmen!

3. Bescheinigung der Compliance auf Basis des SWIFT Independent Assessment Frameworks (IAF)

SWIFT-Anwender müssen jährlich ihre Compliance mit den für die jeweilige Architektur relevanten Mandatory Controls in Form einer „Self-Attestation“ bescheinigen. Die Einhaltung muss im Rahmen eines Assessments überprüft werden, welches ab 2021/2022 von einer unabhängigen Stelle durchgeführt werden muss. Im üblichen Community-Standard-Assessment kann dies entweder eine interne Kontrollstelle wie die interne Revision, der Risk- bzw. Compliance-Manager sein, oder ein qualifizierter externer Dienstleister wie die TÜV TRUST IT.

Anhand des SWIFT Customer Security Frameworks bewerten wir zunächst Ihre SWIFT-Infrastruktur. Ein auf Basis der Ergebnisse stattfindendes Assessment zeigt anschließend auf, ob eine Compliance zu den SWIFT Vorgaben nachweisbar ist.

Ihr Nutzen

- Erfüllung der regulatorischen Anforderungen zum unabhängigen SWIFT-Assessment
- Know-how Aufbau in der eigenen Organisation
- Interne Ressourcenschonung

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51
D-51069 Köln
Tel.: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

Wienerbergstraße 11
Turm B, 2. Stock · A-1100 Wien
Tel.: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com