SWIFT Customer Security Programme (CSP) – Sind Sie bereit?

Als Reaktion auf die wachsende Anzahl von Cyberangriffen auf Infrastrukturen von SWIFT-Kunden hat SWIFT ein Sicherheitsprogramm (Customer Security Programme – CSP) für ihre Teilnehmer definiert, um gemeinsam gegen Cyber-Bedrohungen zu kämpfen. Alle Finanzinstitute, welche über eine SWIFT BIC verfügen, werden gezwungen, sich diesem Sicherheitsprogramm zu unterstellen – unabhängig davon, ob sie die Infrastruktur selbst betreiben oder outgesourced haben.

Das Sicherheitsprogramm wurde im April 2017 von SWIFT in dessen erster gültigen Fassung publiziert. Es definiert Anforderungen, welche von allen angeschlossenen Kunden und Teilnehmern (nachfolgend „Kunden" genannt) eingehalten werden müssen. Das Programm hat zum Ziel, den Informationsaustausch innerhalb der SWIFT-Community zu verbessern und einen hohen Sicherheitsstandard der lokalen SWIFT-Infrastruktur bei den Kunden zu gewährleisten. Ferner muss ein Compliance-Framework implementiert werden, um den ständig wachsenden Cyber-Bedrohungen entgegenzutreten und die Fähigkeiten zur Abwehr von Cyber-Angriffen bei den Kunden zu stärken.

Das Programm fordert jeden SWIFT-Kunden auf, ein Kontroll- und Compliance-Framework zu implementieren. Das Kontroll-Framework besteht aus einem Set von 16 verbindlichen (Mandatory Controls) und 11 optionalen Kontrollen (Advisory Controls). Die Kontrollen bauen auf den vorhandenen SWIFT-Sicherheitsrichtlinien auf und orientieren sich an Best-Practice-Standards wie NIST, ISO/IEC 27002 und PCI-DSS. Die verbindlichen Kontrollen definieren die Grundlage, welche von allen SWIFT-Teilnehmern eingehalten werden muss. SWIFT empfiehlt, die optionalen Kontrollen zu implementieren, um die lokale SWIFT-Infrastruktur optimal zu schützen. Die folgende Übersicht illustriert die Kontrollziele, die Prinzipien sowie die Kontrollen des SWIFT CSP:

(*Quelle:* https://i2.wp.com/)

Jeder SWIFT-Teilnehmer muss bis zum 1.1.2018 melden (Self-Attestation), ob er die Kontrollen erfüllt oder nicht. Bei Nicht-Erfüllung wird dies dem Nationalen Regulator weitergeleitet. Jeder SWIFT-Kunde kann bei anderen SWIFT-Kunden Einsicht in die Self-Attestation verlangen und somit den Compliance-Status nach dem SWIFT-Standard erfragen. Die Freigabe zur Einsicht muss nicht zwangsläufig gewährt werden, kann jedoch bei Nichtgewährung u.U. entsprechende Reaktionen hervorrufen.

Verpassen Sie diesen wichtigen Termin nicht und bereiten Sie sich frühzeitig auf die Selbstbeurteilung vor. ISPIN AG verfügt über ausgewiesene Spezialisten im Bereich dieses SWIFT CSP und kann Sie kompetent und effizient bei der Selbstbeurteilung, der GAP-Analyse und/oder der Massnahmenplanung und -umsetzung unterstützen. Kontaktieren Sie uns via info@ispin.ch.