



DAS SWIFT CUSTOMER SECURITY PROGRAMME

In den letzten Jahren hat die Anzahl an schweren Angriffen in der Bankenwelt durch Cyber Attacken drastisch zugenommen. Obwohl jede Bank und jedes Unternehmen für seine eigene Abwehr zuständig ist, hat SWIFT beschlossen die Branche im Kampf gegen Cyberkriminalität zu vereinen und mit der Einführung des „Customer Security Programme“ (CSP) in Aktion zu treten.

SWIFT, die Society for Worldwide Interbank Financial Telecommunication, betreibt ein globales, hochverfügbares und sicheres Kommunikationsnetzwerk zum schnellen und sicheren Austausch von Finanznachrichten.¹ SWIFT verarbeitet circa 27,45 Mio. Nachrichten pro Tag und hat über 11.000 Teilnehmer weltweit.²

Das Netzwerk an sich wurde bisher noch nicht Opfer eines Hackerangriffes, allerdings ist aufgrund der wichtigen Rolle, welches das Kommunikationsnetzwerk in der Finanzindustrie einnimmt die Sicherheit innerhalb des

Netzwerkes von großer Bedeutung.

Mit dem „Customer Security Programme“, welches in 2016 eingeführt und in Q2/2017 in Kraft getreten ist, hat SWIFT eine Übersicht an Cybersicherheit-Standards veröffentlicht, die alle Teilnehmer in ihre Systemlandschaft implementieren müssen. Dies garantiert SWIFT die grundsätzliche Sicherung seines internationalen Netzwerkes gegen Cyber-Angriffe und die allgemeine Sicherheit der Finanzbranche.

Das Customer Security Control Regelwerk (CSC Regelwerk) ist seit März 2017 allen Teilnehmern des SWIFT Netzwerkes zugänglich. Das Regelwerk erklärt und beschreibt alle notwendigen im CSP enthaltenen Sicherheitskontrollen.

Diese Sicherheitskontrollen sind auf die drei allumfassenden Rahmenziele „Secure your Environment“, „Know and Limit Access“ und „Detect & Respond“, und acht Kernprinzipien basiert.

Daten und Fakten

- Abgabe einer Selbst-Überprüfung für alle Teilnehmer des SWIFT Netzwerkes
- 27 Sicherheitskontrollen (16 Pflicht, 11 empfohlen)
- Abgabe der ersten Selbst-Überprüfung bis zum 01. Januar 2018, jährliche Wiederholung der Abgabe
- Abgabe der Selbst-Überprüfung in das KYC Registry
- Durchführung einzelner Inspektionen durch SWIFT ab Januar 2018 als zusätzliche Maßnahme

Insgesamt werden 27 Sicherheitsüberprüfungen CSC Regelwerk durchgeführt, 16 davon sind Pflicht, 11 nur angeraten.

Alle SWIFT Teilnehmer müssen eine Selbst-Überprüfung ihres Compliance-Status auf Basis des CSC Regelwerkes vornehmen. Eine jährliche Wiederholung dieser Selbst-Überprüfung ist von SWIFT vorgeschrieben. Der Compliance-Status jedes Teilnehmers muss bis zum 1. Januar 2018

¹ Vgl. Gabler Wirtschaftslexikon (URL) <http://wirtschaftslexikon.gabler.de/Definition/swift.html>

² Vgl. SWIFT (URL) <https://www.swift.com/about-us/swift-fin-traffic-figures#topic-tabs-menu>

in das KYC Registry³ eingetragen werden. Grundsätzlich ist hier jedes Unternehmen die oberste Instanz und kann selbst entscheiden, ob der eigene Compliance-Status für andere Nutzer einsehbar ist oder nicht. Allerdings können Unternehmen sich ab sofort weigern mit anderen Teilnehmern im Netzwerk zu kommunizieren, die einen Nicht-Compliant Status oder einen Nicht-Veröffentlichten Status haben. Dies verbessert die Transparenz und Sicherheit zwischen den Teilnehmern und hilft Unternehmen risikobasierte Entscheidungen zu treffen, indem der Status des Gegenübers einer Geschäftstransaktion überprüft werden kann.

Zusätzlich zu der jährlich verpflichtenden Selbst-Überprüfung wird SWIFT ab 2018 jedes Jahr eine Auswahl an Kunden für zusätzliche Absicherung untersuchen und durch interne und externe Auditoren für ein sicheres Netzwerk sorgen.

³ Know Your Customer, Plattform zum Austausch-Management von standardisierten Kundendaten

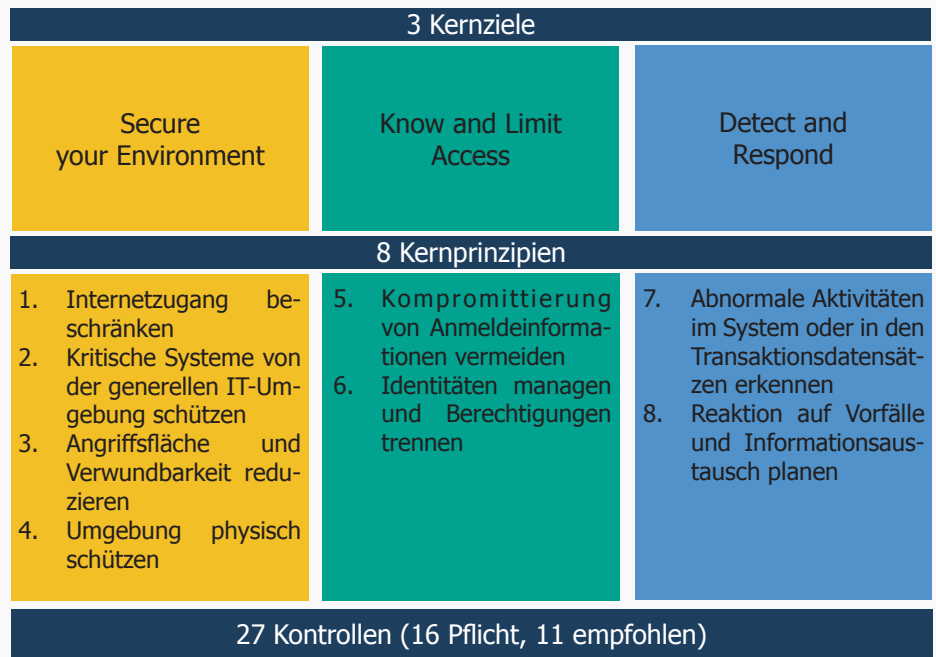
R&L AG FAKTEN

- Spezialist in den Bereichen Payment, SWIFT und Info Management
- Consulting, IT-Services und Software
- Zuverlässiger Partner seit 1998
- Ansässig in Deutschland
- Member of Be Group
- Umfassendes Know-How und langjährige Projekterfahrung im Bereich SWIFT
- Internationale Player als Kunden
- Integrierter Beratungsansatz

KONTAKT

R&L AG
Frühlingstraße 2
D-84034 Landshut
Tel: +49 (0) 871 27 66-0
Fax: +49 (0) 871 27 66-199
information@rl-ag.com
www.rl-ag.com

DAS SWIFT CUSTOMER SECURITY CONTROL REGELWERK (SWIFT CSC REGELWERK)



Quelle: Angepasst von swift.de

WAS DIE R&L AG FÜR SIE TUN KANN

Die R&L AG bietet Ihnen eine breite Auswahl an Services zum Thema „Customer Security Programme“ an:

- Überprüfung und Analyse der aktuellen internen und externen Sicherheitsinfrastruktur und der bestehenden Sicherheitskontrollen
- Durchführung einer Eigeninspektion zur Überprüfung des Compliance-Status in Bezug auf die Kontrollen und Ziele des CSP und die Definition möglicher Sicherheitslücken im System
- Durchführung eines SWIFT Readiness Reports
- Implementierung aller notwendigen Kontrollen des SWIFT CSC Regelwerkes
- Implementierung aller empfohlenen Kontrollen des SWIFT CSC Regelwerkes
- Entwicklung und Implementierung aller möglichen zusätzlichen Kontrollen für erhöhte Sicherheit und zukünftige Compliance mit dem SWIFT CSC Regelwerk
- Übernahme der Rolle des internen Auditors zur Durchführung von zusätzlichen Überprüfungen als Vorbereitung auf die Untersuchungen von SWIFT nach dem 1. Januar 2018
- Unterstützung und Training Ihrer Mitarbeiter auf dem Themengebiete SWIFT Compliance
- Unterstützung und Implementierung aller zusätzlich entstandenen Anforderungen an die IT-Infrastruktur nach einer Überprüfung durch SWIFT
- Jährliches Update der bestehenden IT-Sicherheitsinfrastruktur auf Basis des aktuellen SWIFT CSC Regelwerkes

Die R&L AG ist ein weltweit etablierter Experte im Bereich SWIFT und dessen Umsystemen und unterstützt Sie bei der Implementierung aller vom „Customer Security Programme“ gestellten Anforderungen und der Weiterentwicklung Ihrer Sicherheitsstandards und -kontrollen.

SWIFT Customer Security Programme