

## SWIFT „CUSTOMER SECURITY PROGRAMME“ CSP GET READY TO BE PREPARED

### 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.<sup>1</sup> SWIFT verarbeitet circa 42,1 Mio. Nachrichten pro Tag und hat über 11.000 Teilnehmer weltweit.<sup>2</sup>

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.

Um die Sicherheit des globalen Zahlungsverkehrs zu verbessern, hat SWIFT 2016 das Customer Security Programme (CSP) ins Leben gerufen, das von SWIFT Teilnehmer verlangt, von SWIFT definierte Sicherheitskontrollen zu implementieren und am Ende eines jeden Kalenderjahres eine Attestation über den Grad der Einhaltung vorzulegen.

Alle Unternehmen, die am SWIFT-Net zur Zahlungsabwicklung teilnehmen (d.h. einen eigenen angebotenen SWIFT BIC haben), müssen die verpflichtenden Sicherheitskontrollen des SWIFT Customer Security Programms einhalten. Diese Kontrollen sind im SWIFT Customer Security Controls Framework (CSCF)

#### Daten und Fakten

- Verpflichtende Abgabe einer Attestation für alle Teilnehmer des SWIFT-Netzwerks
- 31 Sicherheitskontrollen (22 verpflichtend, 9 empfohlen)
- Jährliche Einreichung der Attestation basierend auf dem jährlich veröffentlichten und angepassten SWIFT CSCF
- Ab 2021 ist ein Independent Assessment für die Einreichung der Attestation erforderlich
- Abgabe der Attestation über SWIFT KYC SA

dokumentiert, das mindestens einmal jährlich aktualisiert wird. Jedes Jahr werden neue Kontrollen eingeführt und empfohlene Kontrollen aus dem Vorjahr werden regelmäßig zu verpflichtenden Kontrollen hochgestuft.

Diese Sicherheitskontrollen basieren auf den drei übergreifenden Rahmenzielen „Secure your Environment“, „Know and Limit Access“

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

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

und „Detect & Respond“ sowie auf acht Sicherheitsprinzipien. Insgesamt sind im Customer Security Controls Framework (CSCF) 31 Sicherheitskontrollen aufgeführt, von welchen maximal 22 verpflichtend und 9 empfohlene sind, abhängig vom Architekturtyp.

Jedes SWIFT-Mitglied muss jährlich eine Attestation in die KYC Security Attestation Application (KYC-SA) einreichen.

Ab 2021 sind alle SWIFT-Nutzer verpflichtet vor Abgabe der Attestation ein Independent Assessment durchzuführen. Dies kann entweder durch ein internes oder ein externes Assessment erfolgen, dem das Independent Assessment Framework (IAF) zu Grunde liegt.

Neben dem IAF behält sich SWIFT auch das Recht vor bei ausgewählten Nutzern, ein verpflichtend externes Assessment zu beauftragen.

<sup>3</sup>Für Nutzer entwickelte Plattform zur Abgabe ihrer Security Attestation, welche den Complaine Status des Unternehmens gegenüber der SWIFT Customer Security Controls bestätigen.

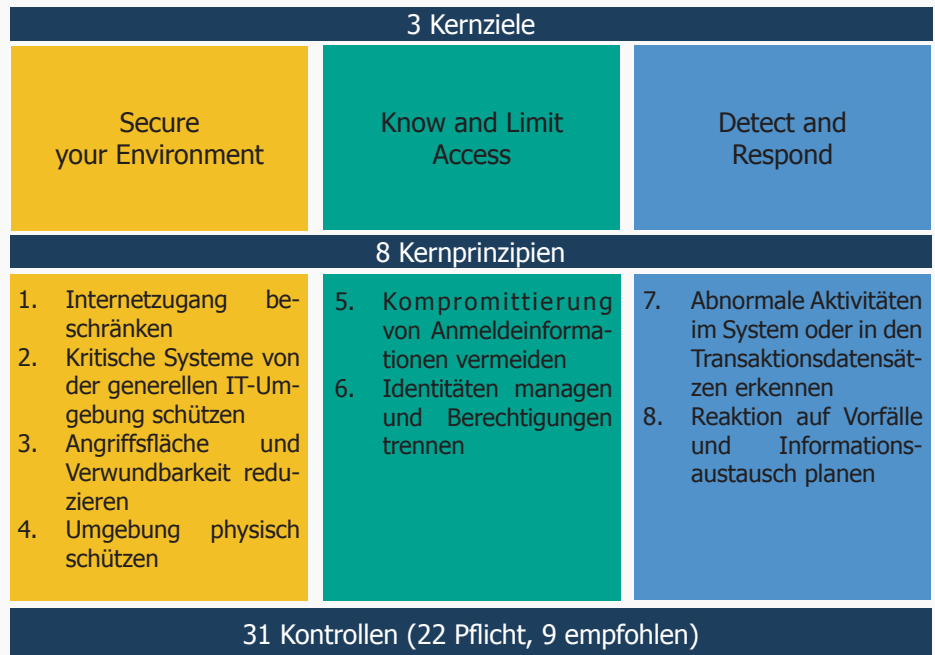
## BE AG FAKTEN

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

## KONTAKT

Be Shaping the Future -  
Financial Industry Solutions AG  
Frühlingstraße 2  
D-84034 Landshut  
Tel: +49 (0) 871 27 66-0  
information@be-stf.de  
www.be-stf.de

## DAS SWIFT CUSTOMER SECURITY CONTROLS FRAMEWORK (SWIFT CSCF)



Quelle: Angepasst von swift.de

## WAS DIE BE AG FÜR SIE TUN KANN

Die Be 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 von Machbarkeitsstudien
- Implementierung aller notwendigen Kontrollen des SWIFT CSCF
- Implementierung aller empfohlenen Kontrollen des SWIFT CSCF
- Entwicklung und Implementierung aller möglichen zusätzlichen Kontrollen für erhöhte Sicherheit und zukünftige Compliance mit dem SWIFT CSCF
- Unterstützung und Training Ihrer Mitarbeiter auf dem Themengebiet SWIFT und dem SWIFT

„Customer Security Programme“

- Unterstützung und Implementierung aller zusätzlich entstandenen Anforderungen an die IT-Infrastruktur nach einem Independent Assessment
- Jährliches Update der bestehenden IT-Sicherheitsinfrastruktur auf Basis des aktuellen SWIFT CSCF

Die Be 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.

**Be** SHAPING THE FUTURE

SWIFT Customer Security Programme