CONSILEON

SWIFT-CSCF Zertifizierung schnell und einfach erreichen

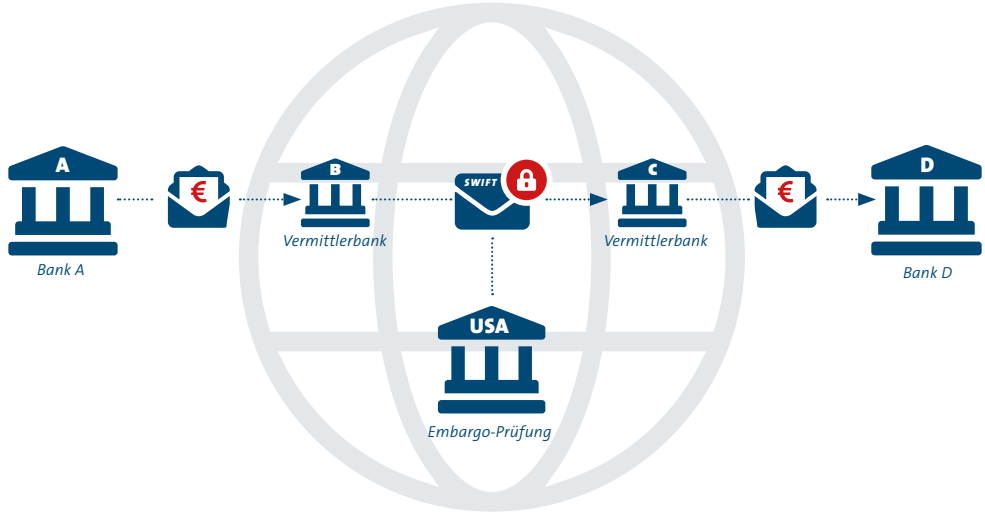
Consileon führt für Sie das SWIFT-Assessment durch und setzt notwendige Maßnahmen gemeinsam mit Ihnen um.

www.consileon.de

Warum sich bei SWIFT alles verändert hat

Kein internationaler Zahlungsverkehr ohne die SWIFT

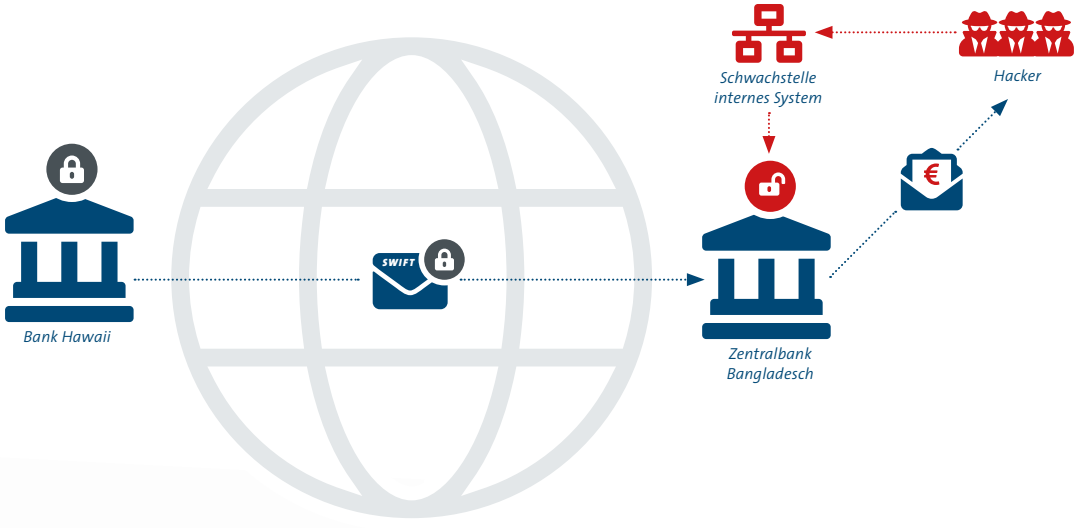
Lange Zeit betrieb die Society for Worldwide Interbank Financial Telecommunication (SWIFT) vor allem einen sicheren Kommunikationskanal für den internationalen Zahlungsverkehr der Banken. Das ist auch heute noch so. International kann ohne die SWIFT praktisch kein Geld bewegt werden. Aktuell sind etwa 11.000 Banken und Finanzinstitute an die SWIFT angeschlossen und bewegen zusammen rund sechs Billionen US-Dollar pro Tag.



Vereinfacht dargestellter Ablauf einer Überweisung unter Nutzung des SWIFT-Netzwerks.

Die Schwachstelle wird gezielt angegriffen

Aber ein Ereignis änderte alles. Es erfolgte ein Angriff von drei Hackern auf eine japanische Bank, bei dem es den Kriminellen gelang, in das interne System der Bank einzubrechen. Für diese Attacke nutzten sie eine fingierte Bewerbung. Da intern keine weiteren Sicherungsmechanismen die Personalabteilung von den Zahlungssystemen trennten, konnten die Cyberkriminellen fingierte Überweisungen unter Verwendung des sicheren SWIFT-Netzwerke tätigen.



Vereinfachte Darstellung des Hackerangriffs auf die Zentralbank von Bangladesch.

Zeit ist der kritische Faktor

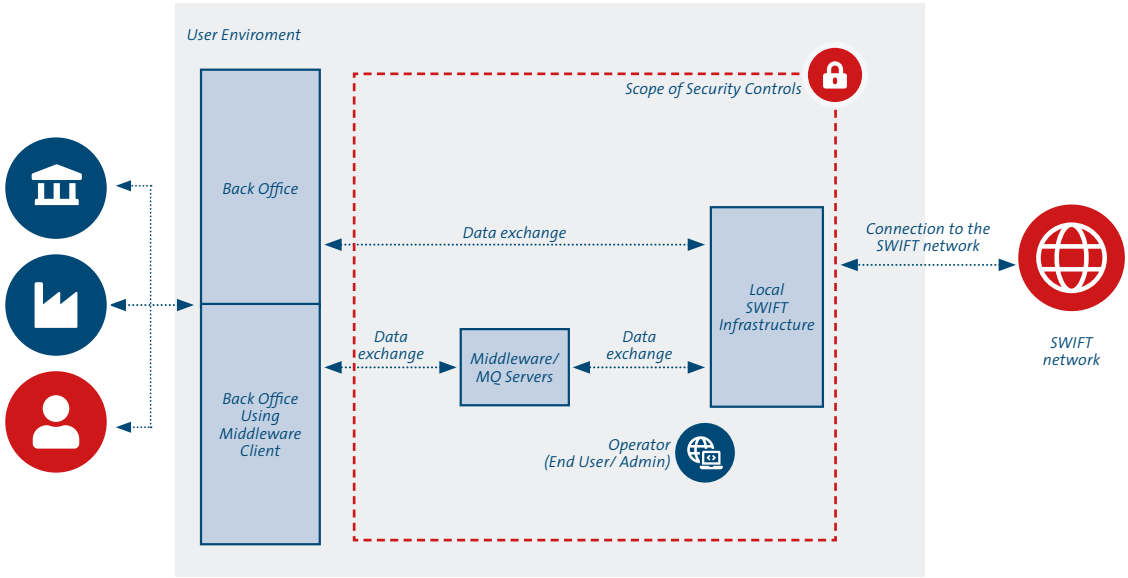
Kriminelle müssen sehr viel Zeit aufwenden, um die geeignete Gegenstelle für ihre fingierten Überweisungen zu finden. So dauerte es im vorliegenden Fall mehr als ein Jahr, bis die Angreifer die für ihre Zwecke ideale, lokale Bank ausfindig machen konnten.

Auch für die Bank wurde Zeit zum kritischen Faktor. Allein das Erkennen des Geldverlusts nahm zwei Tage in Anspruch und erst nach fünf Tagen wurde die Zielbank informiert. Zu diesem Zeitpunkt hatten die Hacker bereits den Betrag von 81 Millionen Dollar abgeholt und im Casino verspielt. Eine schnellere Reaktion hätte dies verhindern können.

Die Rizal Commercial Banking Corporation (RCBC) in Manila, deren Managerin sowie die für die Freigabe verantwortlichen Filialleiter erhielten drastische Strafen. Die Hacker hingegen konnten zwar identifiziert, aber nicht gefasst werden.

Gelernt: Sicherheit beginnt bei den Akteuren

Aufgrund dieses Ereignisses setzt sich bei der SWIFT die Erkenntnis durch, dass sie auch innerhalb der angeschlossenen Banken für ausreichende Sicherheit sorgen muss, um einen solchen Diebstahl in Zukunft zu verhindern. Deshalb verpflichtet die SWIFT alle beteiligten Institute zu einem strengen Sicherheitsprogramm, welches dafür sorgt, dass alle Bereiche, die für den Zahlungsverkehr relevant sind und mit SWIFT kommunizieren, streng abgeschirmt sind von den restlichen IT-Systemen des Finanzinstituts und dem Internet.



Schematische Darstellung der Sicherungsmaßnahmen der SWIFT.

Strenge Vorgaben werden zur Herausforderung

Die obligatorischen Anforderungen der SWIFT sind streng und detailliert, aber technisch durchaus machbar. Gleichzeitig sind bereits weitere Vorgaben formuliert, von denen jedes Jahr einige verpflichtend werden.

Am besten lassen sich diese Sicherheitsmaßnahmen an einigen Beispielen zeigen:

- Extrem strenge Vorgaben bei der Nutzung von Passwörtern.
- Verschlüsselung des gesamten internen Datenverkehrs.
- Videoüberwachung und Bewegungssensoren in der Serverumgebung.
- Mindestens tägliche Überprüfung der IT auf Manipulationen.
- Sichere externe Speicherung von Protokollen für zwölf Monate.
- Regelmäßige Übungen von Reaktionen auf einen Cyber-Einbruch.

Ein Kunde meldet sich zu Wort

„Zur Verbesserung der Sicherheit globaler Zahlungen hat SWIFT das Customer Security Programme (CSP) eingerichtet, welches SWIFT-Nutzer dazu verpflichtet, den Grad der Umsetzung der Vorgaben aus dem SWIFT CSP zu attestieren. SWIFT aktualisiert dieses regelmäßig und überführt dabei regelmäßig empfohlene in verbindliche Kontrollen. Bereits im Jahr 2019 wurde uns als Betreiber einer SWIFT A1 Full Stack Architektur das Independent Assessment Framework auferlegt. Im Rahmen dieser Herausforderung sind die Stärken von Consileon Business Consultancy – neben der methodischen und fachlichen Expertise – auch der partnerschaftliche Ansatz und die Flexibilität, herauszustellen. Maßgeschneiderte Lösungen gemeinsam mit uns zu entwickeln, gehörte ebenso zur Kompetenz und dem Bestreben von Consileon wie, uns bis zur Erreichung eines Testates zu begleiten.“

Patrick Werner – Senior Vice President, Swiss Euro Clearing Bank

Was wir für Sie tun können

Consileon ist bei der SWIFT gelistet. Die folgenden Leistungen erhalten Sie von uns:

- ☑ Wir sind Ihr Partner für das externe Assessment und die CSCF-Zertifizierung.
- ☑ Wir helfen Ihnen, Ihre operative Cyber Security auf den notwendigen Standard für SWIFT zu heben.
- ☑ Wir designen mit Ihnen die IT-Architektur Ihrer SWIFT Secure Zone.
- ☑ Wir etablieren mit Ihnen einen robusten Cyber Incident Response Prozess, der den heutigen Bedrohungen standhält
- ☑ Wir führen Red-Teaming-Übungen durch. Das bedeutet, dass wir kontrollierte Angriffe auf Ihre IT-Systeme durchführen, um Sicherheitslücken aufzudecken.

Gerne berät Sie unser Experte für IT-Sicherheit

Jan Oetting | +49 152 22877905 | jan.oetting@consileon.de