Richtlinien

Bewertung des Geschäftspartners bezüglich der Internetsicherheit

Ein Leitfaden für die ersten Schritte

Inhalte

Qualifikationen und einschränkende Bedingungen

Dieses Dokument enthält allgemeine und nicht bindende Richtlinien für SWIFT-Benutzer, wie Internetsicherheitsdaten von Geschäftspartnern innerhalb des Ökosystems der Finanzdienstleistungen einzusetzen und auszulegen sind. Es enthält Vorschläge für das empfohlene Vorgehen bei der Kontrolle und für die Prozesse zum Austausch und zur Einbindung der Daten zum Internetsicherheitsrisiko in den bestehenden Risikomanagementrahmen des Instituts.

Es behandelt keine benutzerspezifischen Themen oder Anforderungen.

Die Informationen in diesem Dokument sind weder vollständig noch ersetzen sie eine solide Beurteilung oder die Compliance mit bewährten Vorgehensweisen.

Einzig und allein die Benutzer sind für aufgrund von Richtlinien und Empfehlungen ergriffene Maßnahmen und getroffene Entscheidungen sowie für die Auslegung der Daten, die in diesem Dokument dargelegt sind, verantwortlich. SWIFT lehnt jegliche Haftung in Bezug auf die Inhalte dieses Dokuments und die auf der Grundlage dieser Inhalte oder ihrer Folgen bzw. in Verbindung damit ergriffenen Maßnahmen und getroffenen Entscheidungen ab. Nichts in diesem Dokument darf so ausgelegt werden, als ob es eine Verpflichtung oder Zusicherung seitens SWIFT darstellt.

SWIFT stellt dieses Dokument nur zu Informationszwecken zur Verfügung. Die Information in diesem Dokument kann sich im Laufe der Zeit ändern. Benutzer müssen sich immer auf die letzte verfügbare Version beziehen.

Kundenstimme

Welche wesentlichen Herausforderungen sehen Sie bei der Anwendung des Internetrisikomanagements auf Ihre Geschäftspartner?

„Eine unserer wesentlichen Herausforderungen ist der Zugriff auf die bei unseren Geschäftspartnern bestehenden Internetkontrollen. Der Mangel an Kenntnissen über das Kontrollniveau bei den einzelnen Geschäftspartnern macht das Internetrisikomanagement so schwierig. Sie sind nur so stark wie Ihr schwächstes Glied. Das ist der Grund, warum eine sorgfältige Prüfung der Internetsicherheit der Geschäftspartner so wichtig ist.

Die Hauptprobleme sind unter anderem folgende:

- Die Ermittlung eines einheitlichen von allen Geschäftspartnern eingesetzten Standards, der zum Benchmarking eingesetzt werden kann
- Die Sicherstellung des Informationsaustausches mit den Geschäftspartnern hinsichtlich ihrer Sicherheitskontrollen oder dem Mangel daran
- Die Validierung der Richtigkeit der von den Geschäftspartnern bereitgestellten Informationen
- Die Nutzung und die Verarbeitung der Daten auf eine Weise, die dem Unternehmen wertvolle Risikodaten zur Verfügung stellt, so dass es sie verstehen und auf der Grundlage angemessene Geschäftsentscheidungen treffen kann
- Die Nachbereitung der Probleme, um zu gewährleisten, dass sie behoben und abgeschlossen werden, und die Vereinbarung der zwischenzeitlichen Einführung von Gegenmaßnahmen“

Kurzfassung

Die Internetsicherheit bleibt eine der größten Bedrohungen im Sektor Finanzdienstleistungen. Diese Richtlinie erläutert, wie Organisationen innerhalb des Bankenwesens und Zahlungsverkehrs an die Beurteilung des Internetsicherheitsrisikos durch ihre Geschäftspartner herangehen können, mit denen sie täglich Geschäfte tätigen.

Die Richtlinie bezieht sich auf vier Bereiche, die jedes Institut abdecken muss: die Einrichtung eines Steuerungsmodells; die Einrichtung von Rahmenbedingungen für das Internetsicherheitsrisikomanagement; Maßnahmen zur Bekämpfung des Internetsicherheitsrisikos und den Einbezug der von Geschäftspartnern eingehenden Daten zur „Attestation" der Internetsicherheit.

Internetsicherheitsrisiken müssen, einschließlich der Daten der Geschäftspartner, zusammen mit anderen betrieblichen, finanziellen und regulatorischen Arten von Risiken gesteuert werden. Viele Institute arbeiten daran, die Beurteilung des Internetrisikos in ihre bestehenden Prozesse für Geschäftspartner zu integrieren.

Die Aufsicht über diesen Prozess – die **Führungsstruktur** – muss so gestaltet werden, dass gewährleistet ist, dass die richtigen Mitarbeiter mit dem richtigen Verantwortungsbereich die Entscheidungsgewalt besitzen und dass die Prozesse solide und wiederholbar sind. Mit einer soliden Führungsstruktur können Institute die Umsetzung von Rahmenbedingungen für das **Internetsicherheitsrisikomanagement** angehen. Dies beinhaltet die Risikobeurteilung der Geschäftspartner durch Folgendes:

- Die Sammlung der notwendigen Daten, um risikoorientierte Entscheidungen zu unterstützen
- Die Verarbeitung dieser Daten und deren Übernahme in eine gewichtete, risikobasierte Bewertung, normalerweise dargestellt als numerisches Ergebnis oder als Ampel in rot-gelb-grün
- Ergreifung geeigneter Maßnahmen zur Behebung oder „Behandlung" des Risikos.

Institute können in unterschiedlichem Maße risikobereit sein, aber Maßnahmen zur Behebung des Internetsicherheitsrisikos können Folgendes einschließen:

- Die Einführung zusätzlicher Prüfungsebenen für Transaktionen der Geschäftspartner
- Die Beschränkung der Art der Transaktionen, die mit dem Geschäftspartner zusammen getätigt werden
- Die Anforderung an den Geschäftspartner, zusätzliche Kontrollen oder Maßnahmen zur Aufdeckung von Betrugsfällen einzuführen
- Die Anforderung an den Geschäftspartner, dass sie ihre Daten durch eine unabhängige Bewertung belegt
- die Neubeurteilung der mit dem Geschäftspartner abgeschlossenen Vereinbarungen und Kontrakte.

Im Rahmen dieses Steuerungsmodells und Risikomanagements sollten die Institute erwägen, Daten über die Internetsicherheitsvorsorge ihrer Geschäftspartner mit einzubeziehen.

Die Rahmenbedingungen des Customer Security Controls Framework (CSCF), das SWIFT als Teil seines Customer Security Programme (CSP) eingeführt hat, sind dafür außerordentlich wertvoll. Das CSCF beschreibt eine Reihe von für SWIFT-Benutzer verbindlichen und empfohlenen Sicherheitskontrollen und etabliert einen Grundschutz für die gesamte Gemeinschaft. Es muss von allen Benutzern in ihrer lokalen SWIFT-Infrastruktur eingeführt werden, die ihre Compliance mit den Vorschriften über verbindliche Sicherheitskontrollen selbst bestätigen müssen („Self-Attestation").

Wenn die Self-Attestations veröffentlicht werden, können Benutzer diese ihren Geschäftspartnern jeweils zur Verfügung stellen, wodurch anhand der einzelnen Kontrollen der Nachweis der Compliance erbracht wird, und ebenso können Geschäftspartner sie voneinander anfordern. Benutzer können die Daten zu ihrer besseren „**Nutzung**" und ihrer besseren Integration in ihren risikobasierten Entscheidungsrahmen entweder von Geschäftspartner zu Geschäftspartner oder in der Masse anzeigen und exportieren.

Das CSCF hilft dabei, die Transparenz und Standardisierung in der Gemeinschaft zu erhöhen, damit Organisationen die Internetsicherheit besser in ihre Entscheidungsfindung mit einbeziehen zu können. Diese „Self-Attestation"-Daten sind reich in der Gestaltung und eine einzigartige Quelle von Internetsicherheitsrisikodaten für SWIFT-Benutzer.

Kontext

Bedrohungen der Internetsicherheit und Betrugsrisiko sind weltweit eine große Gefahr. Die Raffinesse der Bedrohungsakteure nimmt zu, massive Datenschutzverletzungen sind normal. Praktisch jeder kann Opfer von Cyber-Angriffen, die eine fortgeschrittene anhaltende Bedrohung darstellen, werden und dank des „Internet of Things“ können allgegenwärtige „intelligente“ Geräte als Waffe für verteilte Überlastangriffe (DDoS) eingesetzt werden.

Im Rahmen von Finanzdienstleistungen geht von diesen Bedrohungsakteuren durch raffinierte Angriffe auf die Internetsicherheit eine Bedrohung aus, deren Hauptmotiv es ist, vom Opfer **Vermögenswerte zu erbeuten**.

Aber natürlich arbeiten Organisationen innerhalb des Bank- und Zahlungsverkehrs nicht in einem Vakuum – sie arbeiten täglich mit einer Vielzahl von Geschäftspartnern zusammen und tätigen Geschäfte mit ihnen. Das Risiko ist real, da die Internetangriffe auf SWIFT-Kunden von einer kleinen Anzahl raffinierter und gut finanzierter Bedrohungsakteure ausgeht. **Wie muss eine Organisation das mögliche Risiko sehen und behandeln, dass sie Geschäfte mit einem ahnungslosen Opfer eines Internetangriffs macht?** Wenn das Risiko nicht bewältigt wird und Finanzmittel verloren gehen, kann das Finanzrisiko beträchtlich sein.

Diese Richtlinie betrachtet, wie eine Organisation die Bewertung des Internetsicherheitsrisikos angehen kann, das durch ihre Geschäftspartner besteht, und bezieht sich auf vier Hauptbereiche:

- Die Einrichtung eines Steuerungsmodells für Internetsicherheitsrisikomanagement
- Die Einrichtung von Rahmenbedingungen für das Internetsicherheitsrisikomanagement
- Übernahme von Maßnahmen zur Risikominimierung in Bezug auf Internetsicherheit
- Der Einbezug von Internetsicherheits-Attestation-Daten der SWIFT Geschäftspartner.

Im folgenden Dokument werden diese vier Themen erörtert.

Kundenstimme

Haben Ihnen die Internetsicherheits-Attestation-Daten dabei geholfen, mindestens eine dieser Herausforderungen zu meistern, und wenn ja, wie?

„Der Kundensicherheits-Attestation-Prozess von SWIFT hat unser allgemeines Managementprogramm für Mitglieder ergänzt, mit dem diese Herausforderungen gemeistert werden. Durch den Erhalt der Attestation-Daten können wir jetzt die Ebene der eingeführten Kontrollen der Geschäftspartner verstehen. Durch das Verständnis der Art und Ebene der bei jedem Geschäftspartner eingeführten Kontrollen sind wir eher in der Lage, das Internetsicherheitsrisiko zu steuern.

Das SWIFT CSP stellt uns einen einheitliches Maßnahmenbündel zur Verfügung, das von allen Geschäftspartnern genutzt werden und für das Benchmarking eingesetzt werden kann. Es ist für uns das, was die SAT-Prüfung für ein US-Hochschulzulassungsteam ist. Das Attestation-Tool ist für die Anforderung und Erteilung der Zugriffsberechtigung eines Geschäftspartners sehr einfach einzusetzen. Das SWIFT CSP Programm unterstützt den Grad des Vertrauens, das wir in die Maßnahmen des Geschäftspartners setzen, indem es dem Geschäftspartner Mittel an die Hand gibt, damit ihre Maßnahmen durch interne Revision oder externe Prüfung bestätigt werden. Wir entwickelten ein quantitatives Modell, um die Daten aus dem Attestation-Tool zu verarbeiten und Berichte und Schaubilder zu erstellen.“

Einrichtung eines Steuerungsmodells für das Internetsicherheitsrisikomanagement

Internetsicherheitsrisiken, auch von Geschäftspartnern ausgehende, müssen zusammen mit sonstigen Risikoarten betrieblich, finanziell und regulatorisch gesteuert werden.

Die Aufsicht über den Risikomanagementprozess – die Führungsstruktur – muss so gestaltet werden, dass gewährleistet ist, dass die richtigen Mitarbeiter mit dem richtigen Verantwortungsbereich die Entscheidungsgewalt besitzen, dass die Prozesse solide und wiederholbar sind und dass Ausnahmen bewältigt werden können.

Die Struktur des Führungsausschusses

Die Führungsstruktur in Bezug auf das Internetsicherheitsrisiko muss als ganzheitliche Funktion betrachtet werden. Das bedeutet, es wird zentral von den für die Geschäftstätigkeit als Ganzes Verantwortlichen beaufsichtigt statt sich auf eine isolierte Backoffice-Funktion in der IT oder im Betrieb zu beschränken. In der Praxis muss das Risikomanagement bezüglich Geschäftspartnern Teil (oder Unterabteilung) einer **Führungsausschuss-Struktur wie dem Risikoausschuss** mit eigenem Auftrag und ausreichenden Ressourcen sein.

Innerhalb der fachübergreifenden Kontrolle muss auch die Ausrichtung der Verantwortungsbereiche anhand der „drei Verteidigungslinien“ erwogen werden. In der Praxis bedeutet das, dass die täglichen das Betriebsrisiko betreffenden Entscheidungen in der ersten Linie (z. B. Geschäftstätigkeit, Betrieb, IT/Internet), da dort die Verantwortung für die Ausführung der internen Kontrollen und betrieblichen Verfahren liegt. Ausnahmen und Eskalationen werden in der zweiten Verteidigungslinie verwaltet (z. B. Compliance mit den Vorschriften, Risiko) da diese Unternehmensbereiche betrieblich ein gewisses Maß an Unabhängigkeit besitzen. Die Sicherheit wird von der dritten Verteidigungslinie überwacht (z. B. interne Revision), die unabhängig ist.

Geschäftlich orientierte Stakeholder

Die Führungsaufgaben werden von Mitarbeitern mit entsprechender Seniorität ausgeführt, welche die Macht haben, wirkungsvolle Entscheidungen über die richtigen internen Stakeholder-Gruppen hinaus zu treffen.

Sicherlich müssen viele der täglichen das Betriebsrisiko betreffenden Entscheidungen über das Geschäftspartner-Management von **Geschäftsleuten** getroffen werden statt ausschließlich von Ingenieuren oder Spezialisten für Internetsicherheit. Allerdings muss die Gesamtführungsstruktur ganzheitlich sein und Vertreter folgender Bereiche umfassen:

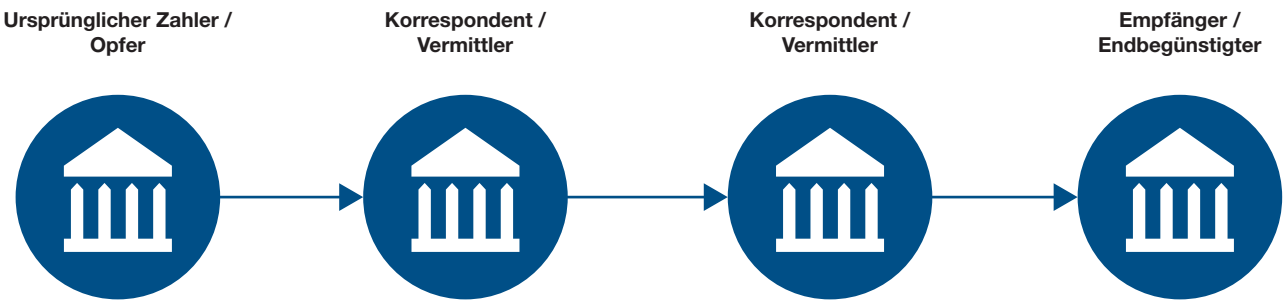
- **Beziehungsmanagement** in den Bereichen Geschäftstätigkeit und Geschäftspartner, um Markt- und Geschäftspartnerrisiko zu bewerten und die Verbindung mit dem Geschäftspartner zu halten
- **Zahlungsabläufe** zur Umsetzung betrieblicher Kontrollen, Anpassung von Limits und Eingriffe in normale Geschäftsabläufe
- **Technik,** z. B. IT/Informationssicherheit/ Internetsicherheit, um die Umsetzung zusätzlicher technischer Kontrollen oder spezieller Maßnahmen zur Betrugsaufdeckung anzufordern
- **Risiko, Compliance mit den Vorschriften und interne Revision,** um Ausnahmen zu steuern und unabhängige Sicherheitsprüfungen durchzuführen.

Aufgrund der Sensibilität der Daten und der möglichen Auswirkung auf Sicherheitsgefährdungen, beaufsichtigt eine Führungskraft diesen Prozess, und diese Führungskraft trägt zur Risikobewertung und zum Eskalationsprozess bei und beaufsichtigt die sich daraus ergebenden Entscheidungen über Maßnahmen.

Klarer Auftrag

Der Führungsausschuss, der das Geschäftspartnerrisiko beaufsichtigt, muss einen klar umrissenen Auftrag bzw. eine klare Aufgabenstellung haben, worin die längerfristige Strategie sowie das tägliche Betriebsmodell, einschließlich Aufgaben und Verantwortungsbereiche beschrieben werden. Laut diesem Auftrag müssen das Aufsichtsgremium und die Führungskräfte auch regelmäßig über den Stand des Geschäftspartnerrisikos, bestimmte Vorfälle und die Entwicklung sowie die Trends informiert werden.

Rahmenbedingungen für die Bewertung des Geschäftspartners bezüglich der Internetsicherheit



Diese Richtlinien sind bestimmt für:

- **Kleine und mittelständische Unternehmen**, die vom ursprünglichen Zahler Anweisungen erhalten. Diese SMEs verfügen im Vergleich zu größeren Instituten, die mehrere Beziehungen zu Geschäftspartnern sowie komplexe interne Strukturen haben, nur über eine beschränkte Anzahl von Geschäftspartnern.
- **Korrespondenzbanken**, die (unabhängig von ihrer Größe) als Vermittler der Transaktion zwischen dem ursprünglichen Zahler und dem Endbegünstigten agieren.

Kundenstimme

Können Sie beschreiben, wie Sie die Internetsicherheits-Attestation-Daten konkret verwenden, und zwar über die einfache Übermittlung Ihrer Self-Attestation im Tool hinaus; genauer gesagt, wie Sie diese Daten im Rahmen des Sicherheitsrisikomanagements für Ihre Geschäftspartner einsetzen?

„Das Attestation-Tool bietet einheitliche Antworten, daher ist es uns möglich, jede Attestation zu bewerten und basierend auf den Antworten einen numerischen Wert zu vergeben. Dadurch können wir wiederholbare quantitative und qualitative Maßnahmen für jede Attestation einzusetzen. Im Vorfeld haben wir uns lediglich auf Fragebögen verlassen, die in vielen Beispielen widersprüchliche Antworten enthielten."

Einrichtung von Rahmenbedingungen für das Internetsicherheitsrisikomanagement

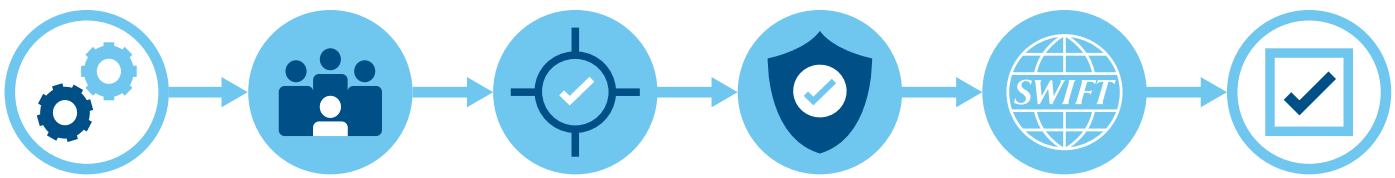
Mit einer soliden Führungsstruktur betrachten Institute normalerweise die Internetsicherheit aus einer Risikoperspektive heraus. Das bedeutet, dass sie die Höhe des Risikos bewerten und Budget investieren, wo es am nötigsten ist, und das Risiko dort akzeptieren, wo der entsprechende Schwellenwert oder die entsprechende Risikobereitschaft nicht erreicht wird. Dieser Prozess bzw. diese Rahmenbedingungen des Internetsicherheitsrisikomanagements umfassen mehrere Maßnahmen:

1. **Die Erhebung der erforderlichen Geschäftspartner-Risikodaten**

2. **Die Bewertung des Risikoniveaus durch die Verarbeitung der Daten. Normalerweise erfolgt diese Bewertung durch die Zuordnung eines Gesamtergebnisses, dass dann mit dem Umfang der Risikobereitschaft des Unternehmens abgeglichen wird**

3. **Auf der Grundlage des Risikoergebnisses die Durchführung geeigneter Maßnahmen zur Steuerung oder „Behandlung“ der Risiken.**

Die Rahmenbedingungen für die Bewertung des Geschäftspartners bezüglich der Internetsicherheit



Einrichtung eines **Steuerungsmodells** für Internetsicherheitsrisikomanagement

Schaffen von Rahmenbedingungen für das **Internetsicherheitsrisikomanagement**

Einsatz von **Gegenmaßnahmen** zur Behebung des Internetsicherheitsrisikos

Einbeziehen der **Internetsicherheits-Attestations-Daten** der SWIFT-Geschäftspartner

Daten zum Geschäftspartner

Die Institute erfassen und verarbeiten eine Vielzahl von Daten, um das Risikoprofil der Geschäftspartner in Bezug auf die Internetsicherheit zu bestimmen.

Die Risikodaten kann man, grob gesagt, in drei Kategorien unterteilen: sich aus dem externen Umfeld der Geschäftstätigkeit der Geschäftspartner ergebende Daten; die Geschäftsbeziehung mit dem Geschäftspartner beschreibende Daten; und transaktionelle Daten.

1. Sich aus dem externen Umfeld der Geschäftstätigkeit des Geschäftspartners ergebende Risiken

- **Land/Region der Geschäftstätigkeit** – Kann auf der Ebene von Internetsicherheit, Regulierung und Straftat/Betrug im Rechtshoheitsgebiet der Geschäftstätigkeit des Geschäftspartners als Maßnahme dienen. Die Bewertung kann unter Heranziehung öffentlich zugänglicher Quellen wie des Basler Geldwäscherisikoberichts beurteilt werden
- **Art der Branche** – Daraus ergibt sich die Wahrscheinlichkeit eines Angriffs, da einige Sektoren häufiger als andere unter Internetsicherheitsangriffen und Datenschutzverletzungen leiden
- **Grad der regulatorischen Aufsicht** über den Geschäftspartner und das Ausmaß, in dem die örtliche Aufsichtsbehörde Richtlinien oder Grundsätze zur Internetsicherheit erlässt.

2. Risiken in Bezug auf die Geschäftsbeziehung zum Geschäftspartner

- **Tiefe / Länge der Beziehung zum Geschäftspartner** – Jüngere Beziehungen beinhalten möglicherweise ein höheres Risiko als längerfristig bestehende, tiefe und vertrauensvolle Beziehungen
- **Größe / Mehrheitsverhältnisse der Geschäftspartner** – Daraus ergibt sich die Verfügbarkeit an Budget, kompetenten Mitarbeitern und Tools, um Bedrohungen zu bekämpfen, insbesondere wenn die betreffenden Geschäftspartner Teil einer größeren Gruppe sind, z. B. der global systemrelevanten Banken
- **Bekannte Internet- oder Sicherheitsvorfälle** und sonstige verfügbare Nachrichten, Informationen oder Materialien zur Sorgfaltsprüfung
- **Bestehende Risikobewertungen der Geschäftspartner,** z. B. betrieblich, finanziell und regulatorisch.

3. Transaktionsrisiken

- **Arten von Transaktionen** – Beschränkung der Art der mit dem Geschäftspartner getätigten Transaktionen, da bestimmte Transaktionsarten, zum Beispiel Zahlungen, von Natur aus angreifbarer sind als andere, z. B. Auszüge
- **Transaktionswert** – Dient als Darstellung des Kreditrisikos
- **Transaktionshäufigkeit** – Je größer der Umfang der Transaktion pro Periode ist, desto größer ist die mögliche Angriffsfläche.

Nach der Erhebung dieser Geschäftspartnerdaten wird der Prozess der Risikobewertung angewandt.

Risikobewertungsprozess

Nach der Erhebung von Geschäftspartnerdaten verarbeiten und übertragen die Institute sie in eine risikobasierte Bewertung. Diese Bewertungsmethode kann von Institut zu Institut variieren, folgt aber allgemein einem von drei Ansätzen:

- **Expertenbasiert** – die Bewertung wird durch ein Expertenurteil und eine qualitative Beurteilung der Risiken durch Spezialisten
- **Regelbasiert** – die Bewertung erfolgt über einen Entscheidungsbaum unter Verwendung einfacher Regeln, wie der Geschäftspartner gegenüber jedem Risikofaktor abschneidet.
- **Modellbasiert** – die Bewertung wird analytisch daraus abgeleitet, wie der Geschäftspartner gegenüber jedem gewichteten Risikofaktor abschneidet.

Ungeachtet des gewählten Ansatzes wird der Geschäftspartner normalerweise eine Gesamtpunktzahl zugewiesen, die in der Regel als Ampel (rot, gelb oder grün) dargestellt wird.

Das Risiko abschwächende Maßnahmen hängen von dieser Bewertung im Vergleich mit der internen Risikobereitschaft ab. Zum Beispiel können Geschäftspartner mit einer geringen oder grünen Bewertung als keiner weiteren Prüfung bedürfend eingestuft werden, während Geschäftspartner mit einer hohen oder roten Bewertung für das Risiko abschwächende Maßnahmen ausgewählt werden können.

Einführung von das Internetsicherheitsrisiko abschwächenden Maßnahmen

Die Rahmenbedingungen zum Risikomanagement können es einem Institut ermöglichen, das mit einem Geschäftspartner verbundene Ausmaß des Sicherheitsrisikos zu bewerten und einzustufen. Das Institut kann sich dann entscheiden, dieses Risiko anzunehmen oder das Risiko abschwächende Maßnahmen in Betracht ziehen.

Die das Internetsicherheitsrisiko abschwächende Maßnahmen können Folgendes beinhalten:

1. Maßnahmen in Bezug auf die Geschäftsbeziehung mit dem Geschäftspartner

- Eine proaktive **Kontaktaufnahme mit den Führungskräften**, um die Beziehung zu verstärken und eine allgemeine Beruhigung herzustellen
- Die Aufforderung an den Geschäftspartner, über eine interne Bewertung oder einen Dritten bzw. eine externe unabhängige Bewertung oder über die Beibringung von Unterlagen über technische Daten oder Prüfungsergebnisse **Nachweise für ihre Informationen** zu erbringen
- Die Aufforderung an den Geschäftspartner, **zusätzliche Kontrollen** oder Maßnahmen zur **Betrugsaufdeckung** einzuführen
- Die Neubewertung der **Vereinbarungen und Verträge** des Geschäftspartners, einschließlich der Möglichkeit der Verminderung des durch den Geschäftspartner verursachten Risikos oder der Änderung bzw. Beendigung des Vertrages.

2. Maßnahmen in Bezug auf eine strengere transaktionelle Kontrolle des Geschäftspartners

- Die Kennzeichnung zur Überprüfung von Transaktionen, die **vordefinierte Grenzwerte** verletzen. Dazu können Transaktionstyp, Transaktionswert, Transaktionswährung und das Profil des Endbegünstigten gehören
- Die Einführung einer **zusätzlichen genauen Prüfung**, z. B. einer persönlichen Aufsicht durch zwei Personen bzw. einer bilateralen Verifizierung der mit dem Geschäftspartner getätigten Transaktion in Bezug auf alle gekennzeichneten Transaktionen.

Die obige Liste von Maßnahmen ist nicht als vollständig anzusehen, und die Institute können sonstige Kontrollen und Tools haben, die sie zur Risikosteuerung einsetzen können.

Ergreifen von Maßnahmen bei Geschäftspartnern mit höherem Risiko

Bei Geschäftspartnern mit höherem Risiko können Institute eine Kombination der oben genannten Maßnahmen einsetzen. Normalerweise wird ein Institut zusätzliche Prüfungen durchführen und Zahlungsanweisungen über einem vorgegebenen Wert oder einer vorgegebenen Menge überwachen wollen. das Institut muss Schwellenwerte anpassen können und auch die Tools und die Kapazitäten besitzen, um eine zunehmende Anzahl von Warnungen zu bearbeiten sowie zusätzlich Transaktionen manuell zu verarbeiten, auch wenn sie aktuelle Kontaktdaten des Geschäftspartners benötigen.

Dieser Zustand zunehmender Prüfungen muss nicht zwingend dauerhaft sein. Sobald der Geschäftspartner es schafft, wieder in die Kategorie „geringes“ Risiko eingestuft zu werden, zum Beispiel weil sie zusätzliche Maßnahmen einhält, können Schwellenwerte geändert oder gestrichen werden.

Über jegliche Entscheidungen zur Einführung abschwächender Maßnahmen hinaus bleibt jedes Institut alleine für die vollständige oder teilweise Veränderung, Aussetzung oder Beendigung der Beziehung zum Geschäftspartner verantwortlich.

Wenn der Internetsicherheitsrisikomanagement-Prozess vorhanden ist, ist die Führungsstruktur gut beraten, periodische Überprüfungen des Geschäftspartners durchzuführen, um zu beurteilen, ob sich ihr Risikoprofil geändert hat.

Kundenstimme

Wie werden die Internetsicherheits-Attestation-Daten in das Internetsicherheitsmanagement eingespeist und welche Führungsgremien werden diesbezüglich organisiert.

„Neben anderen Risikoabteilungen werden unserem Chief Risk Officer wöchentliche Berichte zugesandt. Wir verfolgen die Anzahl der gewährten Attestations im Vergleich zur Anzahl der anhängigen Anfragen. Jede der gewährten Attestations bewerten wir nach dem Risiko und bringen dann jede Attestation-Bewertung in ein Qualitätsprofil ein. Unsere Risikoabteilungen haben damit begonnen, die Profilergebnisse in ihre Disziplinen einzubeziehen.“

Anhang A: Einbezug der Attestation-Daten von SWIFT-Geschäftspartnern

Das im Mai 2016 eingeführte SWIFT Customer Security Programme (CSP) unterstützt alle SWIFT-Benutzersegmente, indem die Sicherheit ihrer lokalen SWIFT-bezogenen Infrastruktur verstärkt wird.

Die SWIFT Customer Security Controls Policy (CSCP) definiert den Attestation-Prozess des Benutzers und die dazugehörigen Grundsätze, Aufgaben und Verantwortlichkeiten. SWIFT entwickelte auch ein Customer Security Control Framework (CSCF), welches einen Grundschutz für verpflichtende und empfohlene Kontrollen für die gesamte Benutzergemeinschaft einführt.

Die CSCP Policy verpflichtet die Benutzer zur Self-Attestation der Compliance mit einer Reihe von **verpflichtenden Sicherheitskontrollen** und ermutigt sie auch zur Self-Attestation der Compliance mit einer Reihe von empfohlenen Kontrollen. Sie bescheinigen ihren Grad der Compliance, und ihre **Attestation** wird durch die von SWIFT zur Verfügung gestellte Anwendung KYC Security Attestation (KYC-SA) veröffentlicht und verwaltet.

Eine im KYC-SA Tool verfügbare Hauptfunktion ist die Möglichkeit für Institute, durch eine einvernehmliche Regelung mittels **Zugriffsanforderung und -gewährung** Attestation-Daten mit ihren Geschäftspartnern auszutauschen. Auf diese Weise können Institute das Geschäftspartnerrisiko bewerten und dann auf der Grundlage der durch die Attestation bescheinigten Compliance Entscheidungen darüber zu treffen. Die Attestation-Daten sind sehr informativ und eine einzigartige Quelle für die Daten des Geschäftspartnerrisikos aufgrund der Internetsicherheit.

Wenn Institute damit beginnen, CSP Attestation-Daten in ihre Rahmenbedingungen zum Geschäftspartnerrisiko zu integrieren, ist eine Anzahl von Faktoren zu berücksichtigen:

- Erwägungen zum Steuerungsmodell
- Erwägungen zu den Rahmenbedingungen des Risikomanagements
- Weitere Optionen für abschwächende Maßnahmen.

Diese drei abzuwägenden Bereiche werden im Folgenden innerhalb des Gesamtzusammenhangs des KYC-SA Tools dargelegt.

Es ist wichtig hervorzuheben, dass nur die bescheinigenden Benutzer für ihre Attestation verantwortlich sind und SWIFT deren Richtigkeit nicht bestätigt. Das CSP ist zur Schaffung eines **Standardisierungs-** und **Transparenzniveaus** beim Austausch von Sicherheitsdaten konzipiert, die dann von SWIFT-Benutzern eingesetzt werden können.

Beachten Sie, dass Anhang B Links zu den CSCF-Rahmenbedingungen und zur CSCP-Grundsatzdokumentation beinhaltet.

Anhang B beinhaltet Verbindung der KYC-SA Benutzerrichtlinien, die Schritt für Schritt angeben, wie der Zugriff auf die Attestation-Daten angefordert/gewährt wird und die Attestation-Daten als Excel-Datei exportiert werden. Der Export der Attestation-Daten kann durch den Security Officer der Organisation Geschäftspartner für Geschäftspartner oder insgesamt für alle maßgeblichen Geschäftspartner erfolgen. Allerdings beschreiben diese Richtlinien nicht, wie eine Organisation die Daten nutzen soll, z. B. die Zuordnung der Führungsstruktur, Verarbeitung der Daten, Bewertung des Risikos und Zuordnung von Maßnahmen. Diese Leitlinien werden nachstehend behandelt.

Kundenstimme

Worin besteht die Führungsstruktur in Bezug darauf, Geschäftspartnern den Zugriff auf Ihre Attestation-Daten zu gewähren? Ist das eine geteilte Verantwortung (z. B. zwischen den Abteilungen Risiko, Compliance, Recht usw.)?

„Der Führungsprozess in Bezug darauf, Geschäftspartnern den Zugriff auf Ihre Attestation-Daten zu gewähren, erfordert die Teilnahme mehrerer Teams. Es ist sicherzustellen, dass bei der Gewährung von Zugriff auf unsere Attestations Transparenz besteht. Wir haben einen internen Workflow-Genehmigungsprozess. Nach der internen Genehmigung übernimmt das Administrationsteam mit dem Attestation-Tool die Gewährung des Zugriffs."

Erwägungen zum Steuerungsmodell

Vor der Entscheidung zum Austausch von Attestation-Daten oder der Anfrage an Andere über deren Austausch muss der Gesamtprozess zur Nutzung der Attestation-Daten der Geschäftspartner definiert werden. Insbesondere ist einzubeziehen, wie der Austausch stattfindet und wer welche Aufgabe übernimmt.

Während SWIFT die technische Plattform bietet, muss das Steuerungsmodell der Institution auch angepasst werden, um die Beurteilung der Attestation-Daten in Bezug auf die Sicherheit der Geschäftspartner zu unterstützen. Für die „Gewährung“ und „Anforderung“ des Zugriffs auf die Attestation-Daten müssen geeignete Vertreter des Instituts vorgesehen werden, und die Daten müssen als zusätzliches Element innerhalb der bestehenden Rahmenbedingungen des Geschäftspartnerrisikomanagements angesehen werden.

Gewährung (oder Ablehnung) des Zugriffs auf Geschäftspartner

Um Zugriff auf einen anfordernden Geschäftspartner zu gewähren, muss das Steuerungsmodell klar den Geschäftseigentümer identifizieren, der die Genehmigung zur Entscheidung („Ja“ oder „Nein“) erteilt. Ohne einen klaren „Gewährer“ bleiben eingehende Attestation-Anfragen in der Warteschlange und werden nicht beantwortet.

Das zur Genehmigungsentscheidung hinsichtlich eingehender Anfragen eingesetzte Kriterium wird normalerweise von einer Führungsausschussstruktur oder von Angehörigen der Geschäftsleitung, wie etwa dem CISO, Leiter der Rechtsabteilung oder Chief Compliance Officer abgezeichnet.

Beispiele für die vom „Gewährer“ in Bezug auf den Zugriff der Geschäftspartner verwendeten Entscheidungskriterien

- Die Attestation-Daten werden, ungeachtet ihres Landes, mit globalen Transaktionsbanken ausgetauscht
- Die Attestation-Daten werden mit den Geschäftspartnern im gleichen Land und unter der gleichen Aufsichtsbehörde ausgetauscht
- Die Attestation-Daten werden dann ausgetauscht, wenn wir berichten können, dass unser „Attestation Type“ von einer externen Bewertung unterstützt wird
- Die Attestation-Daten werden mit allen anfordernden Geschäftspartnern geteilt, mit denen wir einen aktiven Datenaustausch betreiben
- Die Attestation-Daten werden mit anfordernden Geschäftspartnern ausgetauscht, die ihre Attestation-Daten auch mit unserem Institut austauschen
- Attestation-Daten werden mit allen anfordernden Geschäftspartnern ausgetauscht

Die Führungsausschussstruktur bzw. die Geschäftsleitung muss die Entscheidungskriterien unterzeichnen. Danach kann die mittlere Führungsebene sie auf eingehende Anfragen anwenden und technischen Benutzern die Entscheidung zur Gewährung oder Ablehnung von Zugriff zukommen lassen.

Ausnahmen werden bis zur Führungsausschuss-struktur oder zur Geschäftsleitung eskaliert.

Auf einer betrieblichen Ebene fassen die Benutzer (oder „Gewährer“) die erhaltenen Anfragen und ergriffenen Maßnahmen regelmäßig (z. B. wöchentlich) in einem Bericht an das Management zusammen.

Beispiel für den Prozessablauf bei der Zugriffsgewährung

1. Zuordnung der Aufgabe „Gewährer“ zu einem Benutzer
2. Eingang einer Zugriffsanforderung von einem Geschäftspartner beim Benutzer
3. der Benutzer überprüft die Anfrage in Bezug auf die Genehmigungskriterien und empfiehlt eine positive oder negative Antwort
4. Die mittlere Führungsebene überprüft die Empfehlung und gibt die Genehmigung zur Ausführung, trifft eine alternative Entscheidung oder eskaliert an die Geschäftsleitung.
5. Der Benutzer „gewährt“ die Anforderung des Geschäftspartners oder „lehnt ab“. Im Falle der Ablehnung des Zugriffs muss der Benutzer in der Lage sein, einen Grund für die Ablehnung zu nennen. Ein Grund ist zum Beispiel, dass keine Beziehung zum Geschäftspartner besteht oder dass man nicht bereit ist, zu diesem Zeitpunkt Attestation-Daten auszutauschen
6. Der Benutzer fasst die Status-Anfragen und Maßnahmen regelmäßig, z. B. wöchentlich, in einem Bericht zusammen

Das Attestation-Tool bietet auch die Möglichkeit, eine „White List“ der BIC derjenigen Geschäftspartner zu erstellen, welche die von der Geschäftsleitung festgelegten Kriterien erfüllen. Dadurch kann diesen Geschäftspartnern auf Anfrage der Zugriff automatisch gewährt und eine manuelle Überprüfung sowie der betreffende Genehmigungsprozess vermieden werden. Diese Eigenschaft ist als „Auto-Grant“ bekannt.

Anforderung von Zugriff auf Geschäftspartner

Die Führungsausschussstruktur bzw. Geschäftsleitung unterzeichnet möglichst die Kriterien zur Gewährung von Zugriff für Geschäftspartner. Die Kriterien für die Anforderung der Attestation-Daten der Geschäftspartner wird dann gleicher Ebene entschieden.

Beispiele für die vom „Anforderer" bei der Anforderung von Zugriff auf Daten von Geschäftspartnern verwendeten Entscheidungskriterien

- Wir fordern von allen unseren Geschäftspartnern Attestation-Daten an
- Wir fordern Attestation-Daten nur von Geschäftspartnern an, mit denen wir nicht regelmäßig zusammenarbeiten
- Wir fordern Attestation-Daten nur von Geschäftspartnern an, die in einem Hochrisiko-Gebiet ansässig sind
- Wir fordern Attestation-Daten nur von Geschäftspartnern an, die bereits als hochriskant eingestuft sind

Nach der Festlegung von Entscheidungskriterien durch die Geschäftsleitung werden die Attestation-Anforderungen im Attestation-Tool durch einen Benutzer („Anforderer") ausgeführt.

Der Status der Anforderungen in Bezug auf den Zugriff auf die Attestation-Daten eines Geschäftspartners wird dem Management regelmäßig (z. B. wöchentlich) berichtet – das gleiche gilt für die Statusberichterstattung in Bezug auf die Gewährung von Zugriff an Geschäftspartner.

Beispiel für den Prozessablauf bei einer Zugriffsanforderung

1. Zuordnung der Aufgabe „Anforderer" an einen Benutzer
2. Die Geschäftsleitung legt Entscheidungskriterien für die Anforderung von Zugriff auf Attestation-Daten der Geschäftspartner fest
3. Der Benutzer sendet die Anforderung über das Attestation-Tool an den Geschäftspartner
4. Der Geschäftspartner „gewährt" die Zugriffsanforderung oder „lehnt ab". In Fällen, wenn eine Anforderung abgelehnt wird, überdenkt die Geschäftsleitung weitere Geschäfte mit dem Geschäftspartner und fordert den Zugriff nach der Behebung des Grundes für die Ablehnung erneut an
5. Der Benutzer fasst die Status-Anfragen und Maßnahmen regelmäßig, z. B. wöchentlich, in einem Bericht zusammen

Kundenstimme

Gingen bei Ihnen im Zuge der Gewährung von Zugriff auf die Attestation-Daten der Geschäftspartner Informationen ein, die Sie veranlasst haben, eine wichtige Entscheidung über die Internetsicherheit zu treffen? Wenn ja, können Sie dies näher ausführen?

„Sobald wir Zugriff auf Attestation-Daten des Geschäftspartners gewährt haben, überprüfen wir die Reaktion auf die Kontrollen. Obwohl wir noch keine Entscheidungen zur Internetsicherheit auf der Grundlage der Attestation eines Geschäftspartners getroffen haben, orientieren sich unsere internen Gespräche über Infizierungsgefahren aus dem Internet an den Antworten von Geschäftspartnern."

Erwägungen zu den Rahmenbedingungen des Risikomanagements

Organisationen, denen der Zugriff auf die Attestation-Daten der Geschäftspartner gewährt wird, können das Tool verwenden, um die Daten zu nutzen. Diese Attestation-Daten, die den Grad der Compliance pro Kontrolle beinhalten, werden in die Rahmenbedingungen für die risikobasierte Entscheidung der Organisation integriert, um zur Steuerung des durch den Geschäftspartner dargestellten Risikos beizutragen.

Institute, die Attestation-Daten über Internetsicherheit in ihren bestehenden Risikomanagementprozess einbinden möchten, können auf diesen Informationen basierende Gewichtungen und Bewertungen anwenden.

Beispiele für die Ansetzung von Gewichtungen und Bewertungen

- Wenn keine Attestation des Geschäftspartners vorliegt, muss sie bewertet werden
- Wenn der Geschäftspartner nicht auf KYC-SA Zugriffsanforderungen antwortet, wird sie bewertet
- Die Compliance mit den einzelnen CSCF-Kontrollen muss bewertet werden: z. B. die Compliance mit den Richtlinien, die Compliance durch alternative Mittel, der Mangel an Compliance oder die zukünftige Compliance ab dem vorgegebenen Datum
- Jeder speziellen verbindlichen oder empfohlenen Kontrolle kann eine unterschiedliche Gewichtung zugeordnet werden
- Sonstige Variablen in der Attestation können besonders gewichtet werden, wie etwa Folgende:
  - **Die Infrastrukturart**
  - **Die Komponenten der Infrastruktur** – nutzt der Geschäftspartner eine zertifizierte Schnittstelle?
  - **Dienstleister** – verbindet sich der Geschäftspartner durch einen Dienstleister und welchen Status der Zertifizierung oder Compliance hat dieser Anbieter?
  - **Bewertungsart** – hat der Geschäftspartner interne oder externe Berater engagiert, oder wurde ihre Attestation durch eine interne oder externe unabhängige Bewertungsstelle begründet? Siehe unten

Die Zuordnung aussagekräftiger Gewichtungen und Bewertungen ist eine Genauigkeit erfordernde Aufgabe, wofür die Institute die Zusammenarbeit der internen Stakeholder gewährleisten müssen, wie etwa der Abteilungen für Informationssicherheit, Betrieb, Technik, Risiko, Compliance, Geschäft und Recht sicherstellen müssen.

Die Auslegung der „Bewertungsart“

Dieses Feld in der Self-Attestation erfasst den Umfang, in dem der Geschäftspartner unabhängige Gutachter einsetzt, um den in der Self-Attestation enthaltenen Grad der Compliance zu belegen.

– **Unabhängige Bewertung durch Dritte (die eine externe Prüfung beinhalten kann)** – das Institut bestätigt die Compliance mit der Kontrolle durch den Einsatz eines unabhängigen externen Gutachters. Sein Name muss in der Self-Attestation des Instituts genannt werden. – **Interne unabhängige Bewertung (die eine interne Revision beinhalten kann)** – das Institut bestätigt die Compliance mit der Kontrolle durch den Einsatz eines internen Gutachters.	Kann einen höheren Grad von angemessener Sicherheit zulassen, dass der jeder Kontrolle zugeordnete Compliancestatus unabhängig bestätigt ist. Kann einen höheres Niveau an Vertrauen in den Geschäftspartner voraussetzen, die dieses Sicherheitsniveau bereitstellen. Ermöglicht die Prüfung des Namens des externen Gutachters.
– **Beratende Prüfung durch ein externes Unternehmen** – das Institut hat einen Dritten für beratende Leistungen hinsichtlich ihrer Compliance-Bewertung engagiert. Der Name des Dritten muss in der Self-Attestation des Instituts genannt werden. – **Beratende Prüfung durch interne unabhängige Teams** – das Institut engagiert eine unabhängige interne Stelle für beratende Leistungen hinsichtlich ihrer Compliance-Bewertung.	Kann zu einem gewissen Vertrauen in die unabhängige Bestätigung des angeführten Kontrollstatus führen. Empfohlene Bewertungen werden nicht unter festen, vordefinierten Rahmenbedingungen ausgeführt. Das Vertrauen kann stärker sein, wenn ein vollständiger Bewertungsbericht erstellt wird und verfügbar ist. Kann durch eine gezielte Bewertung oder eine Stichprobenkontrolle ergänzt werden.
– **Selbsteinschätzung** – das Institut bewertet seinen Input selbst, z. B. durch Unterzeichnung seitens des CISO, des CRO oder sonstiger leitender Funktionen.	Kann zu einem minimalen Grad an Vertrauen führen, dass der Geschäftspartner ihre Compliance mit den CSCF-Kontrollen sorgfältig bewertet hat.

Zusätzliche Maßnahmen zur Behebung des Risikos

Über die allgemeinen in Abschnitt 4 hervorgehobenen Maßnahmen hinaus können die Überlegungen in Bezug auf eine Reihe nachstehend dargestellter zusätzlicher Optionen ausgeweitet werden, welche für die Nutzung von SWIFT spezifisch sind.

Die Anforderung der Compliance mit empfohlenen Kontrollen

Abgesehen von der bestehenden Verpflichtung zur Self-Attestation in Bezug auf die verpflichtenden Kontrollen können Institute fordern, dass einige Geschäftspartner auch Self-Attestations in Bezug auf einige oder alle empfehlenden Kontrollen ausstellen.

Einsatz von Maßnahmen zur Betrugsaufdeckung seitens des Geschäftspartners

SWIFT-Benutzer können fordern, dass einige Geschäftspartner Ressourcen zur Betrugsaufdeckung einsetzen, um Abweichungen oder Ausreißer zu erkennen, die keine normalen Verhaltensmuster darstellen. Dieser Einsatz wird zurzeit im CSCF (Version 2019) als empfohlene Kontrolle definiert.

Beispiel: Daily Validation Report (DVR) von SWIFT

Als Teil des CSP-Programms erweiterte SWIFT sein Compliance Portfolio für finanzielle Straftaten um ein Tool zur Transaktionsmusteraufdeckung. Es dient dazu, das mit dem Zahlungsbetrug verbundene Risiko abzuschwächen.

Der Daily Validation Report (DVR) erleichtert es den Instituten, Zahlungsvorgänge zu bestätigen, potenzielle Risiken hervorzuheben und schnell zu reagieren, wenn ein Betrugsfall auftritt.

Der DVR enthält Informationen über Zahlungsvorgänge des Vortages. Jeden Tag werden Transaktionswert und Gesamtmenge mit dem täglichen Durchschnittswert und der täglichen Durchschnittsmenge des Benutzers über die vorherigen 24 Monate verglichen, so dass jede wesentliche Veränderung der Vorgänge schnell erkannt und verstanden wird.

Zwei Hauptgebiete werden erfasst:

- Die Vorgangsberichterstattung ermöglicht Benutzern, ihre sämtlichen Vorgänge pro Tag anzuzeigen. Die tägliche Gesamtaktivität wird nach Nachrichtenart, Währung, Land und Geschäftspartner sortiert bereitgestellt. Gesamtwert und -menge pro Tag werden genauso bereitgestellt wie Angaben zu den größten Transaktionen.
- Die Risikoberichterstattung soll große und ungewöhnliche ist dafür bestimmt, große und ungewöhnliche Nachrichtenströme hervorzuheben, die ein Betrugsrisiko anzeigen können. Es hilft Benutzern dabei, die größten einzelnen Transaktionen und die größten kumulierten Transaktionsflüsse auszuwählen, die bei ihren Geschäftspartnern in Bezug auf eingehende und ausgehende Zahlungen erscheinen. Vergleiche mit vorherigen durchschnittlichen Tageswerten und -mengen ermöglichen den Benutzern, Vorgangsveränderungen zu bewerten. Die Risikoberichterstattung hebt auch neue Kombinationen mittelbarer und unmittelbarer Geschäftspartnern von Transaktionen während dieses Tages hervor.

Die Informationen werden hauptsächlich für folgende Nachrichtenarten von SWIFT aggregiert: MT 103, MT 202, MT 202COV, MT 205 und MT 205COV. Der DVR wurde im Jahre 2016 eingeführt.

Beispiel: SWIFT Payment Controls Service (PCS)

Der Payment Controls Service (PCS) konzentriert sich speziell darauf, SWIFT-Benutzern beim Erkennen von in laufender Echtzeit abweichenden Aktivitäten zu helfen. Der PCS ermöglicht die Echtzeiterkennung von Zahlungen während des Transaktionsvorgangs, die nicht den Grundsätzen eines Geschäftspartners entsprechen bzw. die uncharakteristisch sind und ein Betrugsrisiko anzeigen. Er erfolgt „Out-of band“, d. h. außerhalb der Räumlichkeiten des Benutzers. Dies bedeutet, dass sogar, wenn das Institut kompromittiert ist, die Daten vertrauenswürdig bleiben.

Der PCS arbeitet in einer von zwei möglichen Echtzeit-Betriebsmodi, die vom Abonnenten definierte Grundsatzregeln verwenden:

- Die Nachricht kopieren und warnen oder
- Die Nachricht halten und warnen

Im Kern ermöglicht der PCS den Benutzern, die Grundsatzregeln über eine Reihe von Parametern zu konfigurieren:

- Geschäftskalender, Nicht-Geschäftstage und normale Geschäftszeiten
- White List / Black List, einzelne und aggregierte Zahlungslimits pro Währung
- White List / Black List, einzelne und aggregierte Zahlungslimits pro Land
- Schwellenwerte für Land, Währung, einzelne Unternehmen oder Konzerne
- Neue Institute: Ermittlung von Zahlungen mit neuen Teilnehmern oder Ketten auf der Grundlage historischer Nachrichtenströme
- Verdächtige Konten: Überprüfen von Kontonummern von Endkunden gegenüber einer institutseigenen Black List von als mit hohem Risiko behaftet geltenden Kontonummern

Der PCS wurde im Oktober 2018 eingeführt.

Beachten Sie, dass ein Institut, bevor es Betrugskontrollen für Empfänger einführt oder einen Geschäftspartner darum ersucht, Betrugskontrollen für Absender einzuführen, die allgemeinen Geschäftsbedingungen sowie sonstige rechtliche Überlegungen überprüfen muss.

Weiterentwicklung der Beziehung und Durchsetzung derselben mit der Relationship Management Applikation (RMA)

Beziehungen, die mehrere Jahre zuvor begründet wurden, können sich im Laufe der Zeit verändern und nicht mehr mit dem heutigen Geschäftsverlauf übereinstimmen. Neben der Kontrolle darüber, wer mit der Relationship Management Applikation (RMA) Nachrichten versenden kann, können SWIFT-Benutzer die Nachrichtenarten durch die Nutzung von RMA Plus beschränken. Zum Beispiel kann ein Benutzer dem Erhalt von Finanz- oder Handelsnachrichten zustimmen, aber den Erhalt von Zahlungsnachrichten ablehnen.

Beispiel: SWIFT RMA und RAM Plus

Die Relationship Management Applikation (RMA) ist der hauptsächliche Austausch- und Genehmigungsprozess zwischen zwei Finanzinstituten und ermöglicht den Instituten zu bestimmen, welche Geschäftspartner ihnen FIN-Nachrichten senden können. Unerwünschter Verkehr wird auf Absenderebene blockiert, was die betrieblichen Risiken in Verbindung mit der Behandlung unerwünschter Nachrichten reduziert.

RMA Plus, die granularere Version der RMA, geht einen Schritt weiter, indem sie Institute bestimmen lässt, welche Nachrichtenarten sie an jeden ihrer Geschäftspartner senden oder von ihnen empfangen möchten. Zum Beispiel kann ein Institut von einem bestimmten Korrespondenten nur Kreditbriefe erhalten wollen.

Institute müssen ihren Geschäftspartnern RMA- oder RMA Plus-Genehmigungen erteilen, um Nachrichten des betreffenden Geschäftspartners zu erhalten, und die RMA-Funktionalität ist in die SWIFT Alliance Access- und SWIFT Alliance Entry-Schnittstelle eingebaut

Im Laufe der Zeit haben viele Institute viele RMA-Beziehungen mit vielen Geschäftspartnern eröffnet. Allerdings wurde die Liste der RMA Genehmigungen eventuell nicht aktualisiert, wenn die Geschäftsbeziehung sich ändert oder beendet wird. Die Institute können daher eine große Anzahl von inaktiven RMA haben und sich dessen möglicherweise nicht bewusst sein.

Durch Rationalisierung und Widerruf ruhender oder inaktiver RMAs, können Institute die Zeit und die Kosten sowie die Risiken reduzieren, die mit den betreffenden Aktivitäten verbunden sind.

Die Institute können diese Rationalisierung selbst durchführen. Alternativ bietet SWIFT die „Säuberung“ der RMA und RMA Plus-Genehmigungen als Dienstleistung an.

Die RMA wurde im Jahre 2009 eingeführt

Anhang B: Glossar

Begriff	Abkürzung	Beschreibung
SWIFT Customer Security Programme	CSP	**Klicken Sie hier, um weitere Informationen zu erhalten**
Customer Security Controls Framework	CSCF	**Klicken Sie hier, um weitere Informationen zu erhalten**
Customer Security Control Policy	CSCP	**Klicken Sie hier, um weitere Informationen zu erhalten**
Know Your Customer – Security Attestation (Anwendung)	KYC-SA	Grundschutz: **Klicken Sie hier, um weitere Informationen zu erhalten** Benutzerhandbuch: **Klicken Sie hier, um weitere Informationen zu erhalten**
Relationship Management Applikation	RMA	**Klicken Sie hier, um weitere Informationen zu erhalten**
Daily Validation Report	DVR	**Klicken Sie hier, um weitere Informationen zu erhalten**
Payment Controls Service	PCS	**Klicken Sie hier, um weitere Informationen zu erhalten**
Shared Infrastructure Programme	SIP	**Klicken Sie hier, um weitere Informationen zu erhalten**
Business Identifier Code	BIC	**Klicken Sie hier, um weitere Informationen zu erhalten**
Chief Information Security Officer	CISO	Allgemeine Bezeichnung für die für die Informationssicherheit in einem Unternehmen verantwortliche Führungskraft.

Informationen zu SWIFT

SWIFT ist eine globale, sich im Eigentum der Mitglieder befindliche Kooperative und der weltweit führende Anbieter sicherer Finanznachrichtenübermittlungsdienste. Wir bieten unserer Gemeinschaft eine Plattform für Nachrichtenübermittlung und Kommunikationsstandards, und wir bieten Produkte und Dienstleistungen zur Erleichterung von Zugriff und Integration, Identifizierung, Analyse und Compliance in Bezug auf Wirtschaftsverbrechen.

Unsere Nachrichtenplattform, Produkte und Dienstleistungen verbinden mehr als 11.000 Banken und Sicherheitsorganisationen, Markt-Infrastrukturen und Unternehmenskunden in mehr als 200 Ländern und Gebieten miteinander, so dass sie sicher kommunizieren und verlässlich standardisierte Finanznachrichten austauschen können.

Als ihr zuverlässiger Partner erleichtern wir globale und lokale finanzielle Datenströme und unterstützen Handel und Gewerbe weltweit; wir bemühen uns konsequent um operative Spitzenleistungen und suchen ständig nach Wegen, um Kosten zu verringern, Risiken abzuschwächen und betriebliche Schwachpunkte zu beseitigen.

Die internationale Führungsstruktur und Aufsicht des in Belgien ansässigen SWIFT verstärkt den neutralen, globalen Charakter seiner kooperativen Struktur. Das globale Niederlassungsnetz von SWIFT gewährleistet eine aktive Präsenz in allen wichtigen Finanzzentren.

Weitere Informationen erhalten Sie unter www.swift.com oder durch ein Gespräche mit Ihrem Account Manager oder über eine E-Mail an weareswift@swift.com.

57386 – Januar 2019