09 | 2018
Ausgabe 76

«Know your enemy»

Interview mit Marc Hofmann, CISO SWIFT, über die Bekämpfung von Cyberrisiken

Digitale Kronjuwelen des Finanzplatzes und Cyberabwehr

Nach der Harmonisierung ist vor der Harmonisierung

it
Schweizer Fachzeitschrift für den Zahlungsverkehr

IMPRESSUM

HERAUSGEBERIN
SIX INTERBANK CLEARING AG
Pfingstweidstrasse 110
CH-8005 Zürich
T +41 58 399 4747

BESTELLUNGEN/FEEDBACK
clearit@six-group.com

AUSGABE
Ausgabe 76 – September 2018
Erscheint regelmässig, auch online unter www.clearit.ch
Auflage Deutsch (1300 Exemplare) und Französisch (400 Exemplare) sowie Englisch (elektronisch auf www.clearit.ch)

FACHBEIRAT
Samuel Ackermann, PostFinance; Boris Brunner, SIX Interbank Clearing AG; Susanne Eis, SECB; André Gsponer (Leiter), ConUm AG; Daniela Hux-Brauss, Credit Suisse AG; Gabriel Juri, SIX Interbank Clearing AG; Jean-Jacques Maillard, BCV; Stefan Michel, SNB; Thomas Reske, SIX Interbank Clearing AG; Peter Ruoss, UBS Switzerland AG; Bettina Witzmann-Walter, Liechtensteinischer Bankenverband

REDAKTION
André Gsponer, ConUm AG; Gabriel Juri (Leiter), Karin Pache und Thomas Reske, SIX Interbank Clearing AG

ÜBERSETZUNG
Englisch: Word+Image AG
Französisch: Denis Fournier

GESTALTUNG
Felber, Kristofori Group, Werbeagentur

DRUCK
sprüngli druck ag

Weitere Informationen zu den Schweizer Zahlungsverkehrssystemen finden Sie unter www.six-interbank-clearing.com

TITELSEITE
Marc Hofmann, Chief Information Security Officer bei SWIFT

Marco Menotti

Liebe Leserinnen und Leser

Der Begriff «Ökosystem» aus der Biologie bezeichnet eine Lebensgemeinschaft von Pflanzen und Tieren in einem Lebensraum. Ein Baum mit seinen Pilzen und anderen Lebewesen bildet ein Ökosystem. Zusammen mit der umliegenden Wiese, die in sich wiederum ein Ökosystem ist, ergibt sich ein grösseres und mit dem ganzen Wald ein noch grösseres Ökosystem.

Ähnlich verhält es sich bei geschäftlichen Ökosystemen. Das Schweizer Mobile-Payment-Netzwerk rund um TWINT beispielsweise kann als Ökosystem für Zahlungen bezeichnet werden (siehe clearit 72, September 2017). Zieht man in Betracht, dass Instant Payments kontinuierlich an Bedeutung gewinnen, ist es naheliegend, diese mobile P2P-Lösung in Kontext mit dem Interbankenzahlungsverkehr zu setzen, wo Zahlungsauslösung und Zahlungsgutschrift seit Jahrzehnten in Echtzeit abgewickelt werden. So kann ein Ökosystem nahtlos in ein anderes übergehen – wie beim Baum und der umliegenden Wiese.

Unter meiner Führung ist SIX dabei, den Zahlungsverkehr entsprechend den heutigen und zukünftigen Bedürfnissen unserer Eigner, der Banken, als neues Ökosystem auf- und vor allem auszubauen. Entscheidend dabei ist, dass wir die heutigen Ökosysteme verstehen, zwischen den verschiedenen Ökosystemen interagieren können und das Potenzial von Synergien ausschöpfen – insbesondere mit Blick auf die technologische oder regulatorische Dynamik, die den Arbeitsalltag im Zahlungsverkehr der Banken immer stärker beeinflusst.

Neu schaffen und nutzen wir ein grosses Ökosystem für Produkte und Services, das u.a. TWINT, eBill, LSV, QR-Rechnung, ATMs, Karten und SIC/euroSIC umfasst. Dadurch sollen Kostenvorteile, Netzwerkeffekte und auch gezielte Innovationen von der SIX für die Banken entstehen. Die SIX Interbank Clearing AG wird in reduzierter Form – mit dem IT Management und Operations Center – weiterhin für den Betrieb der Schweizer RTGS-Plattform sorgen und sicherstellen, dass die Nationalbank ihren gestalterischen Einfluss auf das systemrelevante SIC direkt ausüben kann. Alle Nichtkernbereiche von SIC werden in die neue funktionale Organisation der Business Unit eingegliedert, stellen jedoch der SIX Interbank Clearing die bisherigen Dienstleistungen weiterhin zur Verfügung. Zur neuen Business Unit stossen das Issuing, das Processing und der ATM-Betrieb von SIX Payment Services. Dazu gehören Erweiterungen der heutigen Geschäftsfelder, z.B. durch neue Angebote für eine integrierte Bargeldversorgung («Ökosystem Cash»).

Und last but not least wird auch das «Swiss Corporate API» (siehe clearit 75, Juni 2018) bei uns angesiedelt und als «Ökosystem Connectivity» alle anderen erwähnten Ökosysteme positiv beeinflussen und neue Geschäftsfelder eröffnen, die über den Zahlungsverkehr hinausgehen, Raum für innovative Services schaffen und unser Geschäftsmodell ausweiten und abrunden sollen. Baum, Wiese und Wald für sich allein genügen unserem strategischen Anspruch nicht. Wir fokussieren auf die Vergrösserung der Ökosysteme. In diesem Sinn lautet unser Anspruch bei der Neuaufstellung: «Today we are payments – tomorrow we are Banking Services» – ab 1. Oktober 2018 in der SIX Business Unit Banking Services.

Marco Menotti
Head Business Unit Banking Services, SIX

Marc Hofmann,
Chief Information Security Officer bei SWIFT

Cyber-sicherheit – ein Wettlauf um die Zeit

«Know your enemy.» Erkennungs- und Abwehrstrategien entwickeln, Bedrohungsanalysen erstellen, das Bewusstsein für Cyberrisiken schärfen und den Erfahrungsaustausch innerhalb der Community fördern. Dies sind einige der Aspekte, die Marc Hofmann, Chief Information Security Officer bei SWIFT, im Interview ausführt.

«Praktisch jeder ist Cyberrisiken in irgendeiner Form ausgesetzt», stellten IWF-Experten letztes Jahr in einem Papier fest. Das klingt so banal wie die Mahnung der Polizei vor Unfallgefahren. Wie wirkt diese Botschaft auf Sie, Herr Hofmann?
Ich glaube nicht, dass sich die Unfallgefahren im Strassenverkehr in den letzten Jahrzehnten so stark entwickelt haben wie die Cyberrisiken. Die kriminellen Hacker sind heute wesentlich besser organisiert als noch vor wenigen Jahren und verfügen über vielfältige Ressourcen. Sie agieren wie ein global tätiges Unternehmen. Das hat die Gefahrenlage massiv verändert. Ein anderer Aspekt ist, dass die Angriffsfläche breiter geworden ist: die Digitalisierung, die Öffnung unserer Netzwerke zum Internet – das gilt insbesondere für die Kunde-Bank-Schnittstelle. Nehmen wir Open Banking als Schlagwort oder Internet of Things oder die Regulierung mit PSD2, die mithilfe von APIs die Kundenschnittstelle für Drittanbieter öffnet.

> «Die SWIFT Community hat ein stetig steigendes gemeinschaftliches Interesse an ihrer Sicherheit.»

SWIFT hat vor zwei Jahren als Reaktion auf den Cyberbankraub bei der Zentralbank von Bangladesch eine Reihe von Sicherheitsmassnahmen angekündigt und unter dem Namen «Customer Security Programme (CSP)» eingeführt – in clearit 12/2017 erschien dazu ein Beitrag. Bis Ende letzten Jahres sollten alle SWIFT-Kunden nachweisen, dass sie die obligatorischen Sicherheitskontrollen einhalten. 89% haben dies offenbar getan. Was passiert mit denjenigen, die nicht mitgemacht haben?
Ich bin erfreut, dass mittlerweile über 90% unserer 12'000 Kunden ihre Selbstattestierung abgeschlossen haben. Und diese Zahl wächst, während wir hier sprechen. Das ist eine gute Nachricht. Bei näherer Betrachtung der Zahlen stellen wir zudem fest, dass diese Zahl über 99% aller SWIFT-FIN-Meldungen abdeckt. Bis Ende 2018 streben wir 100% an und werden den verbliebenen Kunden helfen, die CSP-Attestierung durchzuführen. Und da rennen wir grundsätzlich offene Türen ein, denn die SWIFT Community hat ein stetig steigendes gemeinschaftliches Interesse an ihrer Sicherheit. Gemeinsam mit unseren Stakeholdern tun wir alles, um dieses Ziel zu erreichen. Dazu zählt auch, dass wir diejenigen, die die Anforderungen nicht einhalten, an die zuständigen Aufsichtsbehörden melden.

Apropos Community: In einer solchen würde man erwarten, dass ein reger Austausch von Informationen und Erfahrungen zwischen den einzelnen Mitgliedern stattfindet. Das scheint nach unseren

Informationen nicht immer der Fall zu sein. Zumindest gibt es nur wenige Banken, die am Status des «Security attestation» der Gegenparteien interessiert wären. Woran liegt das?
Das deckt sich nicht mit meiner persönlichen Beobachtung. Ich sehe tatsächlich das Gegenteil: ein viel stärkeres und gewachsenes Interesse an der Sicherheit von Gegenparteien. Und das gilt nicht nur für Gegenparteien, das gilt für alle Beziehungen mit Drittparteien – im Gegensatz zu früher, als man sich primär auf die eigene Sicherheit beschränkte. Ich habe in vielen Banken beobachtet, dass dort Vorgaben und Prozesse eingerichtet wurden, um die Sicherheit bei den Partnern zu gewährleisten. Und auch die Anfragen nach Attestierungsinformationen wachsen weltweit. Da wir ja in einem Lernprozess sind, haben wir selbstverständlich noch Luft nach oben.

> «So lange die Angreifer die Hoffnung haben, sie könnten damit Geld verdienen, werden sie ihre Aktivitäten nicht stoppen.»

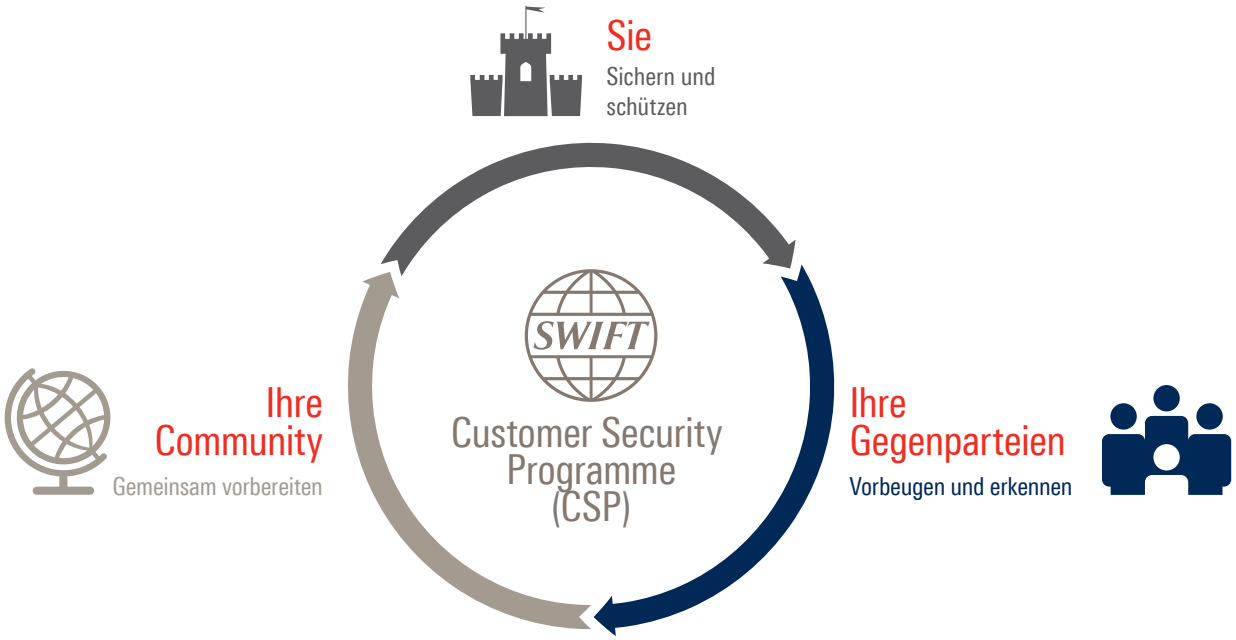
Wie viele Betrugsfälle über welchen Gesamtbetrag konnten aufgrund der CSP-Aktivitäten verhindert werden?
Wir haben tatsächlich greifbaren und messbaren Fortschritt gemacht in der Bekämpfung von Betrugsfällen. Ich kann dabei nicht mit Zahlen oder gar Einzelfällen dienen. Wir haben aber zahlreiche Fälle beobachtet, wo der Zahlungsbetrug mit unseren Massnahmen verhindert werden konnte. Ein weiterer wichtiger Aspekt ist, dass unsere Kunden ein deutlich höheres Bewusstsein zeigen für die eigene Sicherheit und – wie ich vorhin angedeutet habe – auch die der Gegenparteien, die ihre Fähigkeit, Bedrohungen zu erkennen, ebenfalls erhöhen. Also wir werden besser. Meine Beobachtung ist jedoch, dass die Anzahl der Betrugsversuche nicht wirklich zurückgeht. Das Gegenteil ist der Fall. So lange die Angreifer die Hoffnung haben, sie könnten damit Geld verdienen, werden sie ihre Aktivitäten nicht stoppen.

Gibt es Hinweise, dass die Hacker ihre kriminellen Aktivitäten aufgrund des CSP in der Zwischenzeit auf andere Kanäle und Gebiete verlagert haben?
Wir wissen, dass die kriminellen Hacker immer mehr Aufwand betreiben, um die Sicherheitsmassnahmen zu umgehen. Also egal, was die Finanzinstitute eingeführt haben, Kriminelle versuchen, einen Weg drum herum zu finden. Mit der so genannten Deception Technology simulieren wir u.a. falsche Server und Konten, um sie in die Falle zu locken. Darauf reagieren sie mittlerweile, und das wird mit anderen Massnahmen ebenso passieren. Das CSP ist da keine Ausnahme. Was heisst das für uns? Das heisst, wir dürfen uns nicht ausruhen, sondern müssen fortwährend hinterfragen, ob unsere Massnahmen angemessen sind, und müssen logischerweise immer eine Schippe drauflegen. Viele Betrugsversuche stellen wir sehr früh mit unserem Integritätscheck-Tool fest, das aufzeigt, wenn eine Meldung verfälscht übermittelt wird.

Apropos Tool: Mit dem neuen Service «Payment Controls» hat SWIFT ein neues Tool zum Schutz vor Betrug eingeführt – das Echtzeit-Screening ausgehender Zahlungen. Warum nicht auch für eingehende Zahlungsaufträge?
Zunächst einmal ist es die Pflicht eines jeden Unternehmens, die ausgehenden Meldungen dahingehend zu überprüfen, ob sie nicht betrügerisch sind. Und das ist der Grund, warum wir an diesem Ende angefangen haben. Die zukünftige Erweiterung auf die Empfängerseite ist damit nicht ausgeschlossen.

Das ist dann im Wettrennen mit den Kriminellen eine der nächsten Etappen …
Möglicherweise ja. Die Sache ist nur, Sie müssen am Ende die ganze Community mitnehmen können. Die wenigsten Dinge funktionieren ja so, dass ich einen Schalter umlege, und dann haben wir einen Effekt für die ganze Community. Sondern bei den meisten Dingen ist es eine gemeinsame Anstrengung. Und damit gilt: Wir müssen uns zusammen mit unseren Kunden überlegen, wo unsere Prioritäten sind und wo wir den besten Effekt erzielen mit Blick auf die aktuelle, aber auch auf die antizipierte Gefährdungslage.

Cyberbedrohung ist die Kehrseite der Digitalisierung. Politik, Wirtschaft und Gesellschaft scheinen den Ernst der Sache erkannt zu haben. Um nur einige Beispiele zu nennen: EU-Staaten schaffen gemeinsam schnelle Cybereingreiftruppen, der Schweizer Bundesrat bekommt einen oder eine «Mr./Mrs. Cyber Security», und in Deutschland soll das weltgrösste Forschungszentrum für IT-Sicherheit entstehen (Cispa) mit einem Masterstudiengang in Cybersicherheit. Wie vernetzt sich SWIFT



im Wettrennen um die Schaffung von Sicherheit mit den weltweiten Initiativen?
Zunächst mal halte ich das für ein extrem wichtiges Thema, um die Zusammenarbeit im Kampf gegen die Kriminalität zu fördern – und da sind nicht nur Banken oder unsere Kunden gemeint, sondern auch Strafverfolgungsbehörden. Ich glaube, dass die Zusammenarbeit oder zumindest der Informationsaustausch über den Modus Operandi der Cyberkriminellen mit staatlichen Stellen, aber auch mit Universitäten, eine der kritischen Fähigkeiten sein wird, um uns effektiv verteidigen zu können. Deshalb haben wir in dieser Hinsicht bereits zahlreiche Schritte unternommen und planen weitere. Zum Beispiel arbeiten wir mit Organisationen wie dem Internationalen Währungsfonds oder der Weltbank zusammen. Wir sind beispielsweise in der FS-ISAC, einer Organisation der Finanzbranche, die ihre 7000 Mitglieder weltweit mit Informationen über Cybergefahren versorgt. Kürzlich fand der jährliche Gipfel in Miami statt, wo die Chief Information Security Officers der Banken sich berieten und Tacheles redeten.

Diese Zusammenarbeit ist wohl wichtig, ist sie aber auch strategisch?
Definitiv. Aus verschiedenen Gründen. Der nächstliegende Grund ist die nachrichtendienstliche Zusammenarbeit. So teilen wir mit der SWIFT Community zeitnah die so genannten «Indicators of Compromise», also Daten über Bedrohungen wie Schadprogramme oder Tätergruppen, damit sie ihre Verteidigung auch kurzfristig anpassen kann. Diese speisen sich aus Erfahrungen, die andere gesammelt haben. Ich halte es für äusserst wichtig, dass wir solche Informationen austauschen und uns gegenseitig vor potenziellen Gefährdungslagen warnen. Und tatsächlich konnten wir uns gegen einige Attacken – wir haben vorhin über «Wo waren wir effektiv gegen Cyberbetrug?» gesprochen – erfolgreich verteidigen.

Ein weiterer strategischer Aspekt ist, dass wir das Bewusstsein in der gesamten SWIFT Community in diesem Kontext schärfen wollen. Wir geben Beispiele, wie Vorgehensweisen bei Attacken funktionieren und wie kriminelle Angreifer das machen; dass diese teilweise sehr, sehr geduldig sind, dass sie nach dem Eindringen in das Netzwerk eines Unternehmens über Monate oder über ein Jahr lang unbemerkt die Umgebung und Benutzeraktivitäten ausspähen, bevor sie zuschlagen. Wir haben Erkenntnisse darüber, dass die Kriminellen ganz geschickt an Feiertagen oder Wochenenden zuschlagen, um das Verhalten lokaler Betreiber auszunutzen. Diese Informationen müssen wir teilen und das Risikobewusstsein für konkrete Situationen erhöhen, damit Unternehmen dann auch gezielt dort investieren, wo es am meisten Sinn macht. Wir sollten nicht mit der Giesskanne herumlaufen und vergeblich versuchen, alles gleichmässig zu schützen, sondern dort, wo der beste Effekt erzielt werden kann. Wirklich effektiv ist das nur mit Hilfe der Gemeinschaft möglich.

Der Masterplan von SWIFT für die Cybersicherheit ist nach vier Hauptkriterien strukturiert. Im ersten Punkt heisst es: Know your enemy. Wir kennen zwar das Know-your-customer-Prinzip. Aber wie und woran erkennt man einen Feind?
Sehr wichtig ist erst einmal die Erstellung von Bedrohungsanalysen. Der zweite Aspekt ist die Fähigkeit des jeweiligen Security Operations Center (SOC), Eindringlinge zu erkennen. Und das ist ein schwieriges Thema, denn die Hacker wollen ja unerkannt bleiben. Es gibt aber technische Unterstützung, z.B. im Bereich Network Behavior Analysis. Damit lässt sich ungewöhnliches Verhalten im Netzwerk aufspüren, um ihnen auf die Spur zu kommen. Diese Art Verhaltensanalyse ist wie die zuvor erwähnte Deception Technology eine weitere Möglichkeit, Awareness zu schaffen auf der technischen Seite, was die Infrastruktur anbelangt. Und dann gibt es selbstverständlich die Businessseite. Hier geht es darum, wie ich z.B. einen Zahlungsbetrug entdecken kann. Wir haben vorher kurz unseren neuen Service «Payment Controls» gestreift. Unser «Daily Validation Report» ist eine weitere Möglichkeit, die Prozesse rund um die tägliche Abstimmung von Transaktionen gegen Betrug abzusichern. Wenn ich eine Meldung habe, die zu einer ungewöhnlichen Uhrzeit eintrifft oder zu einem neuen, mir unbekannten Zahlungsempfänger weitergeleitet werden soll, muss klar sein, dass da etwas nicht in Ordnung sein kann. Und das ist just mit «Know your enemy» gemeint.

Diesen Sommer soll eine neue Version des CSP Framework publiziert werden mit Änderungen vieler Sicherheitskontrollen. Weshalb muss das Rahmenwerk angepasst werden? Hat die jetzt gültige Version wesentliche Aspekte ausser Acht gelassen?
Nein, das ist nicht der Fall. Aber egal wie ausgeklügelt wir uns gegen Cyberattacken verteidigen – die Kriminellen geben keine Ruhe und werden immer raffinierter. Das heisst, auch wir müssen uns weiter entwickeln. Das gilt ebenso für das CSP. Wir müssen die Kontrollen fortwährend hinterfragen und weiterentwickeln, wenn wir das Rennen nicht verlieren wollen. Da sich die Risiken samt der Gefährdungslage stetig verändern, müssen wir das CSP entsprechend anpassen. In diesem Sinn wird es in Zukunft mit Sicherheit neue obligatorische Sicherheitskontrollen geben – vielleicht fallen irgendwann auch einige weg. Auf jeden Fall erwarte ich, dass das Framework insgesamt noch mehr an Schärfe gewinnt.

Kann man daraus folgern, dass das Framework quasi einem Release-Zyklus unterworfen wird?
So ist es. Wir hinterfragen die Kontrollen fortwährend. In Absprache mit der Community werden wir einen solchen Zyklus einführen.

Bei der Zentralbank von Bangladesch haben die Hacker die betrügerischen Zahlungen zwischen dem Backoffice-System und SWIFT Alliance Access eingespeist. Die wirksamste Kontrolle gegen einen solchen Angriff ist «Back-office Data Flow Security». Wieso wird dieser Kontrollpunkt auch im neuen Framework weiterhin nur empfohlen und ist nicht obligatorisch?
Wir halten das für ein wichtiges Thema. Deshalb ist es auch Teil des Control Framework. Wir sind uns sicher, dass es bei der Weiterentwicklung des Framework Verschiebungen von «Advisory Controls» zu «Mandatory Controls» geben wird. Wir überprüfen regelmässig die Bedeutung und Angemessenheit der jeweiligen Kontrollen und erwägen dann ein Upgrade zum Mandatory Control.

Und in einem nächsten Release wird das eingespielt …
So ist es.

Seit zwanzig Jahren steht SWIFT aufgrund ihrer systemischen Bedeutung für die Stabilität des weltweiten Finanzsystems unter der Aufsicht der G-10-Zentralbanken. Wie legt SWIFT ihrerseits Rechenschaft über ihre eigenen Bemühungen um Cybersicherheit ab?
Natürlich ist das Thema Cybersicherheit nicht nur für die Community, sondern insbesondere für unsere eigene Statussicherheit äusserst wichtig. Das heisst, wir geben dem Thema höchste Aufmerksamkeit bei uns im Haus. Gleichzeitig haben wir in der Vergangenheit – und tun es weiterhin – substanziell in unsere Infrastruktur und in unsere Cyberstrategie investiert. Wir beziehen uns laufend auf internationale Standards (z.B. ISO) sowie Best Practices und eruieren, wo wir noch eine Extrameile gehen können. Über all das, was wir hier tun, halten wir die G-10 regelmässig auf dem Laufenden, um ihnen ihre Governance-Aufgaben zu ermöglichen.

«Wir haben Erkenntnisse darüber, dass die Kriminellen ganz geschickt an Feiertagen oder Wochenenden zuschlagen.»

Marc Hofmann

> **«Wenn ich mir etwas wünschen dürfte, wäre es, dass sich ausnahmslos alle Unternehmen sofort an uns wenden, wenn ein Verdacht auf Missbrauch aufkommt, so dass wir helfen können.»**

Welches sind Ihrer Meinung nach aktuell die grössten Hindernisse für die Gewährleistung von Cybersicherheit in der SWIFT Community?
Tatsächlich ist es so, dass zwar nicht die Mehrheit, aber doch viele unserer Kunden den Austausch von Informationen noch scheuen. Einige betrachten es als Wettbewerbsvorteil, diese für sich zu behalten. Das gilt insbesondere für Informationen über Störfälle. Wenn ich mir etwas wünschen dürfte, wäre es, dass sich ausnahmslos alle Unternehmen sofort an uns wenden, wenn ein Verdacht auf Missbrauch aufkommt, so dass wir helfen können. Oder dass wir Informationen – natürlich erst nach ihrer Freigabe – anonymisiert über unseren Kanal teilen können, um Schaden bei anderen Unternehmen abzuwenden. Nach meiner Erfahrung sind leider viele Unternehmen gar nicht in der Lage, bei einem Verdachtsfall mit uns zu agieren. Erstens weil sie schlicht und einfach nicht wissen, an wen sie sich in Sachen Legal & Compliance intern wenden müssen, um eine Freigabe für den Informationsaustauch zu bekommen. Auch wenn dieses Wissen vorhanden ist, braucht es für die Freigabe manchmal zu lange, womöglich Tage, sei es weil die Verantwortlichen im Urlaub oder zumindest nicht abrufbereit sind.

Der zweite Punkt ist, dass Unternehmen das unter Umständen technisch gar nicht mehr können. Ich habe bei einigen Attacken beobachten können, dass Kriminelle sehr viel an der Infrastruktur des Unternehmens (z.B. Server, inklusive Mail-Server) zerstört hatten, um ihre Spuren zu verwischen. Entweder löschen sie Einträge aus Datenbanken oder sie gehen extrem zerstörerisch vor und verschlüsseln oder löschen einfach alles, was ihnen in den Weg kommt. Mit anderen Worten, die Kunden konnten technisch gar nicht schnell reagieren. Die kriminellen Angreifer wollen im Prinzip die Abstimmung der Zahlungsein- und -ausgänge verhindern oder zumindest verzögern. Am Ende ist es ein Wettlauf um die Zeit. Es gibt nichts Wichtigeres als Zeit, um die Rückforderung von Mitteln voranzutreiben. Das wissen die Hacker auch, und deshalb wollen sie ihre Spuren verwischen und die Reaktion der Geschädigten verlangsamen.

Interview:
Gabriel Juri & Karin Pache
SIX Interbank Clearing

SWIFT CSP SECURITY CONTROLS FRAMEWORK

Eigene Umgebung sichern	1	Internetzugang einschränken
	2	Kritische Systeme von der allgemeinen IT-Umgebung sichern
	3	Angriffsfläche und Schwachstellen verringern
	4	Umgebung physisch sichern
Zugriff kennen und einschränken	5	Manipulation von Zugangsdaten verhindern
	6	Identitäten getrennt von Rechten verwalten
Erkennen und reagieren	7	Ungewöhnliche Aktivitäten in System- oder Transaktionsprotokollen erkennen
	8	Reaktionsfähigkeit und Informationsaustausch planen

Die Zukunft von Payment Security

Sicherheit im Zahlungsverkehr beschäftigt die Menschen spätestens seit der Einführung der Münzen als Zahlungsmittel. Im Zeitalter der fortschreitenden Digitalisierung nehmen die Bedrohungen und die Sicherheitsanforderungen exponentiell zu. Neue Strategien, Tools und Sicherheitsmerkmale sind unabdingbar im Kampf gegen die Cyberkriminalität.

Ein eigentlicher «Wettlauf» zwischen den «Guten» und den «Bösen» prägt die Geschichte des Geldes seit annähernd 3000 Jahren: offizielles versus gefälschtes Geld. Und als Folge davon eine ständige Verbesserung der Sicherheitsmerkmale. Bei Hartgeld sind das zum Beispiel Material, Farbe, Rändelung oder Abmessungen. Bei Banknoten sind es oft Stichtiefdruck, Sicherheitsfaden (Silberfaden), Wasserzeichen, Hologramm, Mikroschrift, UV-Licht- und Infrarot-Fluoreszenz. Obwohl die Sicherheitsmerkmale immer ausgeklügelter werden, ist auf Dauer doch keines so sicher, als dass ein Fälscher es nicht imitieren oder austricksen könnte.

Ähnliches lässt sich für die Geschichte des Internets sagen: Cybersicherheit versus Cyberkriminalität. Bereits die ersten digitalen Computerverbindungen wurden mit technischen Massnahmen geschützt und mit Sicherheitsmerkmalen versehen. Trotzdem gelangen die Angriffe von Hackern. Neue Sicherheitsmerkmale mussten entwickelt werden. Doch auch fürs Internet gilt: Die Gegenseite schläft nicht. – Der Wettlauf geht nicht nur weiter, er hat sich seit den Anfängen stark beschleunigt.

In der heutigen Zeit der zunehmenden und durchgehenden Digitalisierung wächst das Ausmass der Bedrohung durch Cyberkriminalität. Jedes Unternehmen, jede Privatperson kann das Ziel von Cyberkriminellen sein. Die Bedrohung besteht in Informationsdiebstahl, Betrug und Sabotage des Geschäftsbetriebs. Sie erfolgt über verschiedene Kanäle wie Social Media, E-Mail, Intranet, Internet, Telefon und Brief. Und sie geht von ganz unterschiedlichen Gruppen und Individuen aus, von Insidern und Cyberkriminellen, Hackern, organisierten Verbrechersyndikaten, Hacktivisten und staatlich unterstützten Angreifern.

IT-Sicherheit – technische und organisatorische Massnahmen kombinieren

Mit technischen Massnahmen lassen sich die Gefahren einer Infektion durch Schadsoftware mindern und die IT-Sicherheit im Unternehmensnetzwerk steigern. Zu diesen Massnahmen gehören unter anderem aktueller Virenschutz, tägliches Backup aller Daten, Spamfilter, Firewall und Verschlüsselung wichtiger Daten.

Das schwächste Glied in der Kette ist in vielen Fällen nicht die Technik, sondern der Nutzer. Somit braucht es neben technischen auch organisatorische Massnahmen, um die IT-Sicherheit zu erhöhen. Die organisatorischen Massnahmen sollen sicherstellen, dass die Verantwortlichkeiten bezüglich IT-Sicherheit im Unternehmen definiert sind. Ausserdem müssen die Mitarbeitenden geschult, die Risiken regelmässig überprüft und eine Passwort-Policy definiert werden, um die Sicherheit zu gewährleisten.

Neue Sicherheitsmerkmale

Im Wettlauf gegen die Cyberkriminellen gibt es zahlreiche neue Sicherheitsmerkmale, die den technologischen Vorsprung absichern und die IT-Sicherheit in Zukunft zusätzlich erhöhen sollen. Dazu nachfolgend einige Beispiele.

– Die **Zwei-Faktor-Authentifizierung (2FA)** nutzt die Kombination von zwei unterschiedlichen und voneinander unabhängigen Faktoren zur Identifizierung eines Benutzers. 2FA gilt als sehr sicher, hat aber den Nachteil, dass das jeweilige Token (Hardware-Token, Bankkarte oder Schlüssel) jederzeit mitgeführt werden muss. Als Verbesserung und Alternative wurde die **tokenlose 2FA** entwickelt. Diese neue Zwei-Faktor-Authentifizierung nutzt Smartphones als Token. Will

Mit Anomalieerkennung das Unübliche jagen.

sich der Anwender authentifizieren, verwendet er seinen persönlichen Zugang zum Smartphone und ein einmalig gültiges, dynamisches, zusätzliches One-Time-Passwort (OTP), das er über eine entsprechende App auf sein Smartphone bekommt. Der Vorteil bei dieser Methode: Ein zusätzliches Token wird entbehrlich, da das Smartphone ohnehin ständiger Begleiter ist. Nach diesem Prinzip funktionieren zum Beispiel der Google Authenticator und die UBS Access App.

– Die **verteilte elektronische Unterschrift (VEU)** wird in Zukunft unverzichtbar. Bei dieser Art von Unterschrift werden Zahlungsaufträge von der Finanzbuchhaltung oder der Treasury-Abteilung elektronisch an die Bank übertragen, aber noch nicht verbucht. Die Unterschriftsberechtigten können überprüfen, ob die zur Freigabe vorliegenden Zahlungsaufträge korrekt sind und welche Unterschriften bereits geleistet wurden bzw. noch fehlen. Der Berechtigte kann die zu signierenden Aufträge nun elektronisch unterschreiben. Erst wenn alle erforderlichen Unterschriften vorliegen, führt die Bank die Aufträge aus. Wenn die Zahlungsaufträge ausserdem über einen von den Unterschriften getrennten Kanal übermittelt werden, kann die Sicherheit nochmals erhöht werden. Zum Beispiel könnte der Zahlungsauftrag via EBICS an die Bank übertragen werden und die Unterschriften für die Freigabe könnten via E-Banking erfolgen. Ein Cyberkrimineller müsste dann, um erfolgreich zu sein, gleichzeitig zwei in sich sehr sichere Kanäle überlisten.

– **SwissID – die digitale Identität.** Heute weist eine Person ihre Identität mit einem Reisepass, einer Identitätskarte oder einem Führerausweis nach. Bei Transaktionen über das Internet ist dieser Nachweis allerdings sehr umständlich. Daher braucht es einen elektronischen Identitätsnachweis, der es zum Beispiel Online-Portalen erlaubt, eine Person eindeutig zu identifizieren und zu authentifizieren. SwissID ist in der Schweiz eine effiziente und breit abgestützte Lösung für eine digitale Identität. Die

MELANI

Die Webseite der Melde- und Analysestelle Informationssicherung MELANI (www.melani.admin.ch), die von der Schweizerischen Eidgenossenschaft betrieben wird, richtet sich an private Computer- und Internetbenutzer sowie an kleinere und mittlere Unternehmen (KMU) der Schweiz. Sie enthält Informationen zu aktuellen Bedrohungen und häufigen Fällen sowie Dokumentationen, Newsletter und z.B. auch ein Meldeformular.

kostenlose Dienstleistung wird von SwissSign erbracht, einem Joint Venture aus staatsnahen Betrieben, Finanzunternehmen, Versicherungsgesellschaften und Krankenkassen. Mit SwissID loggen Nutzer sich in Schweizer Onlinedienste einfach und sicher ein, weisen sich aus, kaufen Produkte, machen Zahlungen und unterschreiben online.

– Ein **Anomaly Detection System (ADS)** hilft, problematische, anomale Daten zu erkennen und dadurch zum Beispiel unübliche Käufe oder unübliche Begünstigte als potenziell betrügerische Transaktionen zu identifizieren. Die bankseitige automatisierte Anomalieerkennung bei Zahlungsaufträgen ist eine komplexe Aufgabe, die Bereiche wie maschinelles Lernen, Statistik und Data-Mining mit einbezieht.

Mehr Sicherheit durch persönliche Einstellungen für Zahlungen und Karten
Mit der Anpassung der persönlichen Einstellungen für Zahlungen und Karten erhöht sich die Sicherheit von Zahlungsaufträgen zusätzlich. Kunden sollen selber einstellen können, wenn sie bei Kontobewegungen über den von ihnen festgesetzten Betrag per Smartphone benachrichtigt werden wollen. Auch wird es in E-Banking-Systemen vermehrt möglich sein, Zahlungen und Karten für Länder, an die nie Geld überwiesen wird, zu sperren (Geo-Blocking). Zusätzlich werden Kunden periodenbezogene Limiten für Zahlungen einrichten können. Wird das Limit überschritten, lassen sich in der definierten Periode keine Zahlungen mehr erfassen. Bei mehreren Konten wird es möglich sein, einzelne Konten für Online-Zahlungen gänzlich zu deaktivieren. Diese Konten sind dann für Überweisungen und Kontoüberträge gesperrt. Ein weiteres, in Zukunft weit verbreitetes Feature wird sein, dass Zahlungen an neue Begünstigte zuerst bestätigt werden müssen; das heisst, ein Empfänger, an den bisher noch nie Geld überwiesen wurde, muss zur Sicherheit zusätzlich einmalig bestätigt werden. Banken werden ihren Kunden gewisse dieser Möglichkeiten in Kombination anbieten. So wird es einem Kunden zum Beispiel möglich sein zu definieren, dass eine Bestätigung für neue Begünstigte nur ab einem gewissen Betrag notwendig ist.

eBill – Rechnungen sicher bezahlen
Mit eBill können Rechnungssteller ihre Rechnungen direkt aus der Fakturierungssoftware elektronisch übermitteln und sicher und medienbruchfrei als eBill-Rechnung an das E-Banking ihrer Kunden schicken. Zahler müssen keine Zahlungsinformationen mehr abtippen, keine Einzahlungsscheine mehr scannen. Dadurch gibt es auch keine Eingabefehler mehr, stattdessen ein konsequent zuverlässiges, sicheres und transparentes Zahlen von Rechnungen. Rechnungssteller vermeiden dadurch Reputationsschäden, die mit E-Mail-Rechnungen aufgrund von Spam und Phishing leider nicht unüblich sind. Da eBill frei von Medienbrüchen und dadurch der E-Mail-Rechnung überlegen ist, wird sie sich wohl langfristig als die digitale, sichere Rechnung der Schweiz durchsetzen.

Peter Ruoss
UBS Switzerland AG

AUF DEM WEG ZUR E-ID

Am 1. Juni 2018 hat der Bundesrat den Gesetzentwurf zum elektronischen Identitätsnachweis (E-ID) verabschiedet. Die Nutzer einer solchen E-ID sollen bei Online-Dienstleistungen von Unternehmen und Behörden (z.B. Online-Shopping, elektronisches Patientendossier, Bestellung eines Strafregisterauszugs, Anmeldung auf der Gemeinde, Ausfüllen der Steuererklärung etc.) belegen können, dass sie eine bestimmte Person sind – und das mit einem einzigen Login.

Die SwissSign Group AG, ein Gemeinschaftswerk aus staatsnahen Betrieben (SBB, Schweizerische Post, Swisscom), Finanzunternehmen (SIX, UBS, Raiffeisen, Credit Suisse, Zürcher Kantonalbank, Entris), Versicherungsgesellschaften (Axa, Baloise, Helvetia, Mobiliar, Swiss Life, Vaudoise, Zürich) und Krankenkassen (CSS, SWICA) steht in den Startlöchern. Sie bietet mit SwissID eine kostenlose und einfache Möglichkeit zur digitalen Identifizierung an, die alle datenschutzrechtlichen Vorgaben erfüllt und die Privatsphäre ihrer Kundinnen und Kunden schützt.

Digitale Kronjuwelen des Finanzplatzes und Cyberabwehr

Die Swiss Value Chain bildet das Rückgrat des Schweizer Finanzplatzes. Die reibungslose und effiziente Funktionsweise ihrer vernetzten Infrastrukturen – Börsenhandel, Wertschriften- und Zahlungsverkehrsabwicklung – ist eine genauso zentrale Voraussetzung für die Attraktivität des Finanzplatzes wie ihre Widerstandsfähigkeit auch gegen Cyberangriffe. Denn die Frage ist nicht ob, sondern wann solche Cyberangriffe passieren werden.

Die Anschlussfrage lautet, ob SIX, die Betreiberin der vollständig standardisierten, automatisierten und digitalisierten Finanzmarktinfrastruktur, gegen Cyberattacken gewappnet ist. Dabei sind technische Massnahmen allein – im Rahmen des «Business Continuity Planning (BCP)» – nicht ausreichend.

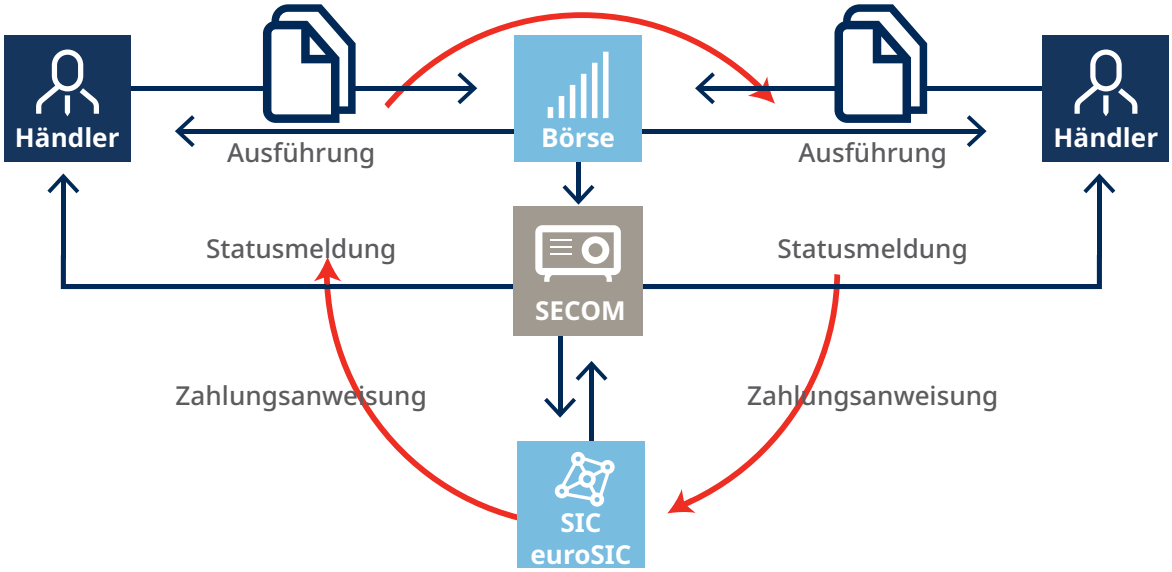
Proaktive Verteidigungslinie

SIX ist der kontinuierlichen Optimierung vorhandener Sicherheitsprozesse (z.B. BCP, internes Kontrollsystem) verpflichtet. Darüber hinaus identifiziert und evaluiert sie neue technologische Risiken und trifft im Einklang mit Best Practices und den weltweiten Sicherheitsstandards in der Finanzbranche alle notwendigen Vorkehrungen, um sich und ihre Kunden in einem sich ständig verändernden Umfeld zu schützen. Dass sich das organisierte Verbrechen in die Onlinewelt verlagert und durch immer raffiniertere Cyberangriffe auf Unternehmen immense Schäden anrichtet, ist zwar in aller Munde, aber das Bewusstsein für die Bedrohung ist noch nicht wirklich flächendeckend entwickelt. Dazu braucht es eine gelebte Risikokultur, die sich nicht von selbst einstellt. SIX fördert diese Kultur seit einiger Zeit proaktiv im Unternehmen. Dabei ist ein angemessenes Risikobewusstsein jedes Einzelnen unerlässlich, wenn man sich vor Augen führt, dass bereits ein verdächtiges E-Mail zu einer relevanten Bedrohung werden kann.

Das erste kognitive Security Operations Center der Schweiz

SIX hat sich deshalb organisatorisch aufgerüstet: Im Januar 2018 ging das erste Security Operations Center

SOC-Prozesse



Swiss Value Chain

(SOC) der Schweiz in Betrieb, das auf Cognitive Computing – also eine selbstlernende Technologie – setzt. Die Security-Analysten arbeiten vor Ort zusammen mit dem Operation Monitoring im Schichtbetrieb rund um die Uhr. Damit werden die Möglichkeiten massiv erweitert, um das Sicherheitsniveau nachhaltig anzuheben, Cybergefahren zu identifizieren und somit SIX und ihre Finanzmarktinfrastrukturen zu schützen. Derzeit ergeben sich aus der Milliarde Logmeldungen dreissig potenzielle Bedrohungen oder Sicherheitslücken pro Tag, die geprüft und behandelt werden.

Cybersicherheit als Geschäftsfeld

SIX unterstützt ihre Kunden neu in der Bekämpfung von Cyberkriminalität. Sie nimmt anderen Unternehmen den kostspieligen Aufbau und den Rund-um-die-Uhr-Betrieb eines SOC ab und stellt die erforderlichen, auf Cybersicherheit spezialisierten Analysten. Insbesondere kleinere und mittlere Banken und Versicherungen erhalten dadurch Zugang zu einer maximalen Sicherheitslösung, wie sie sonst nur Grossunternehmen für sich entwickeln können. Die Daten bleiben dabei jederzeit beim Kunden – und immer in der Schweiz –, nur die Ereignisse werden für die Analyse weitergeleitet. Ergänzend wird SIX Trainings- und Weiterbildungsangebote lancieren und das Teilen von Erkenntnissen zur Bedrohungslage unter allen Beteiligten fördern und vereinfachen.

Thomas Koch
Head Corporate Security, SIX

ORGANISATORISCHE VERNETZUNG

SIX ist ein aktives Mitglied in den Schweizer Security Communities und tauscht Gefahrenmeldungen sowie Informationen mit anderen Finanzteilnehmern aus und erhält entsprechende Meldungen, die vor Cybergefahren schützen.

Zudem hat SIX in diesem Jahr den SIX Cyber Hub lanciert, eine branchenspezifische, interdisziplinäre und multilaterale Initiative. Sie steht allen Teilnehmern am Schweizer Finanzplatz offen. Der SIX Cyber Hub will die Resilienz, die Zusammenarbeit, den Informationsaustausch und das «digitale Vertrauen» in die Cyberwiderstandsfähigkeit des Finanzplatzes Schweiz stärken.

FAKTEN & ZAHLEN

- 1765 Cybereinbrüche wurden 2017 bei Firmen weltweit registriert
- 2,6 Milliarden Dateneinträge wurden dabei entwendet
- USD 3,62 Millionen kostet eine Firma ein Cybereinbruch im Durchschnitt
- 94 Schweizer Firmen waren 2017 Opfer einer Cyberattacke

EU-Datenschutz auch für den Finanzplatz Schweiz

Die revidierte EU-Datenschutz-Grundverordnung ist seit dem 25. Mai 2018 in Kraft. Was beinhaltet sie? Wen betrifft sie? Und welche Auswirkungen hat sie auf den Schweizer Finanzplatz und seinen Zahlungsverkehr?

Die EU-Datenschutz-Grundverordnung (DSGVO oder Englisch: GDPR) wurde erlassen, um die Datenschutzgesetze der europäischen Länder zu harmonisieren, den Datenschutz der EU-Bürger zu bekräftigen und die entsprechende Transparenz zu gewährleisten. Damit wird auch das Datenschutzvorgehen der Unternehmen und Organisationen in den EU-Mitgliedstaaten neu gestaltet.

Wer ist von der Verordnung betroffen?
Sämtliche Unternehmen, die personenbezogene Daten von natürlichen, in der EU wohnhaften Personen (Kunden, Angestellten etc.) verarbeiten, müssen die Verordnung umsetzen, ungeachtet ihres eigenen Standorts. Somit gilt die Verordnung auch für in der Schweiz ansässige Unternehmen, sofern sie Geschäftsbeziehungen mit in der EU wohnhaften Personen

Details zur DSGVO sind unter www.EUGDPR.org verfügbar.

unterhalten bzw. solchen Personen Services anbieten, nicht aber für in der Schweiz domizilierte Personen mit Geschäftsbeziehungen in der Schweiz.

Happige Bussen
Das Nichteinhalten der DSGVO kann mit einer Busse von bis zu 4% des jährlichen Geschäftsumsatzes oder mit EUR 20 Millionen geahndet werden (abhängig davon, welcher der beiden Beträge grösser ist).

Auswirkungen auf den Zahlungsverkehr
Die DSGVO muss auch im Zahlungsverkehr immer dann umgesetzt werden, wenn personenbezogene Daten verarbeitet werden. Einerseits müssen die DSGVO-Rechte natürlicher Personen gewährleistet werden. Anderseits muss sichergestellt sein, dass die Prozesse und Systeme den Datenschutzanforderungen entsprechen und umfänglich dokumentiert sind. Dies betrifft die Speicherung, Verarbeitung und Übertragung von Personendaten sowohl in bankinternen als auch in cloudbasierten Applikationen, die typischerweise E-Banking-Aktivitäten bzw. Zahlungs- und Börsenaufträge betreffen. Dabei gilt es zu beachten, dass in den entsprechenden Middle- bzw. Back-End-Prozessen der Banken bereits heute weitgehend technische Identifikatoren zur Anwendung gelangen, die keine Rückschlüsse auf konkrete Personen zulassen.

Implizite Zustimmung unzulässig
Auch Dienstleister und Arbeitgeber, die nur auf dem Finanzplatz Schweiz aktiv sind, müssen die EU-Richtlinie bei Kunden und Mitarbeitenden mit Wohnsitz in der EU einhalten. Implizite Zustimmungen sind nicht zulässig. Der Kunde oder Mitarbeiter muss der Datenhaltung explizit zustimmen; das Kreuz im entsprechenden Feld ist gegebenenfalls explizit zu setzen. Das Service-Angebot bzw. die Anstellung darf nicht von der Zustimmung hinsichtlich einer erweiterten Datenhaltung abhängig gemacht werden.

Das Schweizer Datenschutzgesetz wird zurzeit, zwecks Anlehnung an die neue DSGVO, überarbeitet und gilt nachher voraussichtlich entsprechend für alle Kunden und Mitarbeitenden von Schweizer Dienstleistern und Arbeitgebern.

Manuela Giordano & Alain Hiltgen
UBS Business Solutions AG

SCHWERPUNKTE DER REVIDIERTEN VERORDNUNG

Datenschutz «by design and by default»
Ein Unternehmen, das personenbezogene Daten verarbeitet, muss sicherstellen, dass der Schutz der Daten zu jedem Zeitpunkt der Verarbeitung mithilfe technischer und organisatorischer Massnahmen gewährleistet ist. Ebenso muss ein Unternehmen sicherstellen, dass standardmässig nur personenbezogene Daten verarbeitet werden, die für den Geschäftszweck notwendig sind. Dies gilt sowohl für die Anzahl der gesammelten Daten und deren Verarbeitung als auch für die Dauer der Speicherung und den Zugriff auf diese Daten.

Die Rechte natürlicher Personen
Die Verordnung bringt natürlichen Personen Transparenz und entsprechende Handlungsermächtigung in Bezug auf ihre personenbezogenen Daten.

Auskunftsrecht der betroffenen Personen
Jede Person hat das Recht zu erfahren, ob, wo und zu welchem Zweck ein Unternehmen personenbezogene Daten von ihr verarbeitet. Zusätzlich muss jeder betroffenen Person eine Kopie der verarbeiteten Daten in elektronischem Format zugänglich gemacht werden.

Recht auf Datenübertragbarkeit
Mit der DSGVO erhalten natürliche Personen das Recht, von einem Unternehmen diejenigen personenbezogenen Daten zu erhalten, die sie ihm im Rahmen der Geschäftsbeziehung zur Verfügung gestellt haben.

Recht auf Löschung
Jede Person hat das Recht, die Löschung ihrer personenbezogenen Daten zu verlangen sowie deren Verbreitung und allenfalls deren Verarbeitung durch Dritte zu stoppen.

Meldung von Datenschutzverletzungen
Mit der DSGVO müssen Datenschutzverletzungen gemeldet werden, die zu einem potenziellen Risiko für die Rechte und die Freiheit einer natürlichen Person führen könnten. Auch die betroffenen Personen müssen eine Information erhalten. Die Meldung hat innerhalb von 72 Stunden zu erfolgen.

Benennung eines Datenschutzbeauftragten
Unternehmen, die in ihrem operativen Geschäftsfeld personenbezogene Daten in grossem Umfang verarbeiten, müssen einen Datenschutzbeauftragten mit entsprechenden Befugnissen ernennen.

Nach der Harmonisierung ist vor der Harmonisierung

Ein wichtiges Etappenziel ist erreicht: Ende Juni 2018 haben über 80% der Schweizer Unternehmen ihren Zahlungsverkehr auf ISO 20022 umgestellt. Die anhaltende Dynamik lässt darauf schliessen, dass die flächendeckende Umstellung Ende Jahr erreicht ist. Das unterstreicht auch eine von gfs.bern im Frühling durchgeführte repräsentative Umfrage. Danach haben bereits 90% der Befragten ein Umstellungsprojekt gestartet und werden es Ende Jahr abgeschlossen haben. Damit ist die Brücke zur QR-Rechnung geschlagen, die Mitte 2020 eingeführt wird.

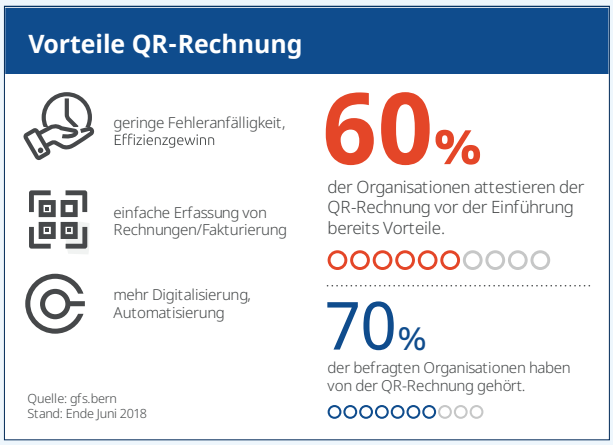
Gemäss gfs.bern-Umfrage ist die erfolgreiche Umstellung im Wesentlichen auf die Leistungsvorteile von ISO 20022 sowie die Informationsarbeit von Banken und Softwareunternehmen zurückzuführen. Sie haben ihre Kunden in den letzten Monaten aktiv mit Informations- und Beratungsarbeit begleitet. Rund 70% der betroffenen Unternehmen wurden von einem externen Partner unterstützt, 90% erhielten von ihrer Bank Informationen und zeigten sich gleichzeitig auch sehr oder eher zufrieden mit der Unterstützung.

In Anbetracht dieser hohen Werte können die Informationsarbeit und die Hilfestellung der Banken und Softwareunternehmen als wesentlicher Erfolgsfaktor für ein Infrastrukturprojekt dieser Grössenordnung gewertet werden.

Leistungsvorteile punkten

ISO 20022 hat sich in den letzten Monaten als wichtige Grundlage für die Optimierung wesentlicher Finanzabläufe erwiesen. 60% der Organisationen verbinden die Standardisierung des Zahlungsverkehrs mit Vorteilen. Dieser Wert steigt auf deutlich über 70%, je regelmässiger und häufiger Zahlungen getätigt werden und je weiter man im Umstellungsprozess vorangeschritten ist.

Zu den meistgenannten Vorteilen zählen die Digitalisierung der Geschäftsprozesse, die Vereinfachung von Ausland- und Inlandzahlungen sowie eine tiefere Fehleranfälligkeit dank der Verwendung der IBAN. Das lässt den Schluss zu, dass sich ISO 20022 in der Praxis bewährt. Über alle Umfrageergebnisse hinweg ist



augenfällig, dass mit zunehmender Alltagserfahrung die Vorteile deutlicher wahrgenommen werden, als es bei Organisationen mit gestartetem Projekt der Fall ist.

Umstellungslücken schliessen
Folglich kann durch die Vermittlung von positiven Umfragewerten und Erfahrungen die Umstellung nochmals forciert werden. Es ist von zentraler Bedeutung, dass bis Ende 2018 alle Firmenkunden die Umstellung auf ISO 20022 abgeschlossen haben. Die Einhaltung dieses Termins ist wichtig, da der bisherige Standard DTA seit Anfang Juli 2018 nicht mehr von SIX unterstützt, weiterentwickelt und dokumentiert wird. Es liegt in der Verantwortung jeder einzelnen Bank, die Lücken bei der Migration ihrer Firmenkunden termingerecht zu schliessen. Ohne flächendeckende Umstellung kann die QR-Rechnung nicht eingeführt werden, und sie wird bereits heute als wesentlicher Bestandteil der ganzen Harmonisierung wahrgenommen.

Hohe Erwartungen an die QR-Rechnung
70% der von gfs.bern Befragten haben von der QR-Rechnung gehört, rund 60% attestieren ihr bereits vor der Einführung nur oder eher Vorteile. Die positive Haltung bestärkt den Finanzplatz Schweiz in der Absicht, die QR-Rechnung gut abgestützt einzuführen und die bislang wertvollen, punktuell eingegangenen Marktrückmeldungen in die nächste Etappe einzubringen. Dazu wird seit Ende Juli ein öffentliches Konsultationsverfahren durchgeführt, über dessen Ausgang Mitte November 2018 informiert wird. Mit diesem Vorgehen wird sichergestellt, dass sich die Marktteilnehmer einbringen können und die QR-Rechnung breit abgestützt und damit erfolgreich ab 30. Juni 2020 eingeführt werden kann.

Gabriel Juri
SIX Interbank Clearing

Konsultation zu den Implementation Guidelines QR-Rechnung

Die Schweizer Implementation Guidelines QR-Rechnung (Version 1.0 vom 27.04.2017) sollen in folgenden acht Punkten revidiert und an die aktuellen Marktbedürfnisse angepasst werden:
- Einführung einer Perforationspflicht für papierbasierte Zahlungen
- Einführung eines Empfangsscheins
- Vereinfachung bei den strukturierten Adressen
- Keine Anzeige von Strukturinformationen des Rechnungsstellers
- Vereinfachung der Kombinationsmöglichkeiten bei strukturierten Referenzen
- Vorerst keine Verwendung des Feldes «Endgültiger Zahlungsempfänger»
- Vorerst keine Verwendung des Feldes für alternative Verfahren
- Einführung einer zusätzlichen lizenzfreien Schriftart für nicht Microsoft-User

Das Konsultationsverfahren richtet sich insbesondere auch an Banken und ERP-Softwarehersteller, die ihre Produkte und Dienstleistungen auf Basis der Schweizer Implementation Guidelines QR-Rechnung entwickeln.

ISO 20022 – erfolgreich eingeführt

90%
der Firmenkunden haben ein Umstellungsprojekt gestartet.

Quelle: gfs.bern
Stand: Ende Juni 2018

80%

der Firmenkunden haben ihre Umstellung abgeschlossen und 80% des Transaktionsvolumens migriert.

Quelle: SIX Interbank Clearing AG
Stand: Ende Juni 2018

MEHR ZUM THEMA:

Mehr über Cybersicherheit
in der Ausgabe 73 vom Dezember 2017

Mehr zur Swiss Value Chain
in der Ausgabe 68 vom September 2016

Mehr zu ISO-Umstellung & QR-Rechnung
in der Ausgabe 74 vom März 2018