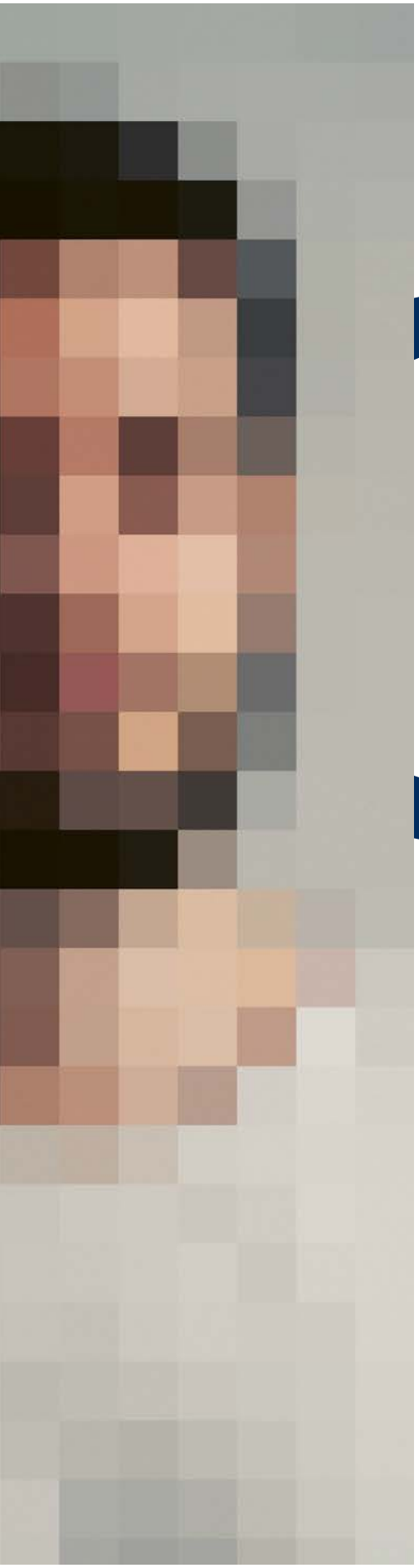
pay

Das Fachmagazin von SIX für den Zahlungsverkehr — #6 — 2022

Wie der Finanzplatz offensiv gegen Cyberkriminelle vorgeht — Future Talk mit Hannes Lubich — Von Hackers und Crackers — Kleingeld am Checkout — Multibanking dank «Relay»

Herausgeberin SIX Group AG, Postfach, 8021 Zürich, Schweiz, six-group.com/pay, pay@six-group.com Fachbeirat Daniel Berger, SIX; Boris Brunner, Leitung, SIX; Angelika Christian, SECB; Laura Felber, SNB; Pierre-Michel Gicot, BCV; Susanne Höhener, Liechtensteinischer Bankenverband; Daniela Hux-Brauss, Credit Suisse (Schweiz) AG; Raphael Reinke, SNB; Peter Ruoss, UBS Switzerland AG; Stefan Schneider, PostFinance; Nino Thommen, SIX Redaktion Gabriel Juri, Leitung, SIX Konzept & Design *MADE* Identity AG, Zürich, Schweiz Lithografie Marjeta Morinc Druck sprüngli druck ag, Villmergen, Schweiz Übersetzungen Mark Rabinowitz, Translation Service Team, SIX (Englisch); Denis Fournier (Französisch) Bildnachweise Jessica Radanavong (Cover), Vova Krasilnikov (S. 3), Arthur Hidden (S. 4), Jassir Jonis (S. 6), Ornella Cacace (S. 2, 10), Tobias Siebrecht (S. 13) Illustrationen Gregory Gilbert-Lodge (S. 2, 7, 12)

2021 gab es über 30 000 polizeilich registrierte Cyberstraftaten in der Schweiz, rund ein Viertel mehr als ein Jahr zuvor.



Cyberabwehr: Die Schweiz rüstet auf

TEXT
THOMAS KOCH
HEAD CORPORATE SECURITY, SIX

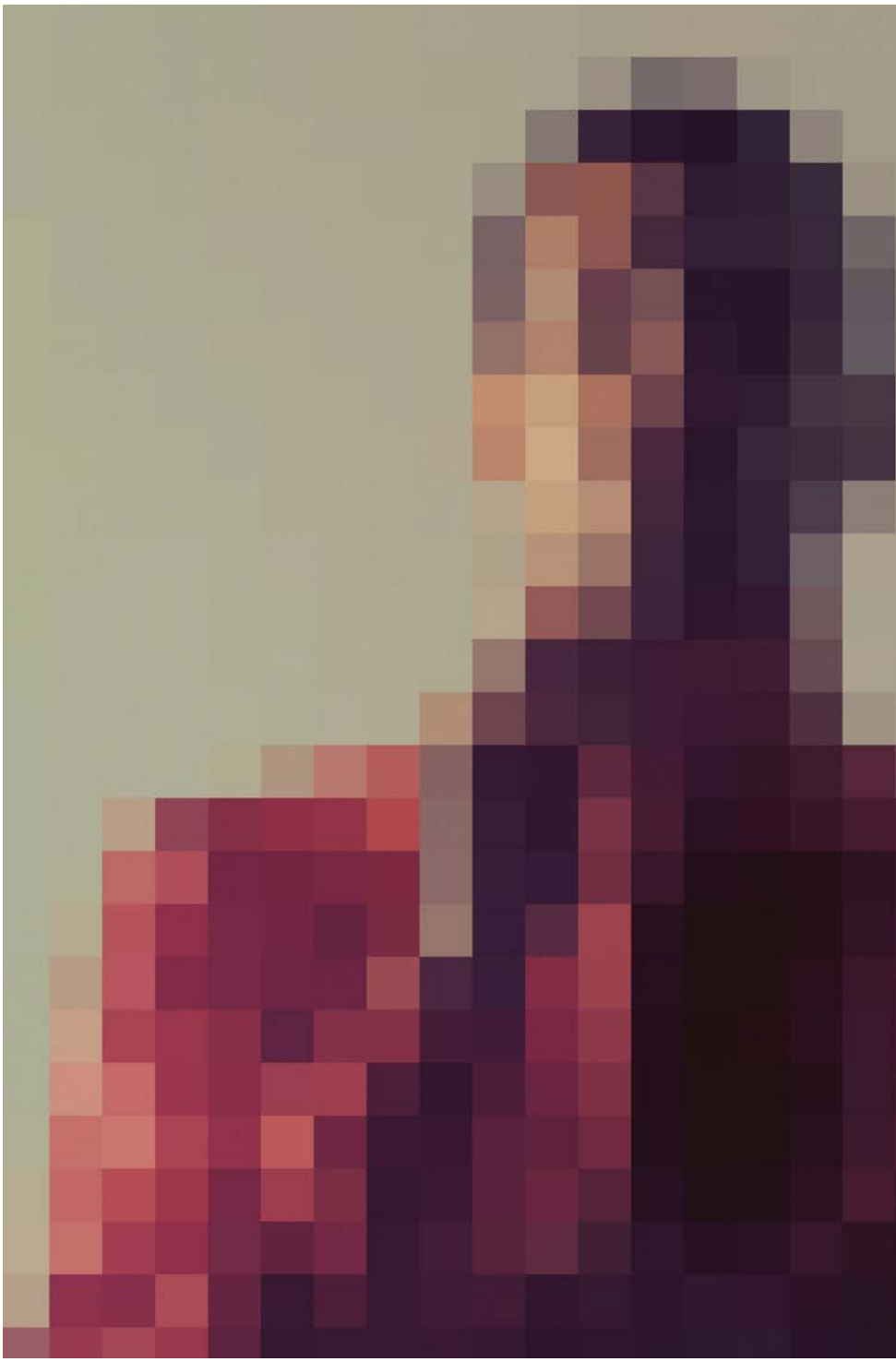
Gelegenheit macht Diebe. In der Gegenwart und zu allen Zeiten der Menschheitsgeschichte. Alles, was nicht niet- und nagelfest ist, wird gestohlen. Gewissermassen im Vorbeigehen entwendet der mittelalterliche Dieb an Jahrmärkten Brot, Geflügel, Wams, Kerzen und Geld – Letztere oft auch aus den Kirchen. Heute sind die Tatorte etwa Einkaufszentren. Oder Museen, aus denen Gemälde, Edelsteine oder Neandertaler-Zähne verschwinden. Oder Computer, wo Daten das Diebesgut werden. Oft gehen Diebstahl und Erpressung Hand in Hand. Bei der musealen Beute ist die Rede von «Artnapping», wenn die Täterschaft damit droht, das Gestohlene zu zerstören, falls kein Lösegeld gezahlt wird. Bei der digitalen Beute spricht man von «Ransom». Hier wie dort gehen die Kriminellen weitgehend gewaltlos vor. Darüber hinaus ist die Dunkelziffer in allen genannten Bereichen hoch und die Geschädigten bemühen sich im Nachhinein um bessere Bewachung und die technische Sicherung ihrer «Schätze».

Ransomware-Attacken auf Unternehmen sind keineswegs neu, nehmen in letzter Zeit aber exponentiell zu. Dagegen verzeichnet die Polizeiliche Kriminalstatistik seit Jahren einen deutlichen Rückgang der nicht-digitalen Diebstahldelikte. Ob nur eine zufällige Korrelation oder Kausalität dahinter stecken, bleibt dahingestellt. Tatsache ist, dass die zunehmende Digitalisierung und Vernetzung enorme Auswirkungen auf die Informationssicherheit haben und das Risiko auch für den Finanzsektor erhöhen. Gleichzeitig verhalten sich die Cyberkriminellen immer raffinierter und verfügen über erhebliche finanzielle Mittel, die oft «Sponsoren» beisteuern. Zur neusten Generation von Angreifern mit entsprechenden Fähigkeiten gehören staatlich oder von Unternehmen gesponserte Gruppen und die organisierte Kriminalität. Deren Motive können über finanzielle Interessen hinaus auch politische Hintergründe haben. Neben Attacken mit Ransomware-Schadsoftware stehen zwei weitere Methoden der Cybererpressung im Vordergrund: Angriffe auf die Lieferkette, die auf schwächere Dritte abzielen, die ihrerseits Zugang zu kritischen Systemen haben, und sogenannte verteilte Denial-of-Service-Angriffe (DDoS), die darauf abzielen, einen Dienst zu unterbrechen oder den Zugang für eine bestimmte Zielgruppe einzuschränken.

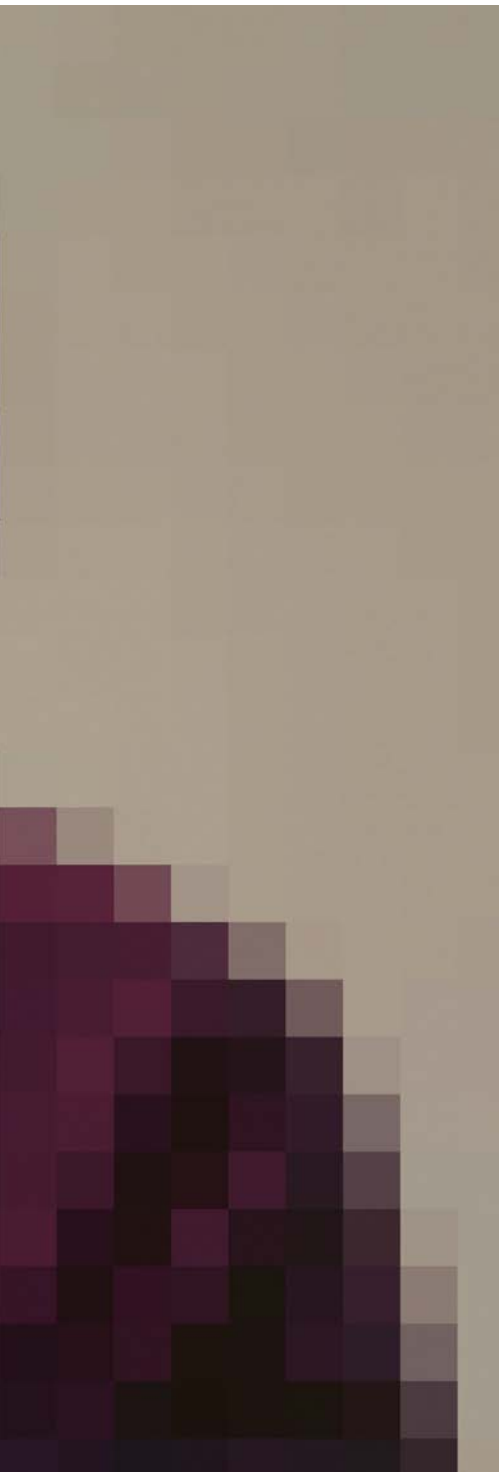
Zuletzt waren mehrere Finanzakteure im Ausland solchen Angriffen ausgesetzt. So zum Beispiel die neuseeländische Börse, wo DDoS den Handel für zwei Tage unterbrochen hat. Bei der American Bank

«Je kritischer die Sicherheitslücke, desto mehr Belohnung erhält eine ethische Hackerin.»

Erhöhung der Sicherheit im SIC-System: Endpunktsicherheit und SSFN Die Auswirkungen von betrügerischen Zahlungen in Grossbetragszahlungssystemen wie dem SIC-System können nicht nur für die direkt betroffenen Teilnehmer, sondern auch für das Zahlungssystem als Ganzes weitreichend sein. Besonders problematisch ist die Einlieferung von betrügerischen Zahlungen infolge einer Kompromittierung von Endpunkten der SIC-Teilnehmern, d. h. Geräten, Applikationen oder Systemen, die ein SIC-Teilnehmer für den Meldungsaustausch mit dem SIC-System benötigt. Zur Erhöhung des Schutzes der Endpunkte aller SIC-Teilnehmer wird die Schweizerische Nationalbank für sie in Kürze ein verbindliches Framework erlassen. Darin enthalten werden betriebliche und technische Anforderungen zum Schutz der Endpunkte sein, die bis Ende 2024 entweder durch die SIC-Teilnehmer oder die durch sie beauftragten Service Provider umzusetzen sind. Daneben wird auf Systemebene die durchgängige Verwendung des internetunabhängigen Secure Swiss Finance Network (SSFN) in der Kommunikation zum SIC-System einen wichtigen Beitrag zur Resilienz und Ausfallsicherheit im SIC-System leisten. Seit Anfang Juni können SIC-Teilnehmer SSFN als zusätzlichen Zugangsweg – nebst Finance IPNet und SWIFTNet – zum SIC-System nutzen.



Die Cyber-Wirtschaftskriminalität (Phishing, Hacking, Malware, DDoS) machte 2021 nahezu 88 % aller digitalen Straftaten in der Schweiz aus.



Systems führte der Ransomware-Angriff nicht nur zu einer Lösegeldforderung in Höhe von 14 Millionen US-Dollar, sondern auch zu einer Sammelklage.

Neue Organisation für die Cyberresilienz des Schweizer Finanzsektors

Im Vergleich auch mit den umliegenden Ländern scheint die Schweiz der Cyberkriminalität weniger stark ausgesetzt zu sein. Gemäss der Studie eines britischen Sicherheitssoftwareherstellers wurden letztes Jahr hierzulande 0,7 Prozent der Firmen wöchentlich von Ransomware heimgesucht. Die entsprechende Rate lag in Österreich bei 1,4, in Deutschland bei 1,6, in Frankreich bei 1,8 und in Italien bei 1,9 Prozent.

In der Schweiz ist das Nationale Zentrum für Cybersicherheit (NCSC) erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Es unterstützt zudem insbesondere die Betreiber kritischer Infrastrukturen beim Schutz vor Cyberrisiken. Unter seiner Leitung wurde ausserdem im April 2022 der Verein «Swiss Financial Sector Cyber Security Centre» (Swiss FS-CSC) gegründet, der seinerseits die institutionelle Zusammenarbeit zwischen Finanzinstituten und Behörden zu strategischen und operativen Fragen rund um die Cybersicherheit fördern will. Insbesondere soll er den Informationsaustausch zwischen den Finanzmarktakteuren erleichtern und die Zusammenarbeit bei präventiven, sektorweiten Massnahmen und bei der Bewältigung von systemischen Krisensituationen verbessern.

Solche Krisen sind dann systemisch relevant, wenn sie die Zahlungs- und Effektenabwicklungssysteme betreffen. SIX als Betreiberin dieser Schweizer Finanzmarktinfrastrukturen hat selbstredend ein ausserordentliches Interesse an dieser Zusammenarbeit und engagiert sich als Gründungsmitglied. Aktuell zählt der Verein über 100 hiesige Banken, Versicherungen und Finanzverbände, welche die Eidgenössische Finanzmarktaufsicht FINMA überwacht. Letztere ist als «Affiliate» ebenfalls mit im Boot. Organisatorische Pfeiler sind das Steuerungsgremium, eine Expertengruppe und die Operative Cybersicherheitszelle (OCS). Das Steuerungsgremium koordiniert bei systemischen Cybervorfällen die Massnahmen zur Krisenbewältigung und übernimmt die Kommunikation innerhalb und ausserhalb des Vereins.

Die vereinsinterne Expertengruppe führt Projekte zur Stärkung der Cyberresilienz durch und organisiert strategische und operative Cyberübungen für ihre Mitglieder.

Die OCS schliesslich verfolgt die Lage im Finanzmarkt, tauscht Informationen über relevante Vorgänge aus, verfasst sektorspezifische Berichte und unterstützt die Vereinsmitglieder bei der Krisenbewältigung. Für diese Aufgabe ist die Zusammenarbeit mit einem in diesem Bereich international erfahrenen Dienstleister vorgesehen.

Offensive Cybersicherheit

SIX als das Rückgrat der systemisch bedeutsamen Finanzmarktinfrastrukturen nimmt eine herausragende Rolle wahr bezüglich Stabilität und Sicherheit des Schweizer Finanzplatzes. Sie führt ein strukturiertes und laufend aktualisiertes Risikoregister, inklusive Risiken der Informationssicherheit. Die Reaktionen auf Bedrohungen umfassten in den letzten Jahren technische Massnahmen zur Unterstützung der Basissicherheit, den Aufbau von Fähigkeiten und Simulationen sowie organisatorische Massnahmen. Die aktualisierte Informationssicherheitsstrategie beinhaltet auch neue Initiativen wie beispielsweise verbesserte Reaktionszeiten im Schwachstellenmanagement, den erweiterten Schutz vor Ransomware-Angriffen oder die ständige Verbesserung und Ausweitung ihres Security Operations Centers (SOC).

Neu befasst sich ein Team mit der sogenannten offensiven Cybersicherheit. Es macht sich die Szenarien, Angriffs-

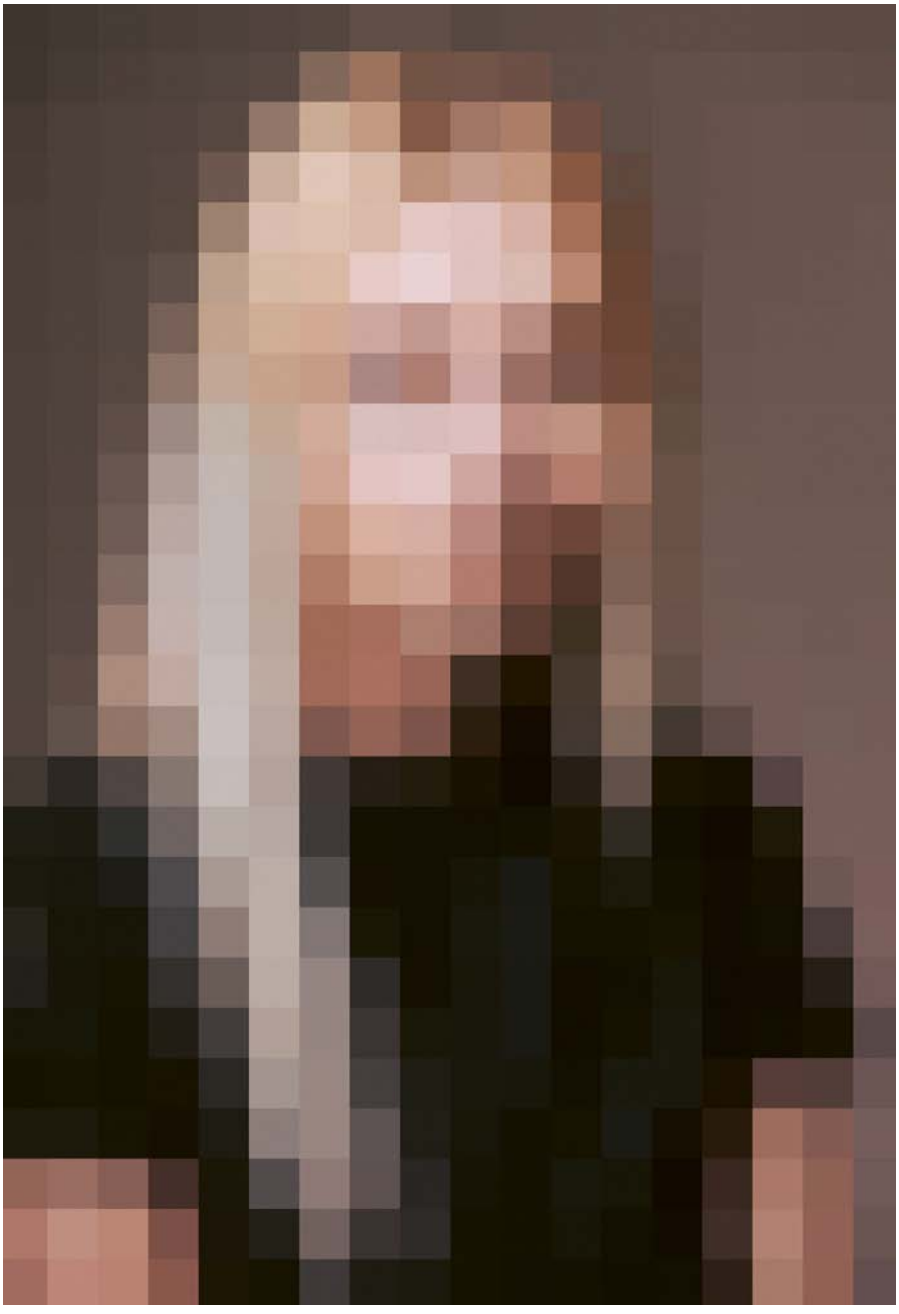
techniken und Methodiken echter Hackerinnen und Hacker zu eigen und bildet sie in einer kontrollierten Umgebung nach. Dazu gehören «Penetration Testing», «Adversary Emulation» und «Vulnerability Disclosure Program». Penetration Testing zielt darauf ab, systematisch in Applikationen und Systeme einzudringen, um Sicherheitslücken aufzudecken und diese den Entwicklerinnen und Betreibern mitzuteilen. Adversary Emulations dienen dazu, die Ausfallsicherheit eines Netzwerks gegen fortgeschrittene Angreifer oder Bedrohungen mit oder ohne Vorwarnung zu testen und die gewonnenen Erkenntnisse in die Schulung defensiver Cybersicherheit einzubeziehen.

Beim Vulnerability Disclosure Program (auch Bug-Bounty-Programm genannt) handelt es sich um den neuesten Trend in der offensiven Cybersicherheit. Es erlaubt das gezielte Angreifen von Systemen durch ausgewählte ethische Hackerinnen und Hacker, die für ihre Arbeit finanziell entlohnt werden. Alle können von überall auf der Welt proaktiv einen Vorfall oder Verdachtsfall, der die Informationssicherheit betrifft, online bei SIX melden.

Anfang April 2022 hat SIX ein solches Programm erarbeitet, das zunächst am Internet angebundene Systeme im Fokus hat. Zu einem späteren Zeitpunkt sollen auch interne Systeme oder Cloud-Services «ethisch» gehackt werden können. Das Bug-Bounty-Programm bietet viele Vorteile. Zum einen gibt es weltweit Tausende in der Hackerszene mit unterschiedlichen, kreativen Ideen, die ein einzelnes Team niemals aufbringen kann. Zum anderen hat Jede Technologie ihre «Spezialistinnen und Spezialisten», die SIX gezielt aussuchen kann. Des Weiteren laufen solche Programme längere Zeit, auch jahrelang, wogegen klassische Penetrationstests üblicherweise nur wenige Wochen dauern. Die Entschädigung richtet sich nicht nach der investierten Zeit, sondern nach den aufgedeckten Schwachstellen. Je kritischer die Sicherheitslücke, desto mehr Belohnung erhält eine ethische Hackerin beziehungsweise ein ethischer Hacker.

Ob im Rahmen von Swiss FS-CSC oder im Austausch mit ethischen Hackerkreisen – die Zusammenarbeit wird das Risiko von Cyberangriffen auf dem Finanzplatz eindämmen helfen. Soweit und so schnell wie möglich sollen Finanzplatzakteure ihre Applikationen und Systeme niet- und nagelfest absichern können, damit Cyberkriminelle weniger Gelegenheit haben, ihr Eigentum oder das von Dritten zu stehlen.

Die grösste prozentuale Zunahme in der Schweizer Cyber-Wirtschaftskriminalitätsstatistik 2021 verzeichneten die Komponenten Phishing mit 88 % und Ransomware mit 53 % gegenüber 2020.



«Die Governance der Cybersicherheit ist nicht delegierbar.»

HANNES LUBICH,
EMERITIERTER HOCHSCHULPROFESSOR
UND STRATEGIEBERATER FÜR IT-SYSTEME,
NETZWERKE UND IT-SICHERHEIT

Die Cyberbedrohungslage in der Schweiz scheint nicht so gross zu sein wie in anderen Ländern. Woran liegt das? Wir sind schon lange ein attraktives Angriffsziel und haben, vor allem in regulierten Sektoren, einen langen Abwehrkampf mit den entsprechenden Lektionen hinter uns. Zudem können sich hiesige Unternehmen aufwendige Sicherheitsmassnahmen eher leisten, als solche in wirtschaftlich schwachen Regionen.

Kriminelle seien immer einen Schritt voraus, sagen Expertinnen und Experten. Ist Cyberschutz tatsächlich beinahe aussichtslos oder sind die Unternehmen einfach nicht auf der Höhe der Zeit? Kriminelle können heute erhebliche Mittel für immer neue Angriffsformen und das dafür nötige Fachwissen und die Infrastruktur aufwenden – in einigen Ländern durchaus auch mit Billigung oder Mitwirkung staatlicher Instanzen. Gegen gezielte Angriffe mit grossem Ressourceneinsatz ist eine effektive Verteidigung daher in der Tat schwierig. Jedoch müssen gerade auch Kriminelle ihre Kosten unter Kontrolle halten. Wird ein Angriff zu teuer, wechseln sie zum nächsten Ziel. Für Unternehmen ist es wichtig, ihren Cyberschutz so gut wie möglich auszugestalten, womöglich durch externes Fachwissen.

Wem nutzt die künstliche Intelligenz (KI) mehr? Den Chief Information Security Officers oder den Cyberkriminellen? Im Moment ist «gezielte» KI eher im kriminellen Profiumfeld im Einsatz – jedoch stützen sich auch immer häufiger Sicherheitssysteme darauf. Allerdings sind diese Systeme oft «geschlossen» und werden nur indirekt als integraler Teil einer Serviceleistung (z. B. Threat Detection & Analysis) genutzt. Zudem ist nicht jedes regelbasierte System eine «künstliche Intelligenz» – hier ist viel Marketing im Spiel.

Wer ist an der Kunde-Bank-Schnittstelle am wenigsten auf Ransomware-Attacken vorbereitet? Vor allem etwa Vermögensverwalter oder Treuhänder ohne Banklizenz, die also weder stark reguliert noch überwacht werden. Aber auch Marktteilnehmende, die nur elektronische Finanzdienstleistungen anbieten, haben nicht immer die nötige praktische Erfahrung. Sie glauben oft, sie könnten die Cybersicherheit zusammen mit der restlichen IT auf externe Dienstleister abwälzen. Die diesbezügliche «Governance» ist jedoch nicht delegierbar.

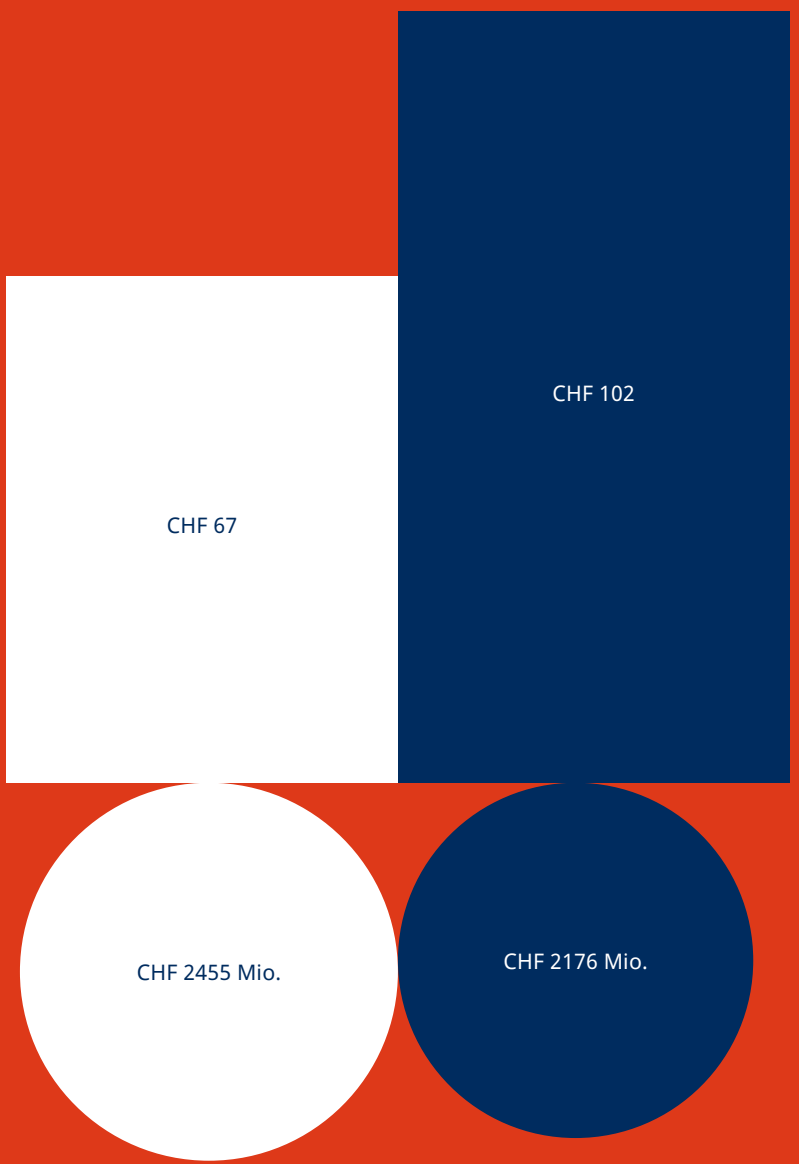
Inwieweit sind gesetzliche Grundlagen für Cybersicherheit zielführend? Gesetzliche Vorgaben erzeugen den nötigen Handlungsdruck, um Cybersicherheit auch dort zu etablieren, wo die Überzeugungsarbeit nicht gelingt. Der Finanzsektor ist hier schon sehr gut abgedeckt. Unternehmen der Industrie sind oft noch nicht ausreichend sensibilisiert. Diese laufen Gefahr, geistiges Eigentum, Umsatz oder ihren Ruf bei Partnern und Kundinnen zu verlieren. Hier können Gesetze durchaus positiv wirken, sofern sie nicht überregulieren und keine neuen Risiken und Chancenungleichheiten im Markt mit sich bringen.

TEXT
GABRIEL JURI

Die Durchschnittsbeträge in- und ausländischer Karten in und ausserhalb der Schweiz unterscheiden sich merklich – exemplarisch für den Monat Juni 2022.

Der Durchschnittsbetrag von Transaktionen mit in der Schweiz herausgegebenen Kreditkarten fällt im Ausland höher aus als im Inland. Ein Grund könnte sein, dass im Ausland eher grössere Ausgaben anfallen (z. B. Wocheneinkäufe oder Hotelübernachtungen), während zuhause tägliche Kleineinkäufe überwiegen.

- Inländische Kreditkarten in der Schweiz
- Inländische Kreditkarten im Ausland

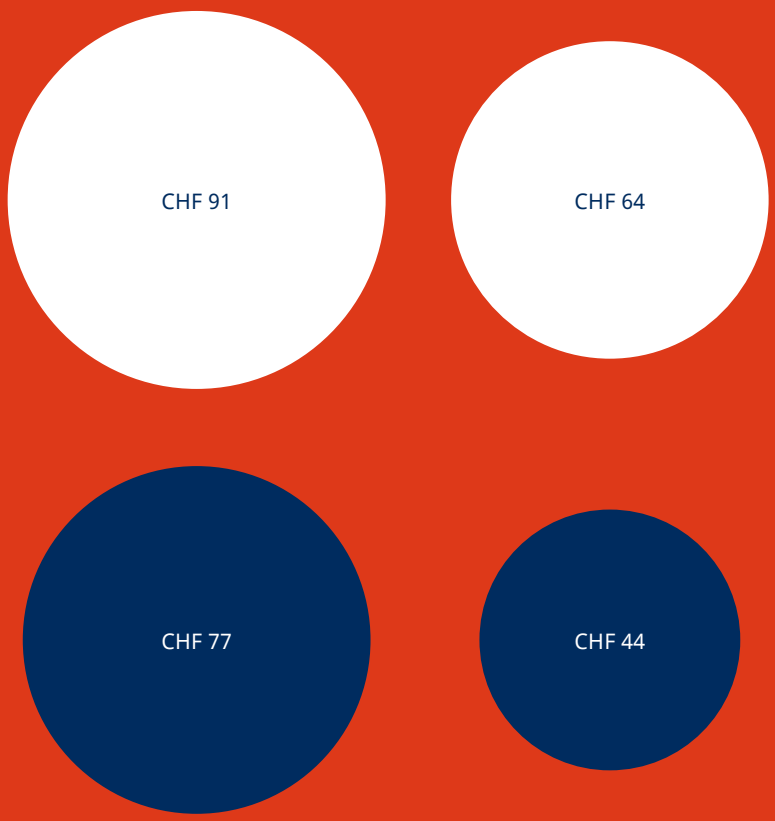


Quelle Datenportal der Schweizerischen Nationalbank, Zahlungen und Bargeldbezüge.
Die Daten entstammen einer Teilerhebung. Mehr Informationen: Finanzmarkt (data.snb.ch)

Debitkartenbeträge pro Transaktion

Personen mit ausländischen Debitkarten (etwa Feriengäste oder Grenzgänger) geben hierzulande pro Zahlung weniger Geld aus als Herr und Frau Schweizer im Ausland.

- Inländische Debitkarten im Ausland
- Ausländische Debitkarten in der Schweiz



Beträge pro Kreditkartentransaktion (nur Präsenzgeschäft)

Beträge pro Debitkartentransaktion (nur Präsenzgeschäft)

Auch mit Fokus aufs Präsenzgeschäft* zeigt sich: Die Durchschnittsbeträge mit ausländischen Karten im Inland unterscheiden sich erheblich von jenen mit inländischen Karten im Ausland – sowohl bei den Debit- als auch bei den Kreditkarten.

* Das Präsenzgeschäft umfasst sämtliche physischen Zahlungen am Zahlterminal vor Ort.

- Inländische Karten im Ausland
- Ausländische Karten in der Schweiz

Mit Ethik gegen das Hacking von Autos und Medizingeräten

TEXT
SIMON BRUNNER

Ortstermin in Zürich-Altstetten. Die Adresse führt zu einem grauen Bürogebäude. Im zweiten Stock öffnet sich eine namenlose Tür. Ein schmuckloser Gang führt in ein spartanisch eingerichtetes Sitzungszimmer. Wir sind zu Besuch bei einer Firma für Cybersicherheit, oder genauer: bei einem ehemaligen Hacker, der Unternehmen dabei unterstützt, Schwachstellen im eigenen Sicherheitsdispositiv zu finden. Sein Name: Marc Ruef.

Zuerst zu den Klischees: Ein Hacker läuft im schmuddeligen Hoodie herum? Ruef trägt gepflegten Vollbart, Anzug und Hemd. Hacker sind kriminell? «Es hat mich in meinem Leben nie interessiert, etwas zu stehlen oder jemandem zu schaden», so der 41-Jährige. Hacker bewegen sich im gesetzlichen Graubereich? Ruef doziert an der ETH und an mehreren Fachuniversitäten.

Der geborene Aargauer kam früh mit Computern in Kontakt: Mit 12 Jahren durfte er auf dem PC seines Vaters programmieren, allerdings nur wenige Stunden pro Woche. Schnell fand er heraus, wie er das Gerät selber entsperren konnte. Da er befürchtete, dass seine Aktivitäten nicht unentdeckt bleiben würden, suchte er eine Bibliothek auf und fand heraus, wie sich der Zeitstempel manipulieren lässt. Gleichzeitig stiess er auf Literatur zu Computerviren. Ab da gab es kein Halten mehr.

Hackers und Crackers

Es sind die 90er-Jahre. «Hacker» ist damals noch eine ehrenvolle Bezeichnung, die Bösen, die Kriminellen heissen «Crackers». Heute ist der Begriff nur dann positiv belegt, wenn er mit Ethik kombiniert wird. Spezialisten wie Ruef, die Computersysteme sicherer machen, sind also «ethische Hacker».

Doch zurück zum Teenager Ruef. Ihm geht es um die grösste intellektuelle Herausforderung. Der Tüftler will zeigen, dass kein IT-System wirklich sicher ist. Die Hacker-Szene ist noch jung, schnell wird er zum festen Teil der Familie. Als Ruef als einer der Ersten seine Erkenntnisse publiziert, wird er von der Szene angefeindet. Diese will nicht, dass Sicherheitslücken öffentlich gemacht und geschlossen werden. Mit 16 startet er ein wegweisendes Sicherheitsportal im Internet, mit 18 folgt das erste Buch, mit 22

Firmenwagen sind besonders anfällig für Hackerangriffe. Marc Ruef im Einsatz.

sein «Lebenswerk», wie er es nennt: «Die Kunst des Penetration Testing». Das ist ein über 900-seitiger Wälzer, der zeigt, wie man das eigene Netz systematisch auf Schwachstellen und Sicherheitslücken absuchen kann. Im Handumdrehen ist das Buch ausverkauft.

Nach der kaufmännischen Grundbildung macht Ruef sein Hobby zuerst bei einer IT-Sicherheitsfirma zum Beruf. Bereits 2002 startet er dann zusammen mit zwei Partnern die scip AG. Heute hat seine Firma 50 Mitarbeitende, berät mittlere und grössere Firmen und zeigt ihnen, wie sie sich besser vor Cyberangriffen schützen können.

Autos sind fahrbare Rechenzentren

Ruef selber hat sich mittlerweile auf aussergewöhnliche Anwendungsbeispiele der Cybersicherheit spezialisiert: Beim Car Hacking geht es darum, dass sich Angreifer in die Autoelektronik einschleusen und zentrale Funktionen wie das Starten oder Abstellen des Motors oder das Entriegeln der Türen übernehmen. «Moderne Autos sind fahrbare Rechenzentren», sagt Ruef, «es wird enorm viel Elektronik verbaut.» Doch es seien eben Ingenieure, die die Autos konzipieren, keine Cyberspezialisten. «Dementsprechend gibt es bei der Sicherheit grosse Lücken», so Ruef.

Ein anderes Steckenpferd von scip sind medizinale Geräte. So konnte Ruef mit seinem Team nachweisen, dass sich die automatische Verabreichung von Medikamenten, wie auch die Anzeige von Spitalmonitoren, über das Netzwerk manipulieren lassen. Ein bösartiger Angreifer könnte eine kranke Person überdosieren, ohne dass die Geräte eine Anomalie anzeigen und den Alarm auslösen würden. «Das Spital, das diese Geräte verwendet, war sehr besorgt», sagt Ruef, «doch der Hersteller wollte – wie so oft – die Sicherheitslücke nicht schliessen. Das war ihm zu teuer.» Erst als sich die US-amerikanische Zulassungsbehörde FDA einschaltete, wurde die Schwachstelle behoben.

Weitere moderne Formen von Cyberkriminalität, mit der sich scip befasst, sind Deepfakes – also realistisch verfälschte Fotos, Audios oder Videos –, das Schummeln beim Milliardenbusiness E-Sports und Sextortion, eine Technik, um mit kompromittierenden Inhalten Opfer zu erpressen.

Auch beschäftigt sich Ruef heute stark mit der Schnittstelle von Gesellschaft und Technologie. Es geht dabei um Fragen zum Datenschutz, zur Verwundbarkeit der Gesellschaft oder zur menschlichen Interaktion mit Systemen der künstlichen Intelligenz. Ausserdem hat Ruef ein System mitentwickelt, das weltweit digitale Angriffe voraussagt – und auch, welche Cybergruppierung in nächster Zeit besonders aktiv sein wird.

Hacken als Unifach?

«Der Bedarf an Cybersicherheit ist in den letzten zehn Jahren explodiert», sagt Ruef. Einerseits freue ihn das – seine Firma profitiert von diesem Boom –, andererseits ist er desillusioniert: «Viele Unternehmen sind zu leichtsinnig: Sie bauen komplexe IT-Systeme auf, aber es fehlen die Ressourcen, um diese zu verstehen und zu bewirtschaften.» Ruef werde oft für sein Mantra belächelt, aber er propagiert stur: «Baut eure Computersysteme so einfach wie möglich.»

Ruef war ein Hacker-Pionier und ein Autodidakt. Wie sieht die Szene heute aus? Die meisten Kandidatinnen und Kandidaten, die sich bei ihm bewerben, hätten einen Hochschulabschluss, beispielsweise in Informatik mit Schwerpunkt Sicherheit oder in Cyber Security. Oft seien sie gut ausgebildet, «aber die Kreativität bleibt etwas auf der Strecke. Hacken kann man eben nicht an der Uni lernen», so Ruef.

Zuletzt sprechen wir über künstliche Intelligenz – befürchtet Ruef, dass uns die Computer eines Tages beherrschen werden? Er lacht und verweist auf ein Poster, das an der Wand hängt. Darauf sind die Resultate eines IQ-Tests abgebildet, den Ruef mit seinem Team für digitale Assistenten entwickelt hat: Siri schneidet am besten ab, gefolgt von Alexa, Cortana und Google. «Ich machte den Test ebenfalls», sagt Ruef, «und ich war froh, den Geräten noch meilenweit überlegen zu sein.»

CBDCs kommen in Gang

Gemäss Beratungsunternehmen PwC hatten Mitte 2021 knapp 70 Prozent der Notenbanken Konzepte bzw. Prototypen für digitale Zentralbankgelder (CBDC) erarbeitet. Als erstes Land haben die Bahamas ihren Sand Dollar eingeführt. Ein Jahr später spricht der «PwC Global CBDC Index» von 80 Prozent der Zentralbanken. Zudem haben drei weitere ihre CBDCs als gesetzliche Zahlungsmittel lanciert: Nigeria, Jamaika und die sieben Mitgliedländer der Organisation Ostkaribischer Staaten. Wer sich über die weltweite rasante Entwicklung dieser Thematik umfassend informieren möchte, konsultiert den interaktiven Tracker der US-amerikanischen Denkfabrik Atlantic Council.

Weitere Informationen
www.pwc.com
www.atlanticcouncil.org/cbdctracker

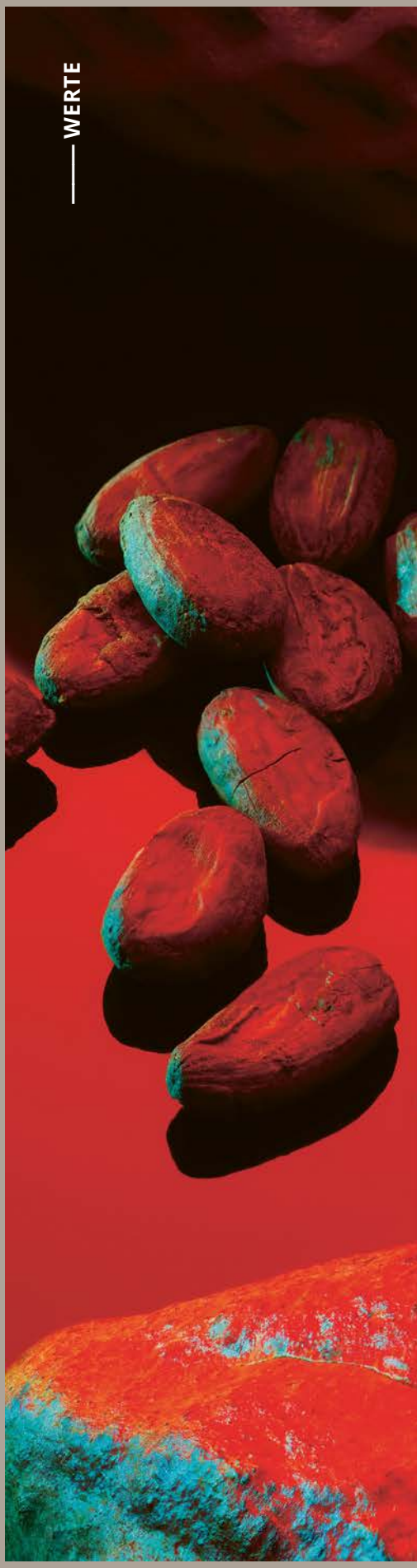
Eine Welt ohne Bargeld?

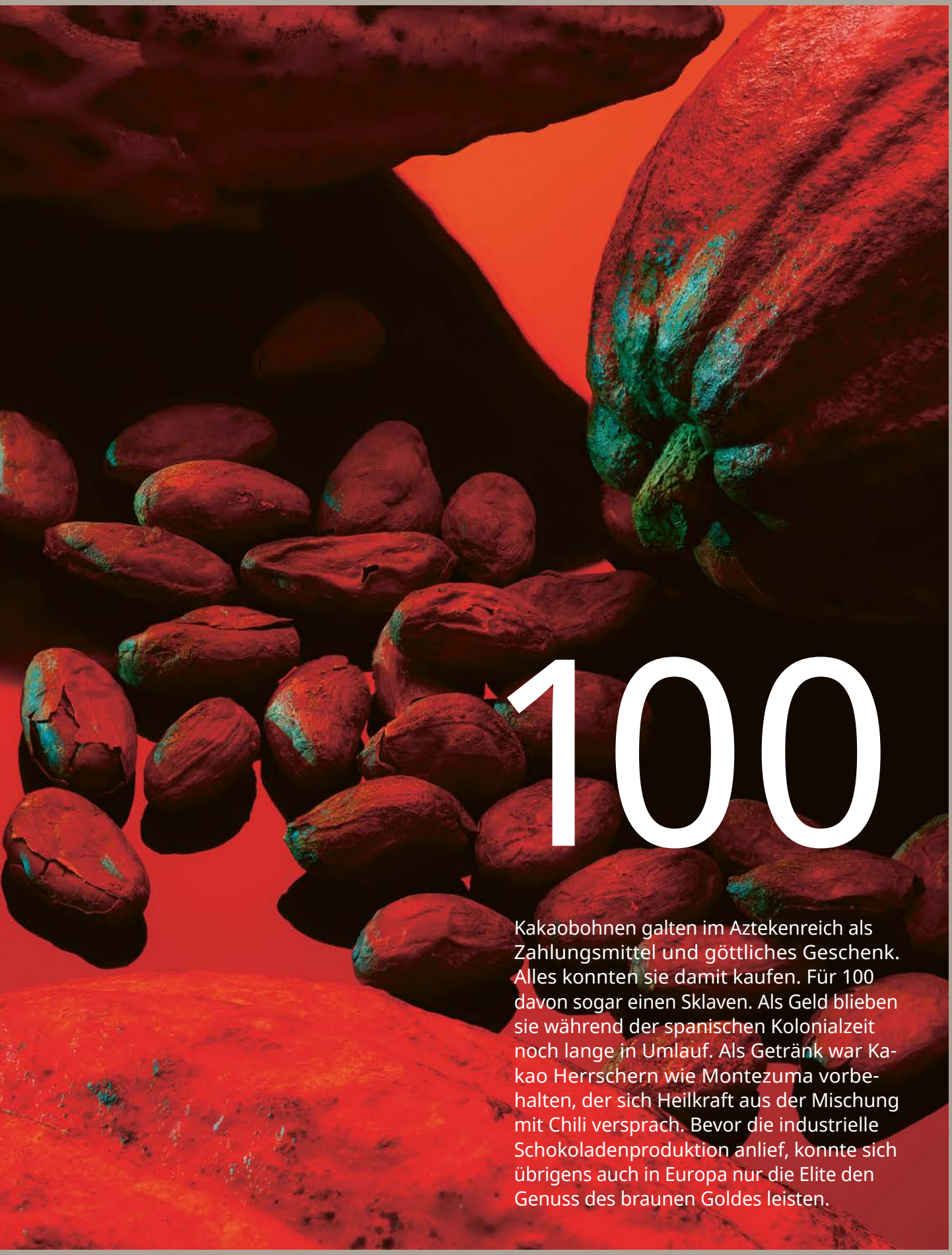
Ist es vorstellbar, dass auch in Deutschland eines Tages die Anzahl der Bargeldtransaktionen wie in Skandinavien, Island und dem Vereinigten Königreich unterhalb von 15 Prozent oder sogar niedriger liegen könnte? Dieser und weiteren spannenden Fragen rund um die Entwicklungen im Zahlungsverkehr geht das neue Gutachten «Welt ohne Bargeld – Veränderungen der klassischen Banken- und Bezahlsysteme» zuhanden des Deutschen Bundestags nach.

Weitere Informationen

Seit 26. August zeigt das Schweizer Finanzmuseum die Sonderausstellung «Banken im Wandel: vom Schalter zur App» – mit einem Blick zurück in die Geschichte der Einzahlungsscheine.

Weitere Informationen
finanzmuseum.ch





100

Kakaobohnen galten im Aztekenreich als Zahlungsmittel und göttliches Geschenk. Alles konnten sie damit kaufen. Für 100 davon sogar einen Sklaven. Als Geld blieben sie während der spanischen Kolonialzeit noch lange in Umlauf. Als Getränk war Kakao Herrschern wie Montezuma vorbehalten, der sich Heilkraft aus der Mischung mit Chili versprach. Bevor die industrielle Schokoladenproduktion anlief, konnte sich übrigens auch in Europa nur die Elite den Genuss des braunen Goldes leisten.

Jetzt wird es ernst mit den strukturierten Adressen

Benötigtes Wissen
— Kenntnis des ISO-20022-Standards
— Vorwissen über Adressdatenhaltung

Seit geraumer Zeit steht fest, dass SWIFT die strukturierten Adressen gemäss ISO-20022-Standard im November dieses Jahres für den grenzüberschreitenden Zahlungsverkehr ermöglicht und auf November 2025 verpflichtend einführt. Auch die Tatsache, dass sich der Finanzplatz Schweiz den internationalen Rahmenbedingungen anpasst und ebenfalls per November 2025 die Verpflichtung zur Nutzung der strukturierten Adressen einführt, ist seit längerem bekannt. Nun wird es zum ersten Mal konkret. Während man in der Schweiz schon seit der Umstellung auf ISO 20022 die strukturierten Adressen nutzen kann, wird dies nun auch bei grenzüberschreitenden Zahlungen mit der Migration im SWIFT-Netzwerk von den bisherigen MT- auf die neuen MX-Meldungen möglich. In zwei Fällen ist die Nutzung der strukturierten Adressen sogar vorgeschrieben, und zwar bei der Nutzung der Elemente «Ultimate Debtor» und «Ultimate Creditor» – endgültiger oder «eigentlicher» Zahlungspflichtiger oder Zahlungsempfänger.

Dies ist allerdings nur möglich, wenn die Senderbank auf MX umgestellt hat. Dafür haben die Banken weltweit bis 2025 Zeit, sodass es in dieser Migrationsphase für Kundinnen und Kunden unabdingbar ist, sich bei ihrer Hausbank zu erkundigen, ob der Ultimate Debtor oder der Ultimate Creditor beziehungsweise die anderen neuen Möglichkeiten der MX-Meldungen bereits genutzt werden können. Dies kann sich unter Umständen auch nach Währungen oder Zahlwegen unterscheiden. Denn um eine End-to-End-Weitergaben der Daten sicherzustellen, muss nicht nur die Senderbank auf MX umgestellt haben, sondern auch die Empfängerbank und allenfalls die intermediären Institute müssen dies getan haben. SWIFT sieht diesbezüglich über die Zeit einige Hilfestellungen in ihrem Netzwerk vor. Die international gestaffelte Umstellung über die kommenden drei Jahre mit mehreren Tausend SWIFT-Teilnehmern ist also komplex. Aufgrund dieser gestaffelten Umstellung empfiehlt die Payments Market Practice Group (PMPG), die neuen Elemente wie den Ultimate Debtor oder den Ultimate Creditor erst ab November 2023 zu nutzen. Im Gegensatz dazu fällt es der Schweizer Interbank-Community mit rund 320 Teilnehmerinstituten leichter, die neue Meldungsversion beziehungsweise allfällige neue Regeln einzuführen. So unterstützen SIC und euroSIC bereits ab November 2022 die neuen Elemente, sowohl für Inlandzahlungen als auch für Weiterleitungen von grenzüberschreitenden Zahlungsaufträgen. Hierzulande ist es zudem nicht entscheidend, ob in der Kunde-Bank-Schnittstelle bereits die neuen Meldungsversionen gemäss Swiss Payment Standards (SPS) 2022 oder noch jene von SPS 2021 verwendet werden. Denn die aktuellen Meldungen nach SPS 2021 lassen bereits die Verwendung der strukturierten Adressen zu. Auch wenn diese weniger Adresselemente ermöglichen, sind die meisten Anwendungsfälle völlig ausreichend abgedeckt. Denn die neuen Meldungsversionen haben nicht andere, sondern nur zusätzliche Elemente, die vor allem anderweitige Adressierungssysteme betreffen. Im Umkehrschluss bedeutet dies, dass sich auch mit der heutigen SPS-Version ein Ultimate Debtor beziehungsweise ein Ultimate Creditor mit strukturierten Adressen versehen lässt, wenn diese Aufträge als grenzüberschreitende Zahlungen via SWIFT-Netzwerk mit MX-Meldungen weitergereicht werden sollen. Ab 2025 sollte alles viel einfacher und klarer sein, wenn die allgemeine Nutzung der strukturierten Adressen weltweit verpflichtend wird.

MARTIN WALDER,
HEAD BILLING & PAYMENTS STANDARDS, SIX

SEPA übernimmt strukturierte Adressen
Mit dem neuen Rulebook SEPA 2023 werden auch die strukturierten Adressen im SEPA-Raum optional eingeführt. Dies ermöglicht eine einheitliche Verarbeitung, unabhängig davon, ob die Zahlungen über SIC, euroSIC, einem SEPA-Anbieter oder über SWIFT geleitet werden. Darüber hinaus ist auf den übernächsten Wechsel im Jahr 2025 ebenfalls die verpflichtende Nutzung der strukturierten Adressen vorgesehen. Die genauen Regeln werden im Rahmen von SPS 2023 im Februar 2023 veröffentlicht.

Strukturierte Daten

```
<Dbtr>
   <Nm>JOHN SMITH[1]</Nm>
   <PstlAdr>
     <StrtNm>HOOGSTRAAT[2]</StrtNm>
     <BldgNb>6[3]</BldgNb>
     <BldgNm>PREMIUM TOWER[4]</BldNm>
     <PstlCd>1000[6]</PstlCd>
     <TwnNm>BRUSSELS[7]</TwnNm>
     <Ctry>BE[8]</Ctry>
   </PstlAdr>
   <ID>
     <OrgId>
         <LEI>HB7FFAZI00MZ8PP80E26[5]
         </LEI>
     <OrgID>
   </ID>
</Dbtr>
```

[1] Name
[2] Street Name
[3] Building Number
[4] Building Name
[5] LEI (Legal Entity Identifier)
[6] Postal Code
[7] Town Name
[8] ISO Country Code

Abbildung 1: Beispiel einer strukturierten Adresse in pacs.008

ISO-20022-Multibanking dank dem «Relay»-Szenario von SWIFT

Benötigtes Wissen
— Fundierte Kenntnisse der pain-Meldungstypen

Obwohl Kunde-Bank-Meldungen von der ISO-20022-Migration bei SWIFT grundsätzlich ausgeklammert sind, gibt es eine Ausnahme: beim sogenannten «Relay»-Szenario. Dieses tritt ein, wenn ein Finanzinstitut seinen Firmenkunden eine Kontenkonzentration anbietet, auch Multibanking genannt. Dabei kann der Firmenkunde mit nur einer technischen Bankanbindung andere Banken weltweit instruieren und Kontoauszüge empfangen. Ohne Multibanking muss ein Unternehmen mit beispielsweise fünf Bankbeziehungen auch fünf technische Anbindungen zu den Banken unterhalten. Mit Multibanking (Abbildung 2) braucht es nur noch eine einzige Bankanbindung, was dem Kunden Zeit und Geld spart.

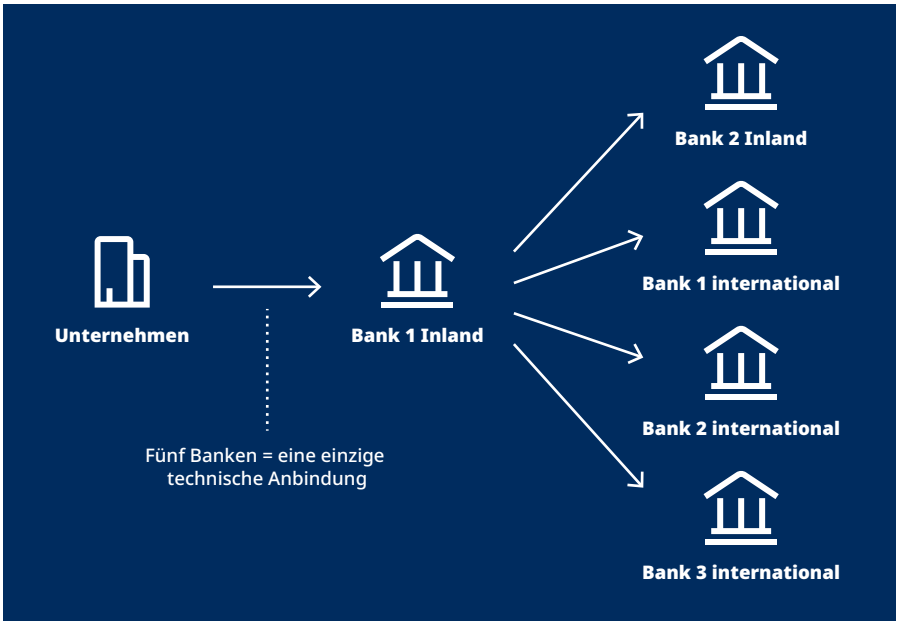


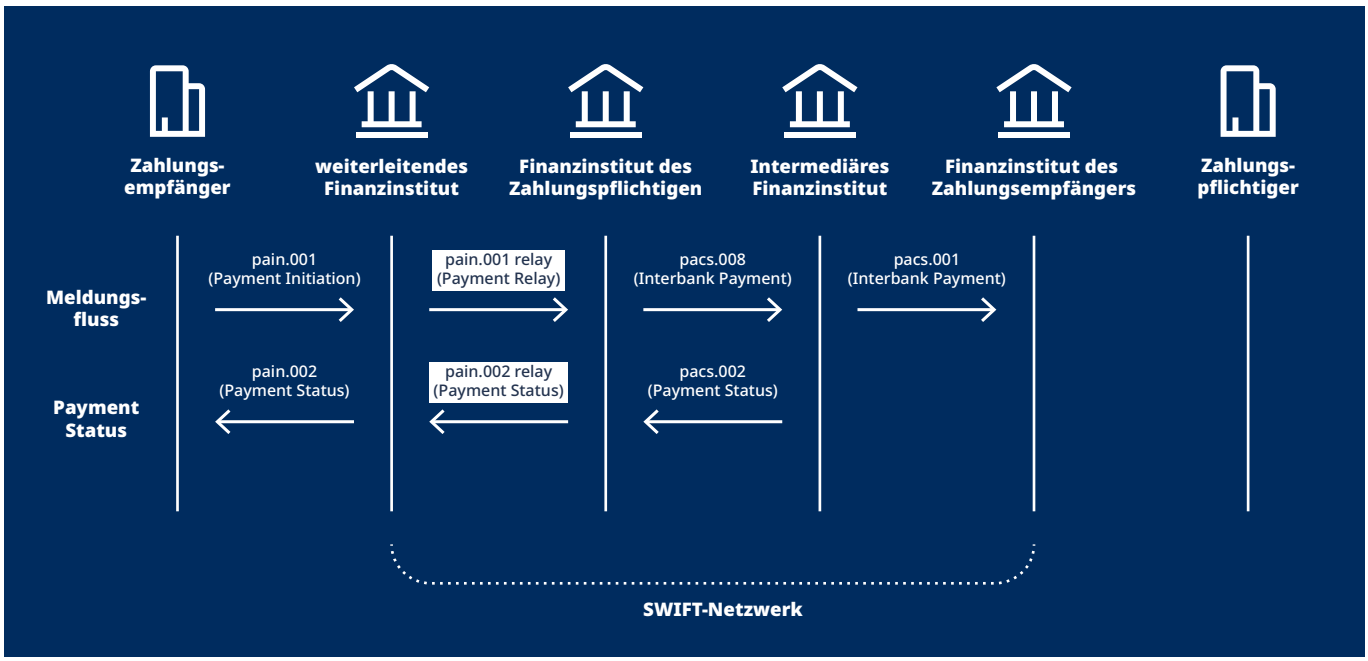
Abbildung 2: Bankaufträge mit Multibanking-Kontoservice

Zeitersparnis und Effizienzgewinn

Multibanking eignet sich für alle Unternehmen mit mehreren Kontoverbindungen. In der Schweiz beispielsweise verfügen 70 Prozent der KMU über mehr als eine Bankbeziehung. Dank Multibanking können Konten von Drittbanken im Inland und dank dem Relay-Szenario von SWIFT auch weltweit über eine einzige Bankanbindung bewirtschaftet werden. So lassen sich einerseits Zahlungen zulasten eines Drittbankkontos im Ausland zugunsten von Lieferanten vor Ort über eine einzige Bankverbindung tätigen. Andererseits erhalten Kundinnen und Kunden damit dank elektronischer Kontoauszüge volle Transparenz über alle Konten, auch über jene bei Drittbanken. Die Zeitersparnis und der Effizienzgewinn steigen dadurch beträchtlich.

Die Promotoren

Die Arbeitsgruppe Cross-Border Payments and Reporting Plus (CBPR+) hat die Nutzungsrichtlinien für das Relay-Szenario in enger Zusammenarbeit mit der Arbeitsgruppe Common Global Im-



plementation (CGI) entwickelt. Sie decken die Interbank-Szenarien «Payment Initiation» (pain.001) und «Payment Status Report» (pain.002) ab.

CGI, in der sowohl die Finanz- (Banken) als auch die Unternehmenswelt vertreten ist, wird von SWIFT unterstützt, um die Einführung der ISO-20022-Standards für Finanznachrichten zu fördern und die Umsetzung auf diese ISO-20022-Meldungen zu vereinfachen.

Die zwei ISO-20022-Meldungen im Relay-Szenario

Payment Initiation

In diesem Relay-Szenario sendet die initiierende Partei die Interbank-Meldung «Customer Credit Transfer Initiation» (pain.001) an das weiterleitende Finanzinstitut oder das Finanzinstitut des Schuldners, um die Bewegung von Geldern vom Debitorenkonto zu einem Gläubiger zu verlangen. Das weiterleitende Institut fungiert dabei als konzentrierendes Finanzinstitut, das die pain.001-Meldung an das Finanzinstitut des Schuldners weiterleitet (siehe Meldungsfluss in Abbildung 3).

Payment Status Report

In diesem Relay-Szenario sendet das beauftragte Finanzinstitut die Interbank-Meldung «Customer Payment Status Report» (pain.002) an die vorherige Partei in der Zahlungskette, um diese über den positiven oder negativen Status einer Anweisung zu informieren. Die pain.002-Meldung dient auch dazu, über einen ausstehenden Überweisungsauftrag dem Zahlungsempfänger Bescheid zu geben (siehe Payment Status in Abbildung 3).

Der SWIFT-Fahrplan

Im November 2022 beginnen für die Finanzinstitute die Migration auf ISO 20022 (MX) für grenzüberschreitende Zahlungen und die Berichterstattung mit einer Parallelphase mit MT-Meldungen bis November 2025. Dieser Fahrplan ist auch für das Relay-Szenario wegweisend. Banken, die Multibanking unterstützen, müssen also bis spätestens 2025 auf das ISO-20022-Relay-Szenario umgestellt haben.

PETER RUOSS,
PRODUCT OWNER PAYMENT SOFTWARE PARTNERSHIPS, UBS SWITZERLAND AG

Durch das Dickicht der digitalen Zertifikate

Benötigtes Wissen
— Grundlegende Kenntnisse von Verschlüsselungsverfahren

Digitale Zertifikate sind nicht mehr wegzudenken. Ihre Ausprägungen TLS, HTTPS, CA, ECC und RSA klingen nicht nur «kryptisch», sie sind es auch – nach der ursprünglichen Bedeutung des Worts «verborgen». Verborgen und allgegenwärtig hinter den Internetverbindungen, die sie durch Verschlüsselung der Daten absichern. So können unbefugte Dritte den Datenverkehr zwischen dem Browser, der besuchten Website und dem Website-Server weder mitlesen noch manipulieren.

Ein digitales Zertifikat – auch Public-Key-Zertifikat oder Identitätszertifikat genannt – ist nichts anderes als ein kryprografischer Schlüssel. Von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt, bezeugt das Zertifikat die Echtheit der Anmeldedaten einer Person im Internet und ihre Identität. Es ist quasi ein Sicherheitsbadge, das sowohl der Daten eingebenden als auch der Daten empfangenden Person versichert, dass die Daten an eine vertrauenswürdige Quelle übermittelt werden.

Transport Layer Security (TLS)

TLS ist der Nachfolger des inzwischen veralteten Secure-Sockets-Layer(SSL)-Protokolls. In der Praxis dient es in Form von digitalen Zertifikaten als Standardmethode zur Sicherung der Maschine-zu-Maschine-Kommunikation.

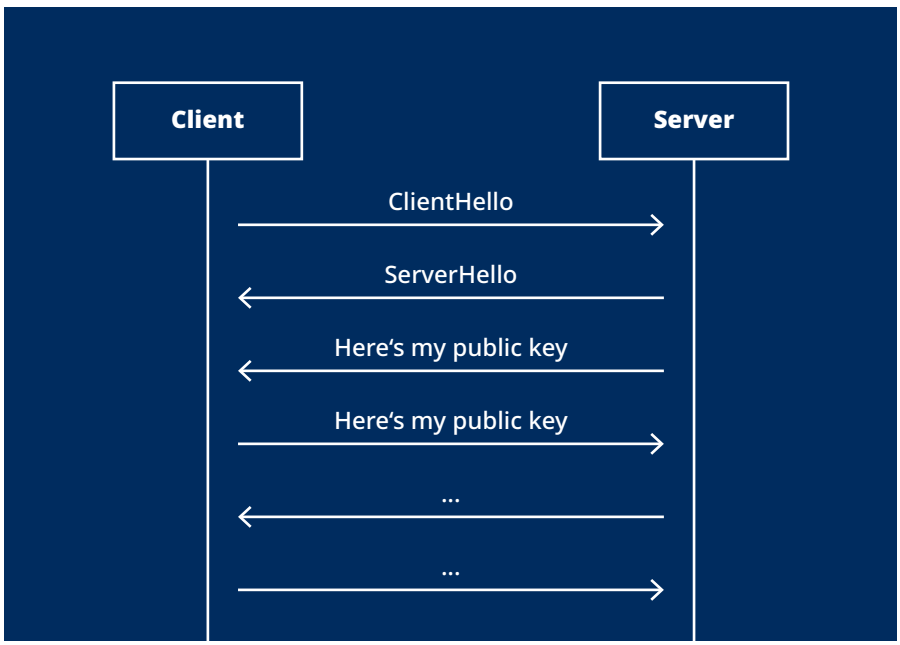
Am häufigsten kommen TLS-Zertifikate bei Websites zum Einsatz. Nur sie können dafür sorgen, dass eine Website als HTTPS (mit einem Schlosssymbol in der Adressleiste gekennzeichnet) verschlüsselt wird und die Daten zwischen Websites, Browsern und Webservern sicher übermittelt werden können, ohne dass sie abgefangen oder geändert werden. Dadurch lässt sich die Identität eines Website-Betreibers authentifizieren.

Wie das TLS-Zertifikat funktioniert

Das TLS-Zertifikat baut eine verschlüsselte Verbindung zwischen einer Website beziehungsweise einem Server und einem Browser auf, ohne dass die Person, die die Website besucht, etwas davon merkt.

Zuerst erfolgt die Authentisierung. Bei jeder neuen Sitzung, die die Person startet, tauschen deren Browser und der Server des Website-Betreibers ihre TLS-Zertifikate aus und validieren diese

Abbildung 4: der iterative Analytics-Prozess



gegenseitig. Sodann findet der Schlüsselaustausch statt.

Dabei teilt der Server seinen öffentlichen Schlüssel mit dem Browser, den der Browser dann zur Erstellung eines Passepartout-Schlüssels (pre-master key) verwendet. Schliesslich entschlüsselt der Server diesen Passepartout mit seinem privaten Schlüssel und baut eine sichere, verschlüsselte Verbindung für die Dauer der Sitzung auf.

Die drei Kryptografietypen

Kryptografie befasst sich im Allgemeinen mit dem Thema Informationssicherheit und im Speziellen mit dem Verschlüsseln und dem Entschlüsseln von Informationen. Dabei kommt ein Algorithmus zum Einsatz, der den Klartext verschlüsselt und so unlesbar macht. Er wird für die Datenverschlüsselung, die Authentifizierung und digitale Signaturen verwendet.

Die symmetrische Verschlüsselung fällt in die erste kryptografische Kategorie. Hier teilen sich Sender und Empfänger einen einzigen Schlüssel, wobei Ersterer den Klartext damit verschlüsselt und ihn so dem Empfänger übermittelt. Dieser nutzt dann denselben Schlüssel, um den verschlüsselten Text zu entschlüsseln beziehungsweise den Klartext des Senders wiederherzustellen.

Die zweite Kategorie umfasst die Public-Key- oder die asymmetrische Verschlüsselung. Hierbei gibt es zwei miteinander verbundene Schlüssel: den öffentlichen und den privaten. Während der öffentliche Schlüssel frei verteilt werden kann, muss der entsprechende private Schlüssel geheim bleiben. Der öffentliche Schlüssel dient zur Verschlüsselung der Daten, die eine Person senden möchte. Der private Schlüssel zur Entschlüsselung der Daten wird in der Regel vom Ersteller des Schlüsselpaars aufbewahrt. Die meistverwendeten Algorithmen hier sind RSA (Rivest-Shamir-Adleman) und ECC (Elliptic Curve Cryptography), wobei TLS-Zertifikate häufig RSA einsetzen. Die empfohlene Grösse dieser Schlüssel nimmt ständig zu (z. B. von 1024 auf 2048 Bit), damit sie hochwirksam bleiben. ECC ist kryptografisch genauso wirksam wie RSA. Ihre Schlüsselgrösse ist jedoch erheblich kleiner, was einerseits den Rechen- und Speicheraufwand reduziert und andererseits eine höhere Geschwindigkeit und Sicherheit bewirkt. Der Nachteil besteht darin, dass nicht alle ECC-basierten Anwendungen mit TLS-Zertifikaten interoperabel sind.

Die Hash-Funktion stellt die dritte kryptografische Kategorie dar. Dieser Algorithmus verwendet keinen Schlüssel, sondern komprimiert den Klartext numerisch anhand fester Längen, sodass der Klartextinhalt nicht mehr wiederhergestellt werden kann. Hash-Funktionen werden häufig von Computersystemen verwendet, um Passwörter zu verschlüsseln.

Wozu dient die digitale Signatur?

Eine digitale Signatur, von sogenannten Trust Service Providers wie beispielsweise SwissSign ausgestellt, ist ein Unterschriftenzertifikat, das kryptografisch durch eine Public-Key-Infrastruktur (PKI) an ein Dokument gebunden ist. Digitale Signaturen validieren und authentisieren die Identität der unterzeichnenden Person und die Integrität des Dokuments. Sie bieten so eine hohe Sicherheit dafür, dass die oder der Unterzeichnende tatsächlich das Dokument verfasst hat. Darüber hinaus gewährleisten sie, dass keine Änderungen am Dokument erfolgt sind. Digitale Signaturen eignen sich mitunter als Zugangssicherung auf vertrauliche Datenbestände oder im E-Government-Umfeld, wie beispielsweise fürs Beantragen von Pässen via Internet.

PETER RUOSS,
PRODUCT OWNER PAYMENT SOFTWARE PARTNERSHIPS, UBS SWITZERLAND AG

Phygital Banking am Beispiel von Zahlkarten

Die physische und die digitale Welt verschmelzen immer stärker miteinander. Kombiniert können sie zu neuen, spannenden Kundenerlebnissen führen. Physische Vorgänge digitalisieren, die virtuelle Welt um physische Services ergänzen – das ist die Quintessenz von «phygital».

Privatpersonen erwarten heute personalisierte, bequeme und sichere Bezahloptionen, die sich gut in ihr physisches und digitales Leben integrieren lassen. Klassische Bargeldschalter verwandeln sich in digitale Selbstbedienungsbereiche, die gleichzeitig eine persönliche Beratung ermöglichen.

Bezahlkarten sind ein gutes Beispiel für Phygital Banking. Nach der Kontoeröffnung ist die Ausgabe einer Karte die nächste wichtige Interaktion zwischen Bank und Kundschaft. Zur Überbrückung der Zeit bis zum Eintreffen der physischen Karte bietet die Bank eine sofort verfügbare virtuelle Karte an, die es den Kundinnen und Kunden ermöglicht, online einzukaufen. Sodann versendet die Bank Updates zur physischen Karte (z.B. über den Postzustellstatus), die die Kundinnen und Kunden jederzeit über das Mobiltelefon einsehen können. Physische Karten können in einer mobilen App gesichert und dann mit digitalen Tools für CO_2-Tracking und -Kompensation kombiniert werden.

Markenerlebnis

Phygital kann auch der physische Trägerbrief der Karte sein: individualisiert mit Inhalten und QR-Codes, die das Eintreffen einer neuen Karte zum Markenerlebnis für die Kundinnen und Kunden machen. Und die Karte selbst: personalisiert mit Bildern, die von den Kundinnen und Kunden ausgewählt wurden. Oder sie wird durch Kioske bereitgestellt, die eine Karteninhaberin bzw. einen Karteninhaber authentifizieren und innerhalb von Minuten eine neue Karte ausgeben können. Mobile Apps können darüber hinaus die Aktivierung der Karte unterstützen, ohne dass man eine Filiale aufsuchen muss.

Was das für Banken und Finanzdienstleister bedeutet und welche enormen Innovationschancen darin liegen, hat kürzlich der Technologiekonzern Giesecke+Devrient in seiner Studie «Chancen in der phygitalen Landschaft» untersucht. Die Umfrage bei Finanzdienstleistern in 15 Ländern zeigt, wie relevant physische Zahlkarten als wichtiges Bindeglied zwischen Bank und Kundschaft bleiben werden. Karten fungieren als einzigartiges Markenelement und dienen als physischer Anker für digitale Dienstleistungen. Phygitale Angebote unterstützen die Banken – angesichts innovativer Benutzererfahrungen bei Neobanken und Big-Techs – dabei, relevant zu bleiben.

GABRIELLE BUGAT,
MITGLIED DER GESCHÄFTSFÜHRUNG BEI GIESECKE+DEVRIENT UND VERANTWORTLICH FÜR DEN BEREICH CARD & DIGITAL PAYMENT

WEITERFÜHRENDE INFORMATIONEN

SWIFT Go: Ein neuer internationaler Standard für Kleinbetragszahlungen

Geld in die ganze Welt zu verschicken, sollte einfach sein. Einfach für Kleinunternehmen, die im Ausland einkaufen. Und einfach für Familien, die Geld an ihre Lieben im Ausland senden möchten.

Die Einführung von SWIFT gpi hat den grenzüberschreitenden Grossbetragszahlungsverkehr für immer verändert – er wurde schneller, transparenter und nachverfolgbar. Nach dieser positiven Erfahrung macht SWIFT heute dasselbe auch für Kleinbetragszahlungen möglich.

Denn der Markt für Kleinbetragszahlungen wächst rasant: McKinsey prognostiziert ein Marktwachstum von 10 Prozent zwischen 2018 und 2023. Vor diesem Hintergrund legt SWIFT den Grundstein für eine intelligentere Lösung und stellt den Banken jene Mittel zu Verfügung, die sie benötigen, um ihre Angebote für Kleinbetragszahlungen zu transformieren.

Der Markt wächst weiter und damit auch die Kundenerwartungen. Da die Dienstleistungen im täglichen Leben immer schneller und intuitiver werden, erwartet die Kundschaft dasselbe auch in komplexeren Bereichen – wie etwa im Zahlungsverkehr. Finanzinstitute müssen innovativ sein, um mit diesen Erwartungen Schritt zu halten.

Auf solidem Fundament

Die Idee hinter SWIFT Go ist einfach: Banken sollen ihrer Kundschaft einen schnellen, einfachen und nachverfolgbaren Weg bieten, direkt von ihren Bankkonten aus Geld in die ganze Welt zu senden. Die Service Level Agreements von SWIFT bilden das Herzstück dieser Lösung und ermöglichen genau das.

Wenn sich eine Bank für SWIFT Go entscheidet, klärt sie mit ihren Gegenparteien alle Gebühren. Dadurch wird sichergestellt, dass die Preise für Zahlungen wettbewerbsfähig sind und die Kundinnen und Kunden vor Auslösung der Transaktion wissen, wie viel ihre Überweisung kostet. Die Lösung verwendet MT103-Meldungen und ist auch für die überweisenden Banken transparent: Sie können Informationen zur Zahlungsverfolgung in ihr Frontend integrieren, um die Vorhersehbarkeit zu erhöhen.

Die Banken verpflichten sich ausserdem, Zahlungen innerhalb von maximum vier Stunden zu bearbeiten und keine zusätzlichen Abzüge vorzunehmen. Dies sorgt für einen schnellen Geldfluss und gibt den Privatpersonen die Gewissheit, dass ihre Zahlungen pünktlich am Ziel ankommen.

SWIFT-Go-Zahlungen laufen über dieselbe Infrastruktur und dasselbe Netzwerk wie SWIFT gpi. Das bedeutet, dass Banken und ihre Kundschaft auf dieselbe Sicherheit und Serviceverfügbarkeit zählen können.

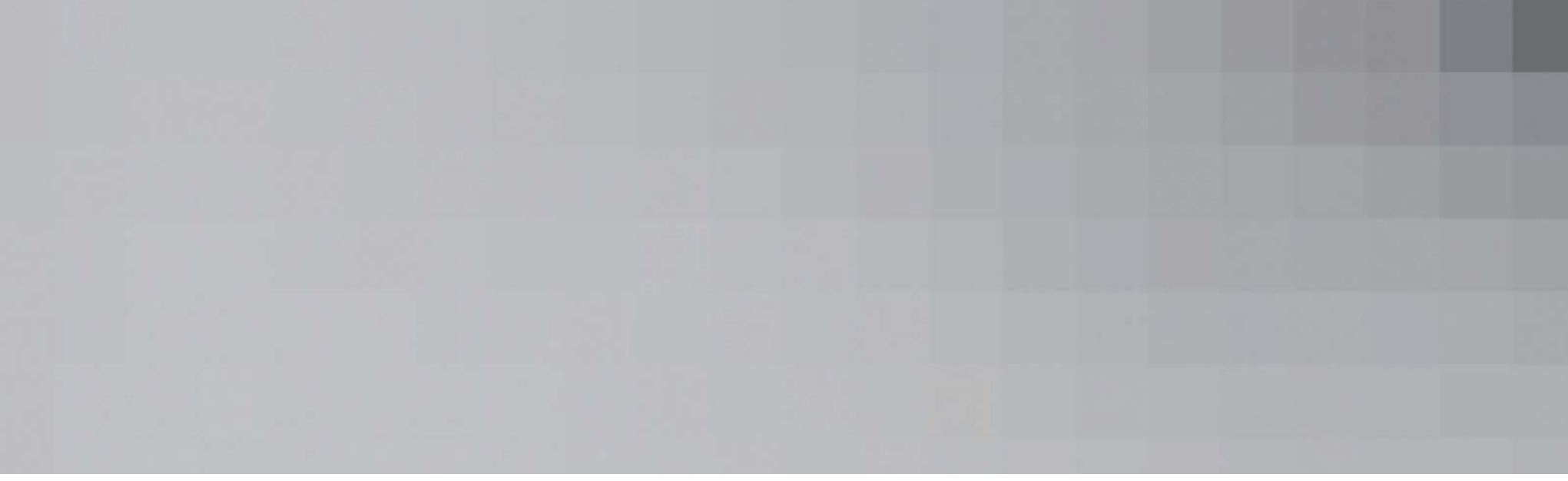
Eine schnell wachsende Gemeinschaft

SWIFT ermöglicht sofortige und reibungslose Transaktionen über ihr Netzwerk aus mehr als 11 000 Instituten, die vier Milliarden Konten in über 200 Ländern miteinander verbinden. SWIFT Go spielt dabei eine entscheidende Rolle, denn es ermöglicht eine stärkere finanzielle Inklusion von KMU und Konsumentinnen und Konsumenten in Entwicklungs- und Schwellenländern.

Mehrere grosse Korrespondenzbanken in wichtigen globalen Handelspartnerländern der Schweiz haben sich bereits für den Service angemeldet, darunter solche aus Grossbritannien, den USA, China, den Vereinigten Arabischen Emiraten und aus Indien. Insgesamt sind es über 250 Banken aus 90 Ländern.

ROGER INDERBITZIN, LEITER VON SWIFT SCHWEIZ & LIECHTENSTEIN

WEITERFÜHRENDE INFORMATIONEN



Alles hat seinen Preis,
alles hat einen Wert.

Warren Buffett (1930)