pay

Le magazine de SIX, spécialisé en trafic des paiements — #6 — 2022

Comment la place financière agit de manière offensive contre les cybercriminels — «Future Talk» avec Hannes Lubich — Hackers et crackers — De la petite monnaie à la caisse — Le multibanking grâce à «Relay»

EN VISITE CHEZ

Voiture, médecine et cyber

10

HEARTBEAT

Une analyse des montants des cartes en Suisse et à l'étranger

08

FUTURE TALK

Hannes Lubich s'explique sur les chances face à la cybermenace

07

EXPERTS ONLY

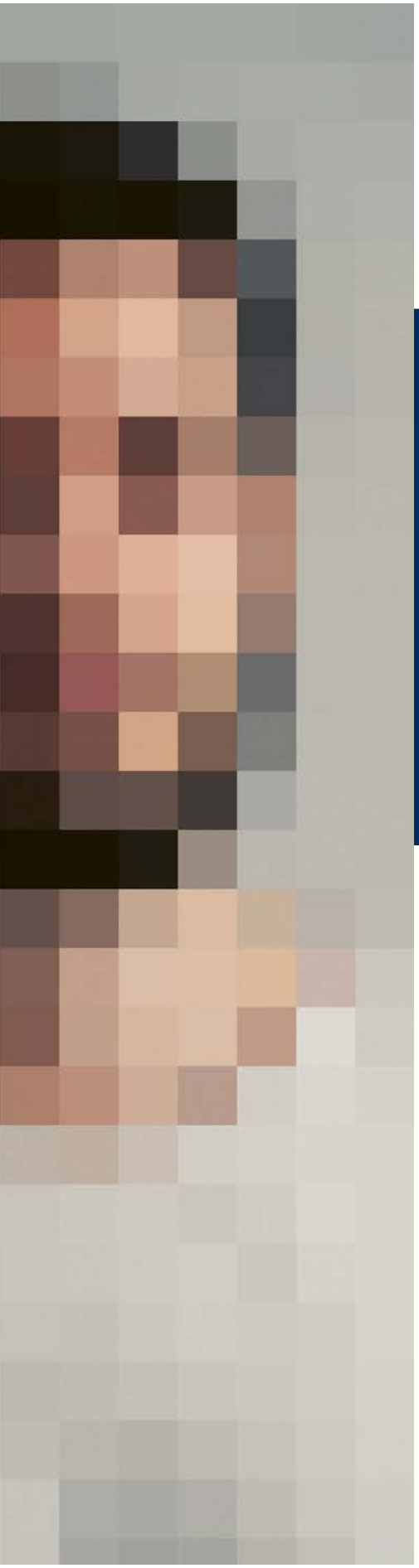
À nous les adresses structurées

14

SECTIONS

Éditrice SIX Group SA, case postale, 8021 Zurich, Suisse, six-group.com/pay, pay@six-group.com Conseil Daniel Berger, SIX; Boris Brunner, direction, SIX; Angelika Christian, SECB; Laura Felber, BNS; Pierre-Michel Gicot, BCV; Susanne Höhener, Liechtensteinischer Bankenverband; Daniela Hux-Brauss, Credit Suisse (Suisse) SA; Raphael Reinke, BNS; Peter Ruoss, UBS Switzerland AG; Stefan Schneider, PostFinance; Nino Thommen, SIX Rédaction Gabriel Juri, direction, SIX Mise en page *MADE* Identity AG, Zurich, Suisse Lithographie Marjeta Morinc Impression sprüngli druck ag, Villmergen, Suisse Traductions Mark Rabinowitz, Translation Service Team, SIX (anglais); Denis Fournier (français) Crédits photo Jessica Radanavong (Cover), Vova Krasilnikov (p. 3), Arthur Hidden (p. 4), Jassir Jonis (p. 6), Ornella Cacace (p. 2, 10), Tobias Siebrecht (p. 13) Illustrationen Gregory Gilbert-Lodge (p. 2, 7, 12)

La police suisse a enregistré plus de 30 000 cyberdélits en 2021, soit environ un quart de plus qu'un an auparavant.



Cyberdéfense: la Suisse se met à niveau

TEXTE
THOMAS KOCH
HEAD CORPORATE SECURITY, SIX

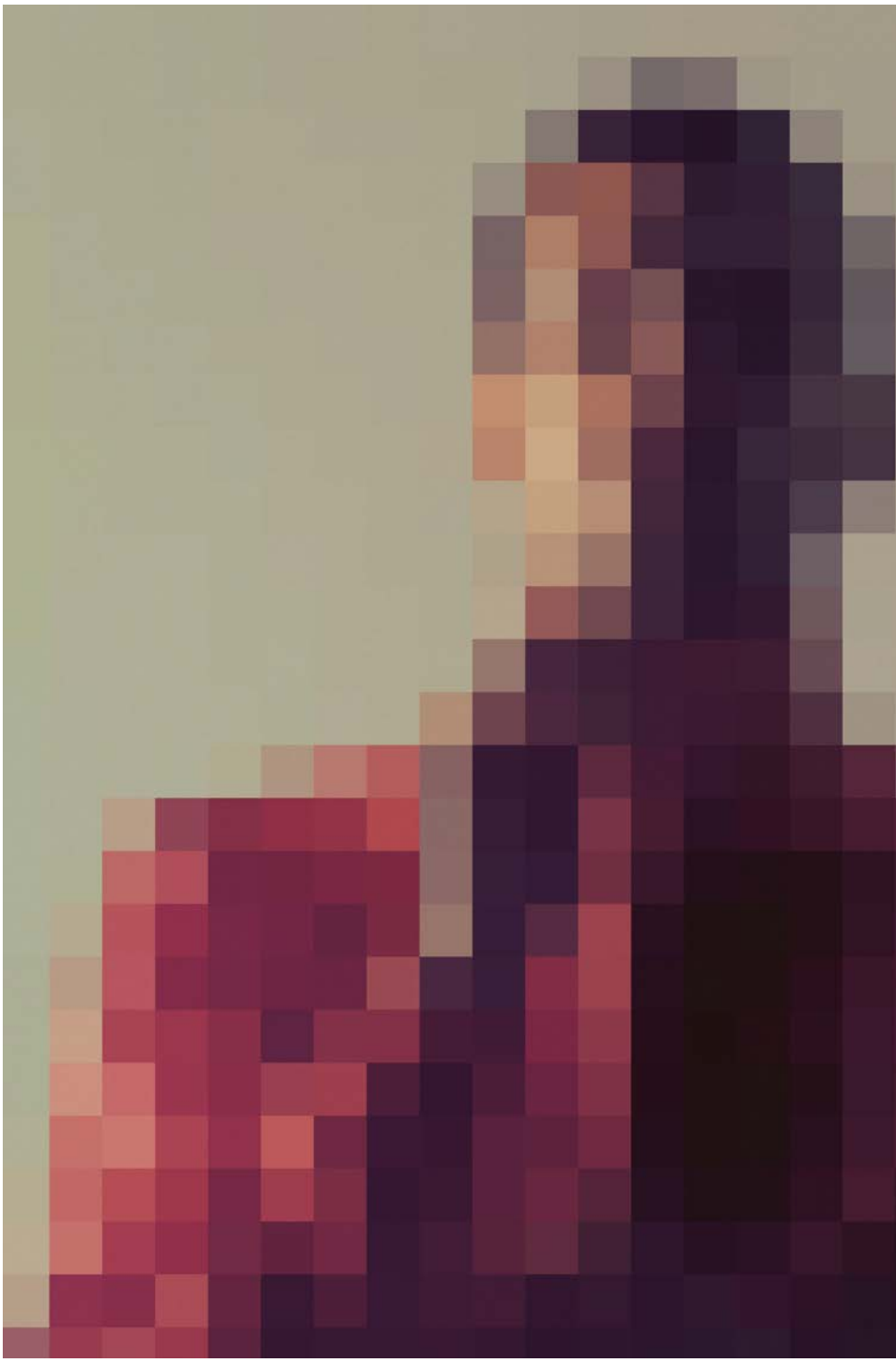
L'occasion fait le larron, aujourd'hui comme toujours dans l'histoire humaine. Tout ce qui n'est pas solidement fixé est «emprunté». Dans les foires du Moyen Âge, le voleur subtilisait du pain, de la volaille, des jambons, des bougies et de l'argent – et dérobait même ce dernier dans les troncs des églises. Aujourd'hui, les lieux du délit sont par exemple les centres commerciaux. Ou les musées, dont les peintures, les pierres précieuses ou les dents de Néandertal disparaissent mystérieusement. Ou les ordinateurs, dont les données deviennent la proie des voleurs. Souvent, le vol et le chantage vont de pair. Dans le cas du butin provenant d'un musée, on parle d'«artnapping» quand l'auteur menace de détruire l'objet volé si aucune rançon n'est payée. Pour un butin numérique, on parle de «rançon». Ici comme là, les criminels sont en grande partie non violents. En outre, le nombre de cas non déclarés est élevé dans tous les domaines précités et les parties lésées s'efforcent par la suite d'améliorer la surveillance et la sécurité technique de leurs «trésors».

Les attaques de ransomware contre les entreprises ne sont pas nouvelles, mais connaissent récemment une croissance exponentielle. Les statistiques policières sur la criminalité révèlent cependant depuis des années une baisse importante des délits de vol non numérique. Il reste à savoir s'il n'y a qu'une corrélation aléatoire ou une causalité derrière cela. Le fait est que la numérisation et la mise en réseau croissantes ont un impact énorme sur la sécurité de l'information et augmentent également les risques pour le secteur financier. En même temps, les cybercriminels sont de plus en plus sophistiqués et disposent de ressources financières importantes auxquelles contribuent souvent des «sponsors». La dernière génération d'attaquants disposant de telles capacités comprend des groupes parrainés par le gouvernement ou par des entreprises et le crime organisé. Leurs motivations peuvent être politiques et dépasser les simples intérêts financiers. En plus des attaques avec des programmes malveillants de ransomware, deux autres méthodes de cyberchantage se distinguent: les attaques de la chaîne d'approvisionnement ciblant des tiers vulnérables ayant accès à des systèmes critiques, et les attaques par déni de service distribué (DDoS) visant à interrompre un service ou à restreindre l'accès pour un groupe cible spécifique.

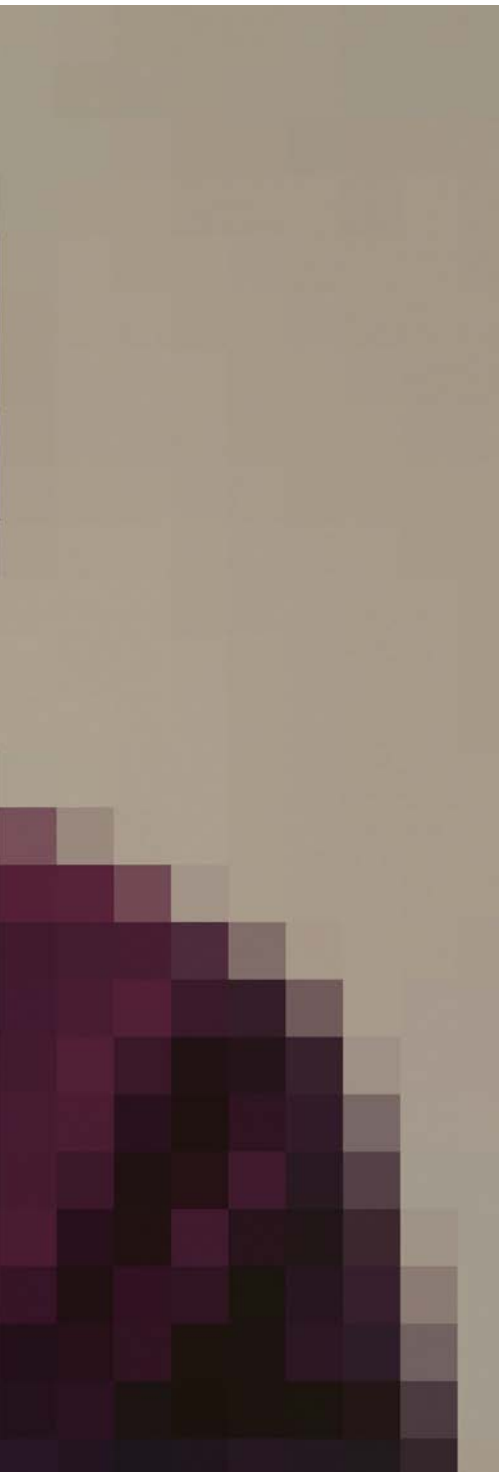
Récemment, plusieurs acteurs financiers à l'étranger ont été exposés à de telles attaques. Par exemple la Bourse de Nouvelle-Zélande, où un DDoS a suspendu

«Plus la vulnérabilité est critique, plus un hacker éthique est récompensé.»

Renforcer la sécurité dans le système SIC: sécurité des points de terminaison et SSFN L'impact de paiements frauduleux dans les systèmes de paiement de montants élevés tels que le système SIC peut être considérable, non seulement pour les participants directement touchés, mais aussi pour le système de paiement dans son ensemble. L'envoi de paiements frauduleux résultant d'une compromission de points de terminaison des participants SIC, c'est-à-dire des appareils, applications ou systèmes requis par un participant SIC pour l'échange de messages avec le système SIC, est particulièrement problématique. Afin d'accroître la protection des points de terminaison de tous les participants SIC, la Banque nationale suisse adoptera prochainement un cadre contraignant pour eux. Il contiendra des exigences opérationnelles et techniques pour la protection des points de terminaison, qui doivent être mises en œuvre d'ici fin 2024 soit par les participants SIC, soit par les prestataires de services qu'ils ont mandatés. Au niveau du système, l'utilisation systématique du Secure Swiss Finance Network (SSFN) indépendant de l'Internet dans la communication avec le système SIC contribuera également à renforcer la résilience et la fiabilité dans ce même système. Depuis début juin, les participants SIC peuvent utiliser le SSFN comme chemin d'accès supplémentaire au système SIC, en plus de Finance IPNet et SWIFTNet.



La cybercriminalité économique (phishing, hacking, malware, DDoS) a représenté en 2021 près de 88 % de toute la criminalité numérique en Suisse.



ses opérations pendant deux jours. Chez American Bank Systems, l'attaque par ransomware a entraîné non seulement une réclamation de rançon de 14 millions de dollars US, mais aussi une action en justice collective.

Nouvelle organisation pour la cyberrésilience du secteur financier suisse

Par rapport aux pays voisins, la Suisse semble moins fortement exposée à la cybercriminalité. Selon une étude d'un éditeur britannique de logiciels de sécurité, 0,7 % des entreprises suisses ont été touchées par un ransomware chaque semaine l'année dernière. Le taux correspondant était de 1,4 en Autriche, de 1,6 en Allemagne, de 1,8 en France et de 1,9 en Italie.

En Suisse, le Centre national de cybersécurité (NCSC) est le premier point de contact pour l'économie, l'administration, les établissements d'enseignement et la population sur les cyberquestions. En outre, il aide en particulier les exploitants d'infrastructures critiques à se protéger contre les cyberrisques. L'association «Swiss Financial Sector Cyber Security Centre» (Swiss FS-CSC) a par ailleurs été créée sous sa direction en avril 2022. Elle vise à promouvoir la coopération institutionnelle entre les établissements financiers et les autorités sur les questions stratégiques et opérationnelles liées à la cybersécurité. Elle vise en particulier à faciliter l'échange d'informations entre les acteurs des marchés financiers et à améliorer la coopération en matière de mesures préventives à l'échelle sectorielle et de gestion des situations de crise systémiques.

Ces crises sont d'une importance systémique lorsqu'elles affectent les systèmes de paiement et de règlement d'opérations sur titres. SIX, en tant qu'opérateur de ces infrastructures de marché financier suisse, a naturellement un très grand intérêt pour cette coopération et s'engage comme membre fondateur. L'association compte actuellement plus de 100 banques locales, compagnies d'assurance et associations financières, qui sont surveillées par l'Autorité fédérale de surveillance des marchés financiers FINMA. Cette dernière participe également en tant qu'«affiliate». Les piliers organisationnels sont le comité de pilotage, un groupe d'experts et la Cellule de cybersécurité opérationnelle (OCS). Le comité de pilotage coordonne les mesures de gestion de crise en cas de cyberincidents systémiques et gère la communication à l'intérieur et à l'extérieur de l'association.

Le groupe interne d'experts réalise des projets visant à renforcer la cyberrésilience et organise des cyber-exercices stratégiques et opérationnels pour ses membres.

Enfin, l'OCS suit la situation sur le marché financier, échange des informations sur les événements pertinents, établit des rapports sectoriels et soutient les membres de l'association dans la gestion de crises. Pour cette mission, il est prévu qu'elle coopère avec un prestataire disposant d'une expérience internationale dans ce domaine.

Cybersécurité offensive

SIX, qui constitue l'épine dorsale des infrastructures de marché financier d'importance systémique, joue un rôle remarquable dans la stabilité et la sécurité de la place financière suisse. Elle tient un registre des risques structuré et continuellement mis à jour, y compris des risques liés à la sécurité de l'information. Au cours des dernières années, les réponses aux menaces ont inclus des mesures techniques pour soutenir la sécurité de base, le développement de compétences et de simulations, et des mesures organisationnelles. La stratégie de sécurité de l'information mise à jour inclut également de nouvelles initiatives telles que des temps de réponse améliorés dans la gestion des vulnérabilités, une protection améliorée contre les attaques de

type ransomware et l'amélioration et l'expansion continues de son Security Operations Center (SOC).

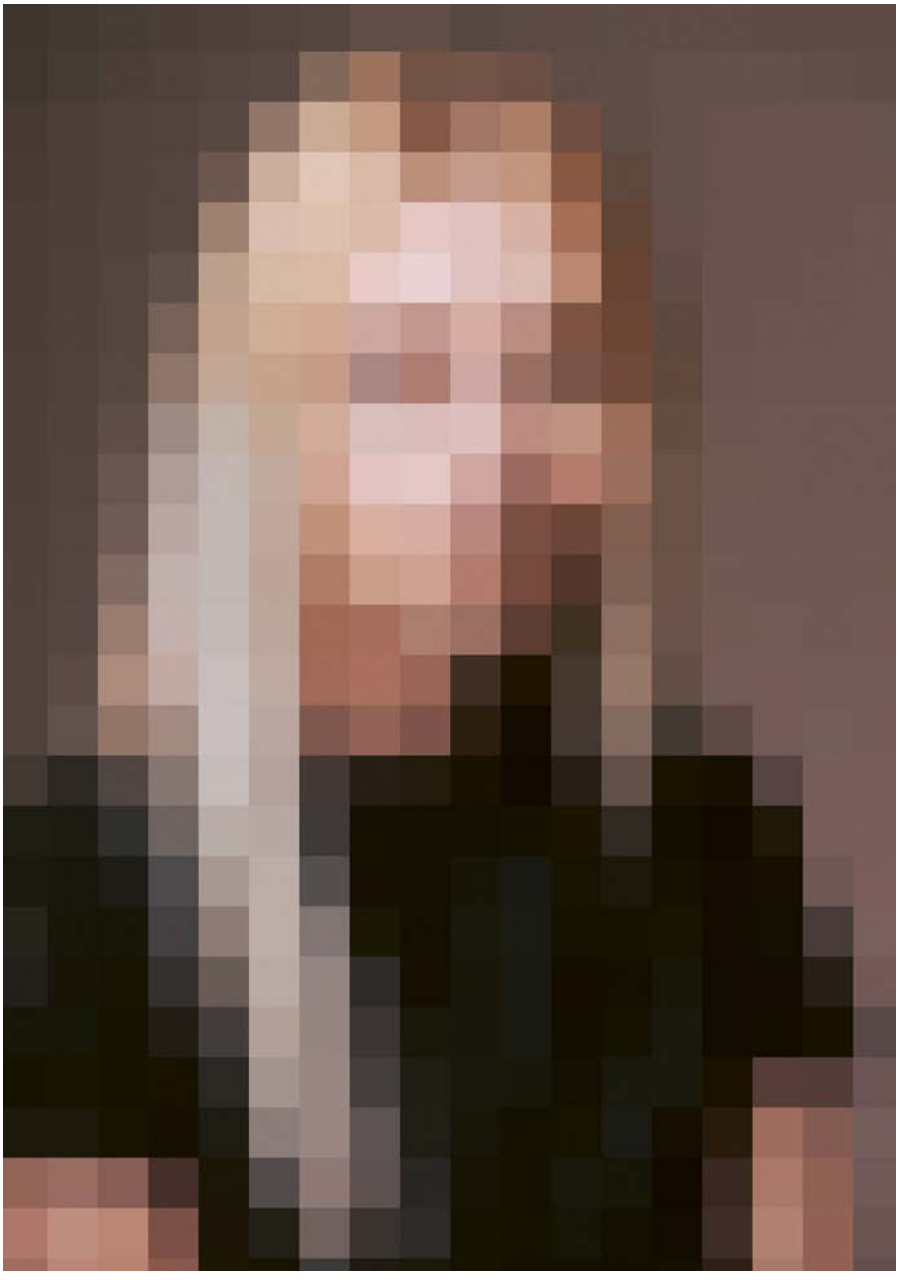
Une nouvelle équipe s'occupe désormais de ce que l'on appelle la «cybersécurité offensive». Elle adopte les scénarios, les techniques d'attaque et les méthodes de vrais hackers et les simule dans un environnement contrôlé. Il s'agit notamment de «Penetration Testing», «Adversary Emulation» et «Vulnerability Disclosure Program». Le test de pénétration (Penetration Testing) vise à pénétrer systématiquement les applications et les systèmes afin de détecter les failles de sécurité et de les communiquer aux développeurs et aux opérateurs. Les émulations d'adversaires (Adversary Emulation) sont utilisées pour tester la résilience d'un réseau contre des attaquants ou des menaces avancés avec ou sans avertissement et pour intégrer les résultats dans la formation de la cybersécurité défensive.

Le programme de divulgation des vulnérabilités (Vulnerability Disclosure Program; également connu sous le nom de programme Bug Bounty) est la dernière tendance en matière de cybersécurité offensive. Il permet d'organiser des attaques ciblées de systèmes par des hackers éthiques sélectionnés, qui sont financièrement récompensés pour leur travail. Toute personne peut, dans le monde entier, signaler proactivement en ligne à SIX un incident ou un cas suspect concernant la sécurité des informations.

Début avril 2022, SIX a élaboré un tel programme, axé initialement sur les systèmes connectés à Internet. À un stade ultérieur, les systèmes internes ou les services cloud doivent également pouvoir être piratés «de manière éthique». Le programme Bug Bounty offre de nombreux avantages. D'une part, il existe dans le monde des milliers de hackers avec des idées différentes et créatives qu'une seule équipe ne pourra jamais rassembler. D'autre part, chaque technologie a ses «spécialistes», que SIX peut sélectionner spécifiquement. De plus, ces programmes se déroulent sur une longue période pouvant atteindre plusieurs années, alors que les tests de pénétration classiques ne durent généralement que quelques semaines. La rémunération n'est pas fondée sur le temps investi, mais sur les faiblesses identifiées. Plus la vulnérabilité est critique, plus un hacker éthique est récompensé.

Que ce soit dans le cadre du Swiss FS-CSC ou d'échanges avec des hackers éthiques, la coopération aidera à réduire le risque de cyberattaques sur la place financière suisse. Dans la mesure du possible et dans les meilleurs délais, les acteurs de la place financière devraient pouvoir sécuriser leurs applications et leurs systèmes de manière à ce que les cybercriminels aient moins de chances de voler leurs biens ou ceux de tiers.

La plus forte augmentation en pourcentage dans les statistiques suisses de la cybercriminalité économique en 2021 a été enregistrée pour les composants phishing avec 88 % et ransomware avec 53 % par rapport à 2020.



«La gouvernance de la cybersécurité ne peut pas être déléguée.»

HANNES LUBICH,
PROFESSEUR D'UNIVERSITÉ ÉMÉRITE ET CONSEILLER STRATÉGIQUE EN SYSTÈMES INFORMATIQUES, RÉSEAUX ET SÉCURITÉ INFORMATIQUE.

TEXTE
GABRIEL JURI

La cybermenace semble moins grande en Suisse que dans d'autres pays. Quelle en est la cause? Nous avons longtemps été une cible attrayante pour les attaques et, en particulier dans les secteurs réglementés, nous avons mené une longue bataille défensive et tiré des enseignements. En outre, les entreprises suisses ont davantage les moyens de mettre en place des mesures de sécurité sophistiquées que les entreprises des régions économiquement faibles.

Selon les experts, les criminels auront toujours une longueur d'avance. La cybersécurité est-elle pratiquement vouée à l'échec ou les entreprises ne sont-elles tout simplement pas en phase avec leur époque? Les criminels peuvent aujourd'hui consacrer des ressources considérables à de nouvelles formes d'attaque, ainsi qu'à l'expertise et à l'infrastructure nécessaires pour arriver à leurs fins – dans certains pays avec l'approbation ou le concours des autorités étatiques. Il est donc difficile de se défendre efficacement contre des attaques ciblées requérant une utilisation importante de ressources. Cependant, les criminels aussi doivent maîtriser leurs coûts. Si une attaque devient trop coûteuse, ils passent à la cible suivante. Il est crucial pour les entreprises de rendre leur cyberprotection aussi efficace que possible, éventuellement par le biais d'une expertise externe.

À qui l'intelligence artificielle (IA) profite-t-elle le plus? Aux Chief Information Security Officers ou aux cybercriminels? Pour le moment, l'IA «ciblée» est plus susceptible d'être utilisée dans l'environnement professionnel criminel, mais les systèmes de sécurité y font également de plus en plus appel. Toutefois, ces systèmes sont souvent «fermés» et ne font qu'indirectement partie intégrante d'une prestation, par exemple de Threat Detection & Analysis. De plus, les systèmes fondés sur des règles ne relèvent pas tous de l'«intelligence artificielle». Ici, il y a beaucoup de marketing en jeu.

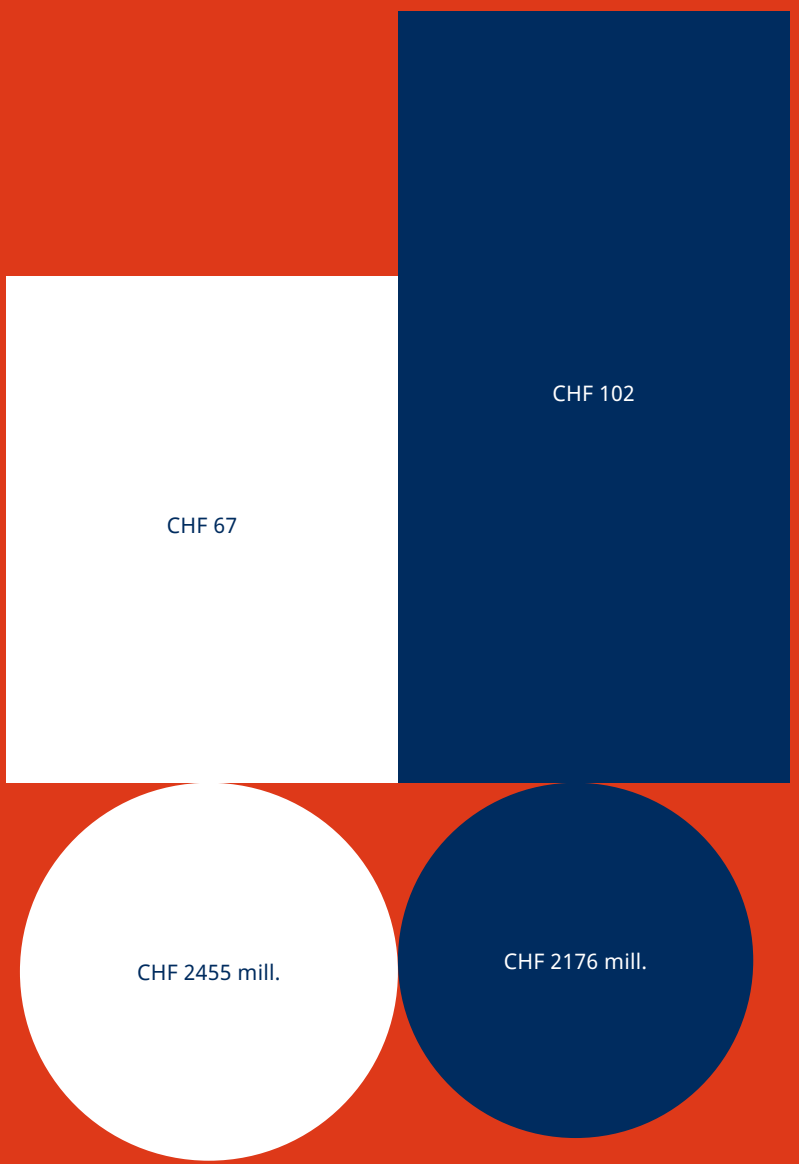
Qui est le moins préparé aux attaques de ransomware ciblant l'interface client-banque? Il s'agit avant tout des gestionnaires de fortune et des fiduciaires sans licence bancaire, qui ne sont ni fortement réglementés ni surveillés. Mais même les acteurs du marché qui proposent exclusivement des services financiers électroniques n'ont pas toujours l'expérience pratique nécessaire. Ils pensent souvent pouvoir déléguer la cybersécurité et le reste de l'informatique à des fournisseurs de services externes. Une «gouvernance» digne de ce nom ne peut cependant pas être déléguée.

Dans quelle mesure les fondements juridiques de la cybersécurité remplissent-ils leurs objectifs? Les prescriptions légales créent la pression nécessaire pour établir la cybersécurité même lorsque le travail de persuasion n'aboutit pas. Le secteur financier est déjà très bien couvert dans ce domaine. Les entreprises de l'industrie manufacturière ne sont souvent pas encore suffisamment sensibilisées. Elles risquent de perdre leur propriété intellectuelle, leur chiffre d'affaires ou leur réputation auprès de leurs partenaires et clients. Les lois peuvent avoir un effet positif ici, à condition qu'elles ne surréglementent pas et n'entraînent pas de nouveaux risques et de nouvelles inégalités des chances sur le marché.

Les montants moyens des cartes suisses et étrangères en Suisse et à l'étranger diffèrent sensiblement – à titre d'exemple pour le mois de juin 2022.

Le montant moyen des transactions effectuées avec des cartes de crédit émises en Suisse est plus élevé à l'étranger que chez nous. L'une des raisons peut être que les dépenses sont plutôt importantes (par ex. achats hebdomadaires ou nuitées d'hôtel) à l'étranger, alors qu'en Suisse, ce sont les petits achats quotidiens qui prédominent.

- Cartes de crédit suisses en Suisse
- Cartes de crédit suisses à l'étranger

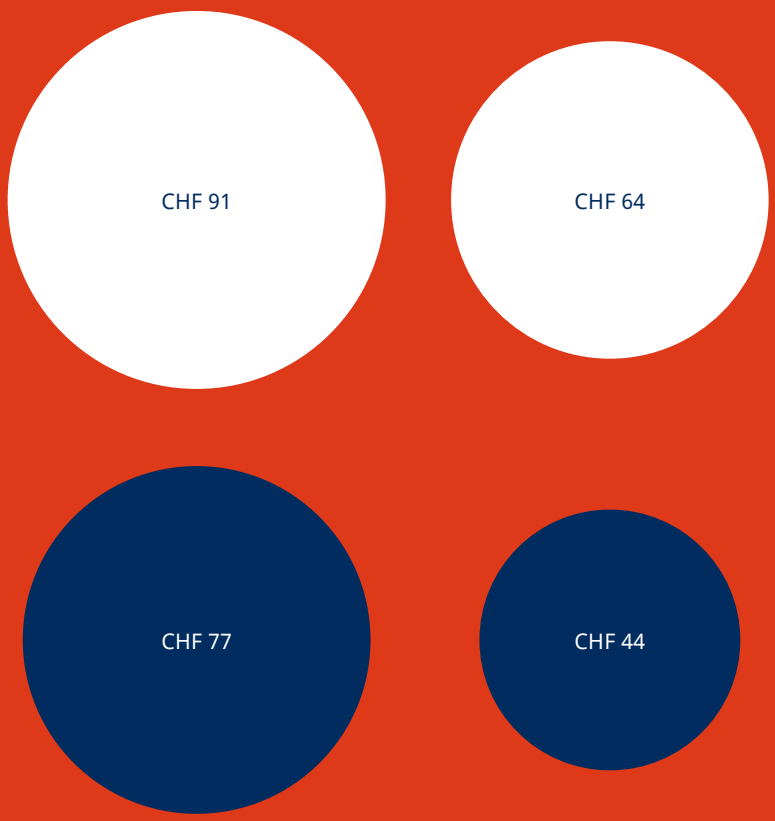


Source Portail de données de la Banque nationale suisse, paiements et retraits d'argent liquide. Les données proviennent d'une enquête partielle. Informations complémentaires: Marché financier (data.snb.ch)

Montants des cartes de débit par transaction

Les personnes titulaires d'une carte de débit étrangère (par ex. vacanciers ou frontaliers) dépensent moins d'argent par transaction dans notre pays que les Suisses à l'étranger.

- Cartes de débit suisses à l'étranger
- Cartes de débit étrangères en Suisse



Montants par transaction par carte de crédit (effectuée sur place)

Montants par transaction par carte de débit (effectuée sur place)

En mettant également l'accent sur les transactions effectuées sur place*, on constate que les montants moyens payés avec des cartes étrangères chez nous diffèrent considérablement de ceux payés avec des cartes suisses à l'étranger, tant pour les cartes de débit que pour les cartes de crédit.

* Les transactions effectuées sur place comprennent tous les paiements physiques au terminal de caisse sur place.

- Cartes suisses à l'étranger
- Cartes étrangères en Suisse

Agir avec éthique contre le hacking de voitures et de dispositifs médicaux

TEXTE
SIMON BRUNNER

Rendez-vous sur place à Zurich-Altstetten. L'adresse mène à un immeuble de bureaux gris. Une porte sans nom s'ouvre au deuxième étage. Un couloir austère mène à une salle de réunion à l'aménagement spartiate. Nous sommes en visite chez une société de cybersécurité ou, plus précisément, chez un ancien hacker qui aide les entreprises à trouver des vulnérabilités dans leurs propres dispositifs de sécurité. Son nom: Marc Ruef.

Passons tout d'abord aux stéréotypes: un hacker court-il en pull à capuche? Marc Ruef porte une longue barbe bien soignée, un costume et une chemise. Les hackers sont-ils des criminels? «Dans ma vie, je n'ai jamais cherché à voler quoi que ce soit ou à nuire à quelqu'un», déclare cet homme de 41 ans. Les hackers agissent-ils dans la zone grise légale? Marc Ruef est chargé de cours à l'ETH et dans plusieurs universités spécialisées.

Ce natif d'Argovie est entré très tôt en contact avec des ordinateurs: dès l'âge de 12 ans, il a été autorisé à programmer sur le PC de son père, mais seulement quelques heures par semaine. Il a rapidement découvert comment déverrouiller lui-même l'appareil. Craignant que ses activités soient détectées, il s'est rendu dans une bibliothèque pour savoir comment manipuler l'horodatage. En même temps, il est tombé sur de la littérature consacrée aux virus informatiques. Dès lors, plus rien ne pouvait l'arrêter.

Hackers et crackers

Nous sommes dans les années 90. «Hacker» était encore un qualificatif honorable à l'époque, les mauvais garçons, les criminels s'appelant des «crackers». Aujourd'hui, le terme n'est considéré positivement que s'il est combiné au mot «éthique». Les spécialistes comme Marc Ruef, qui rendent les systèmes informatiques plus sûrs, sont donc des «hackers éthiques».

Mais revenons à Marc l'adolescent. Il s'agit pour lui du plus grand défi intellectuel. Le bidouilleur veut démontrer qu'aucun système informatique n'est vraiment sûr. Le monde des hackers est encore jeune, et il rejoint rapidement la famille. Lorsqu'il est l'un des premiers à publier ses découvertes, il est attaqué par ses pairs. Ceux-ci ne veulent pas que les failles de sécurité soient rendues publiques et corrigées. À 16 ans, il lance un portail de sécurité pionnier sur Internet. À 18 ans, il publie son premier livre puis, à 22 ans, ce qu'il appelle l'«œuvre de sa vie»: «L'art du Penetration Testing». Il s'agit d'un énorme pavé de plus de 900 pages, qui montre comment analyser

Les voitures de société sont particulièrement vulnérables aux attaques des hackers. Marc Ruef en action.

systématiquement son propre réseau pour détecter les points faibles et les failles de sécurité. Le livre s'écoule en un rien de temps.

Après une formation commerciale, Marc Ruef transforme d'abord son passe-temps en profession auprès d'une entreprise de sécurité informatique. En 2002 déjà, il lance scip AG avec deux partenaires. Aujourd'hui, son entreprise compte 50 collaborateurs, conseille les moyennes et grandes entreprises et leur montre comment mieux se protéger contre les cyberattaques.

Les voitures sont des centres de calcul mobiles

Depuis, Marc Ruef s'est lui-même spécialisé dans des cas exceptionnels d'application de la cybersécurité: le «car hacking» consiste à s'introduire dans l'électronique automobile pour prendre le contrôle de fonctions clés telles que le démarrage ou l'arrêt du moteur, ou encore le déverrouillage des portes. «Les voitures modernes sont des centres de calcul mobiles», explique-t-il. «Une énorme quantité d'électronique est installée.» Mais ce sont des ingénieurs, et non des cyberspécialistes, qui conçoivent les voitures. «En conséquence, il y a de grandes lacunes en matière de sécurité», déclare Marc Ruef.

Les dispositifs médicaux sont une autre spécialité de scip. Par exemple, Marc Ruef et son équipe ont pu prouver que l'administration automatique des médicaments ainsi que l'affichage des écrans d'hôpital peuvent être manipulés via le réseau. Un attaquant malveillant pourrait augmenter la dose de médicaments d'une personne malade sans que les dispositifs indiquent une anomalie et déclenchent l'alarme. «L'hôpital qui utilise ces appareils était très préoccupé», déclare Marc Ruef, «mais le fabricant ne voulait pas combler la faille de sécurité, comme c'est souvent le cas. Cela lui revenait trop cher.» Ce n'est que lorsque l'Agence américaine des produits médicamenteux FDA a été prévenue que la vulnérabilité a été corrigée.

Scip traite également d'autres formes modernes de cybercriminalité, telles que les deepfakes (c'est-à-dire des photos, de l'audio ou des vidéos falsifiées de manière réaliste), la tricherie dans le monde très lucratif de l'e-sport, et la sextorsion, une technique consistant à faire chanter les victimes avec du contenu compromettant.

Aujourd'hui, Marc Ruef se préoccupe aussi beaucoup de l'interface entre la société et la technologie. Il s'agit de questions relatives à la protection des données, à la vulnérabilité de la société ou à l'interaction humaine avec les systèmes d'intelligence artificielle. En outre, Marc Ruef a développé un système qui prédit les attaques numériques dans le monde entier, ainsi que les cybergroupes qui seront particulièrement actifs dans un avenir proche.

Le hacking comme discipline universitaire?

«Le besoin de cybersécurité a explosé au cours des dix dernières années», déclare Marc Ruef. D'un côté, il en est ravi – son entreprise bénéficie de ce boom – et de l'autre, il est désabusé: «De nombreuses entreprises sont trop insouciantes: elles créent des systèmes informatiques complexes, mais manquent de ressources pour les comprendre et les gérer.» Marc Ruef est souvent moqué pour son mantra, qu'il continue néanmoins obstinément à répéter: «Concevez vos systèmes informatiques de manière aussi simple que possible.»

Marc Ruef était un hacker pionnier et un autodidacte. À quoi ressemble le milieu aujourd'hui? La plupart des candidats qui lui soumettent leur candidature ont un diplôme universitaire en informatique avec une spécialisation en sécurité ou cybersécurité, par exemple. Ils sont souvent bien formés, «mais la créativité est un peu laissée sur le carreau. Le piratage informatique ne s'apprend pas à l'université», explique-t-il.

Nous parlons enfin d'intelligence artificielle. Marc Ruef craindrait-il que les ordinateurs nous dominent un jour? Il rit et pointe vers une affiche accrochée au mur. Elle montre les résultats d'un test de QI qu'il a développé avec son équipe pour les assistants numériques: Siri est le meilleur, suivi par Alexa, Cortana et Google. «J'ai également fait le test», dit-il, «et j'étais content d'être encore à mille lieues des appareils.»

Les CBDC entrent en œuvre

Selon la société de conseil PwC, à la mi-2021, près de 70 % des banques centrales avaient développé des concepts ou des prototypes pour des monnaies numériques de banque centrale (CBDC). Les Bahamas ont été les premiers à introduire la leur, le Sand Dollar. Un an plus tard, le «PwC Global CBDC Index» parle de 80 % des banques centrales. Et trois autres ont lancé leurs CBDC comme monnaie légale: le Nigéria, la Jamaïque et les sept États membres de l'Organisation des États de la Caraïbe orientale. Pour en savoir plus sur le développement rapide de cette thématique dans le monde entier, il vaut la peine de consulter le tracker interactif du groupe de réflexion américain Atlantic Council.

Informations complémentaires
www.pwc.com
www.atlanticcouncil.org/cbdctracker

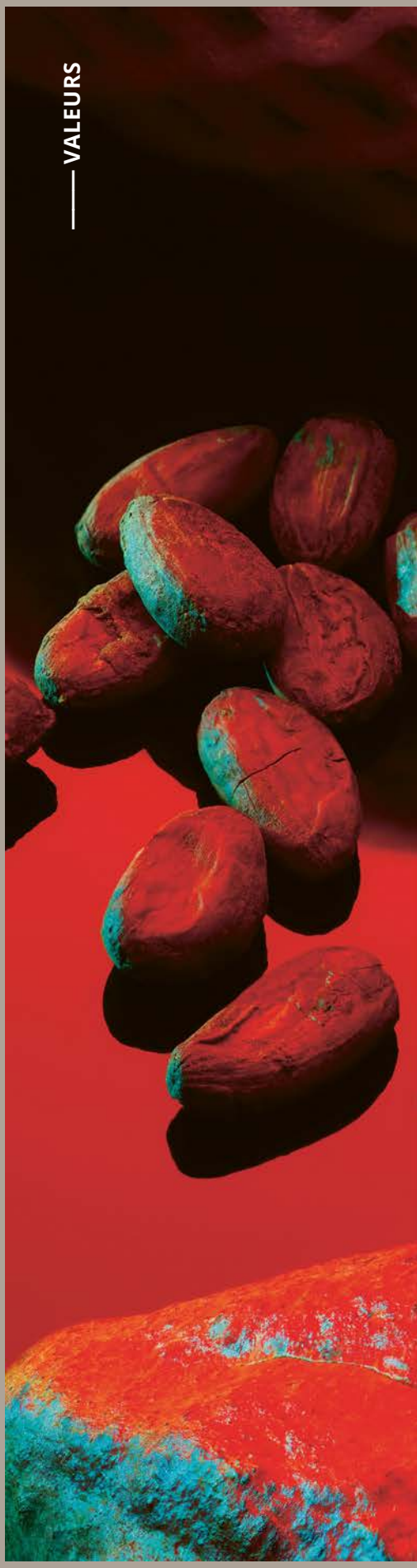
Un monde sans argent liquide?

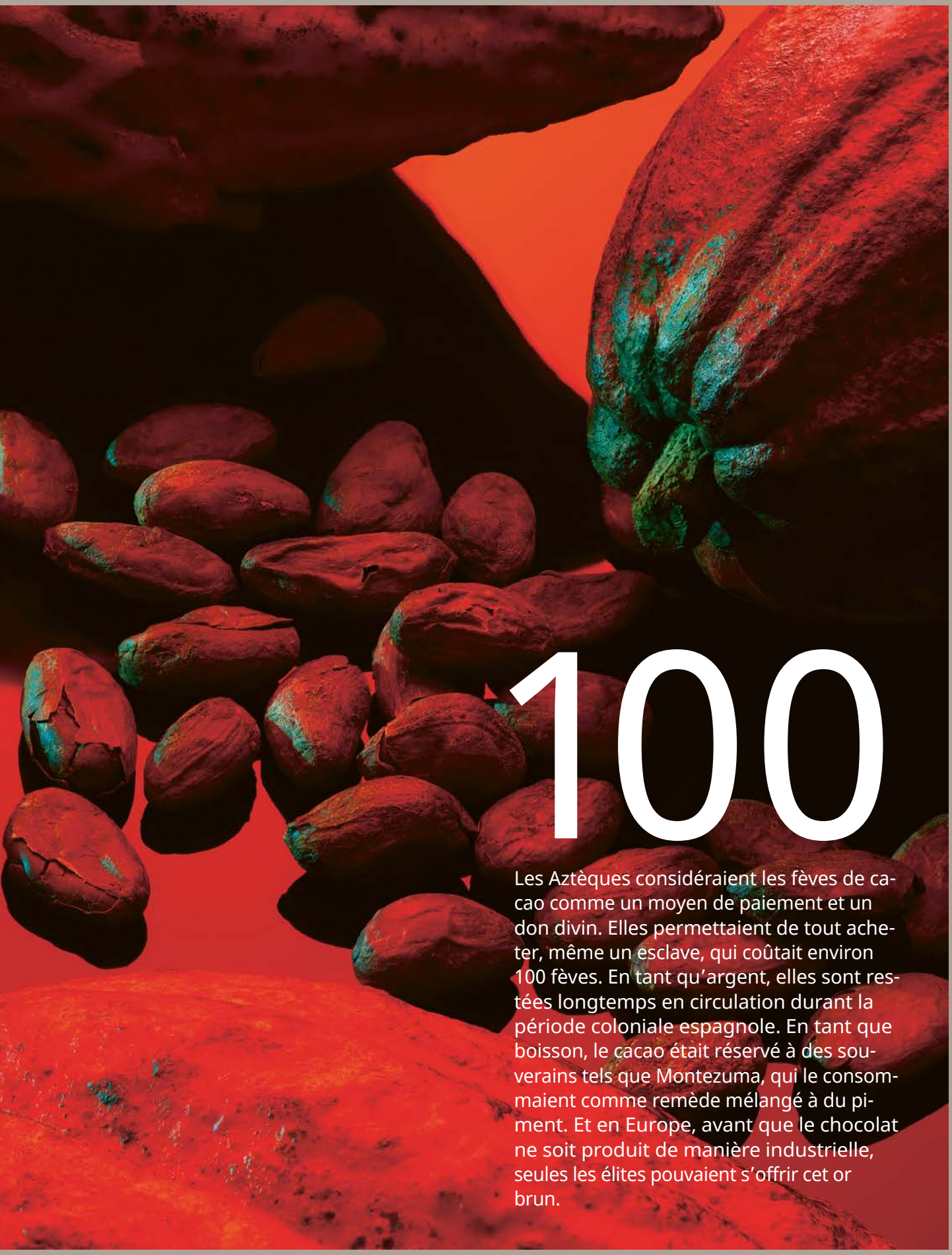
Est-il concevable qu'un jour, y compris en Allemagne, le nombre de transactions en espèces puisse être inférieur à 15 % voire moins, à l'instar de la Scandinavie, de l'Islande et du Royaume-Uni? Le nouveau rapport «Un monde sans argent liquide – Transformations des systèmes bancaires et de paiement classiques» destiné au Bundestag allemand se consacre à ce sujet ainsi qu'à d'autres questions tout aussi captivantes.

Informations complémentaires

Depuis le 26 août, le Musée suisse de la finance présente l'exposition spéciale «Banques en évolution: du guichet à l'app». Avec une rétrospective sur l'histoire des bulletins de versement.

Informations complémentaires
finanzmuseum.ch





100

Les Aztèques considéraient les fèves de cacao comme un moyen de paiement et un don divin. Elles permettaient de tout acheter, même un esclave, qui coûtait environ 100 fèves. En tant qu'argent, elles sont restées longtemps en circulation durant la période coloniale espagnole. En tant que boisson, le cacao était réservé à des souverains tels que Montezuma, qui le consommaient comme remède mélangé à du piment. Et en Europe, avant que le chocolat ne soit produit de manière industrielle, seules les élites pouvaient s'offrir cet or brun.

Les choses sérieuses commencent pour les adresses structurées

Savoir nécessaire
— Connaissance de la norme ISO 20022
— Connaissance préalable de la gestion des données d'adresses

Il est clair depuis longtemps que SWIFT permettra en novembre de cette année d'utiliser les adresses structurées conformément à la norme ISO 20022 pour le trafic des paiements transfrontaliers et les introduira à titre obligatoire d'ici novembre 2025. Le fait que la place financière suisse s'adapte aux conditions-cadres internationales et introduise aussi l'obligation d'utiliser l'adresse structurée en novembre 2025 est également connu depuis un certain temps. Les choses se concrétisent maintenant pour la première fois. Bien que la Suisse ait pu utiliser l'adresse structurée depuis le passage à la norme ISO 20022, cela est désormais possible également par les paiements transfrontaliers avec la migration dans le réseau SWIFT des messages MT précédents vers les nouveaux messages MX. L'utilisation des adresses structurées est même imposée dans deux cas, à savoir lors de l'utilisation des éléments «Ultimate Debtor» et «Ultimate Creditor» – débiteur ou bénéficiaire final «proprement dit».

Toutefois, cela n'est possible que si la banque expéditrice est passée à MX. Les banques du monde entier ont le temps jusqu'en 2025, de sorte que pendant cette phase de migration, il est essentiel pour les clients de demander à leur banque si l'Ultimate Debtor ou l'Ultimate Creditor ou les autres nouvelles possibilités des messages MX peuvent déjà être utilisés. Dans certaines conditions, cela peut également varier selon les monnaies ou les modes de paiement. Pour assurer une transmission des données de bout en bout, il faut que non seulement la banque expéditrice, mais aussi la banque réceptrice et éventuellement les établissements financiers soient passés à MX. Dans son réseau, SWIFT fournit une assistance à cet égard au fil du temps. Le changement, échelonné au niveau international sur les trois prochaines années, implique plusieurs milliers de participants SWIFT et s'avère donc complexe. En raison de ce changement échelonné, le Payment Market Practice Group (PMPG) recommande que les nouveaux éléments tels que l'Ultimate Debtor ou l'Ultimate Creditor ne soient utilisés qu'à partir de novembre 2023 seulement. Par contre, la communauté interbancaire suisse, qui compte environ 320 établissements participants, trouve plus facile d'introduire la nouvelle version de message et d'éventuelles nouvelles règles. Dès novembre 2022, SIC et euroSIC soutiendront les nouveaux éléments, tant pour les paiements domestiques que pour les transmissions d'ordres de paiement transfrontaliers. Dans notre pays, il n'est pas non plus crucial que les nouvelles versions de messages conformes aux Swiss Payment Standards (SPS) 2022 ou encore celles de SPS 2021 soient déjà utilisées dans l'interface client-banque. En effet, les messages actuels selon SPS 2021 acceptent déjà l'utilisation des adresses structurées. Même si elles offrent moins d'éléments d'adresse, la plupart des cas d'utilisation sont suffisamment couverts. Les nouvelles versions de message n'ont pas d'autres éléments, mais seulement des éléments supplémentaires, qui affectent principalement d'autres systèmes d'adressage. À l'inverse, cela signifie que même avec la version SPS actuelle, un Ultimate Debtor ou un Ultimate Creditor peut recevoir des adresses structurées si ces ordres doivent être transmis sous forme de paiements transfrontaliers via le réseau SWIFT avec des messages MX. À partir de 2025, tout devrait être beaucoup plus simple et plus clair si l'utilisation générale des adresses structurées devient obligatoire dans le monde entier.

MARTIN WALDER,
HEAD BILLING & PAYMENTS STANDARDS, SIX

Le SEPA adopte l'adresse structurée
Avec le nouveau Rulebook SEPA 2023, les adresses structurées sont également introduites en option dans l'espace SEPA. Cela permet un traitement uniforme, qu'un paiement soit acheminé via SIC, euroSIC, un prestataire SEPA ou SWIFT. Et l'utilisation obligatoire des adresses structurées est également prévue pour le changement suivant en 2025. Les règles détaillées seront publiées dans le cadre de SPS 2023 en février 2023.

Données structurées

```
<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

Figure 1: Exemple d'adresse structurée dans pacs.008

Multibanking ISO 20022 grâce au scénario «Relay» de SWIFT

Savoir nécessaire
— Connaissance approfondie des types de messages pain

Bien que les messages client-banque soient exclus de la migration vers la norme ISO 20022 de SWIFT, il existe une exception: le scénario dit «Relay». Il intervient lorsqu'un établissement financier propose à sa clientèle professionnelle un regroupement des comptes, également appelée multibanking. Avec une seule connexion bancaire technique, le client professionnel peut envoyer des instructions à d'autres banques dans le monde entier et recevoir des relevés de compte. Sans multibanking, une entreprise avec cinq relations bancaires, par exemple, doit également entretenir cinq connexions techniques avec les banques. Avec le multibanking (figure 2), une seule connexion bancaire est nécessaire, ce qui permet au client de gagner du temps et de l'argent.

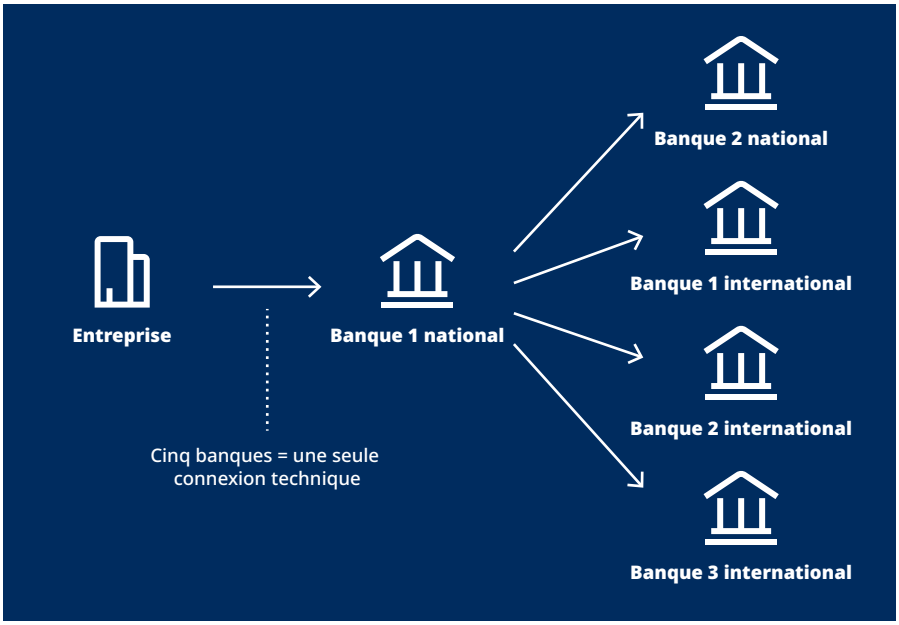


Figure 2: Ordres bancaires avec service de compte multibanking

Gain de temps et d'efficacité

Le multibanking convient à toutes les entreprises entretenant plusieurs relations de compte. En Suisse, par exemple, 70 % des PME ont plus d'une relation bancaire. Grâce au multibanking, les comptes de banques tierces peuvent être gérés en Suisse et, grâce au scénario Relay de SWIFT, également dans le monde entier via une unique connexion bancaire. D'une part, les paiements peuvent être effectués au débit d'un compte bancaire tiers à l'étranger en faveur de fournisseurs locaux via une unique relation bancaire. D'autre part, grâce aux relevés de compte électroniques, les clients bénéficient d'une transparence totale sur tous les comptes, y compris ceux des banques tierces. Cela augmente considérablement les gains de temps et d'efficacité.

Les promoteurs

Le groupe de travail Cross-Border Payments and Reporting Plus (CBPR+) a travaillé en étroite collaboration avec le groupe de travail Common Global Im-

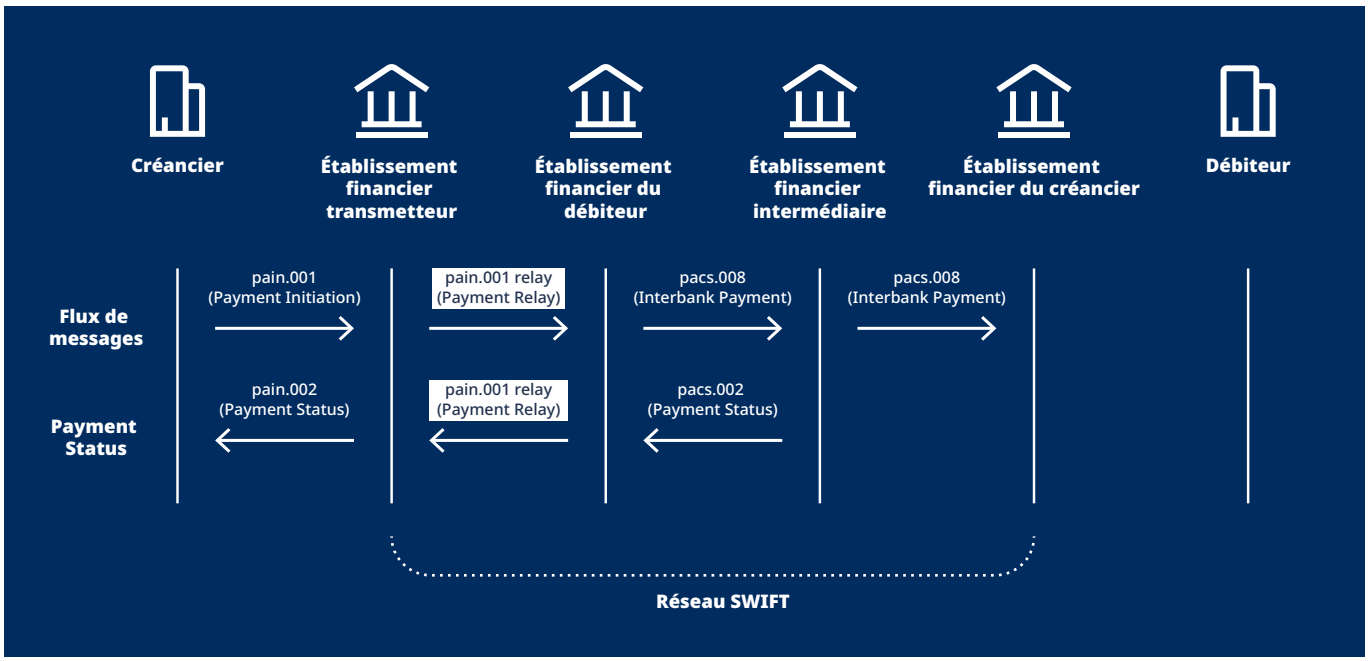


Figure 3: Le flux de messages sur le réseau SWIFT pour le scénario Relay

plementation (CGI) pour élaborer les directives d'utilisation du scénario Relay. Elles couvrent les scénarios interbancaires «Payment Initiation» (pain.001) et «Payment Status Report» (pain.002).

Le CGI, dans lequel sont représentés le monde financier (bancaire) et celui des entreprises, est soutenu par SWIFT pour promouvoir l'introduction des normes ISO 20022 dans les nouvelles financières et faciliter la mise en œuvre de ces messages ISO 20022.

Les deux messages ISO 20022 dans le scénario Relay

Payment Initiation

Dans ce scénario Relay, la partie initiatrice envoie le message interbancaire «Customer Credit Transfer Initiation» (pain.001) à l'établissement financier transmetteur ou à celui du débiteur pour demander le mouvement de fonds du compte débiteur vers un créancier. L'établissement transmetteur agit comme un concentrateur qui transmet le message pain.001 à l'établissement financier du débiteur (voir le flux de messages sur la figure 3).

Payment Status Report

Dans ce scénario Relay, l'établissement financier mandaté envoie le message interbancaire (Customer Payment Status Report» (pain.002) à la partie précédente de la chaîne de paiement pour l'informer du statut positif ou négatif d'une instruction. Le message pain.002 est également utilisé pour avertir le créancier d'un ordre de virement en attente (voir Payment Status sur la figure 3).

Le calendrier SWIFT

En novembre 2022, les établissements financiers commenceront à migrer vers la norme ISO 20022 (MX) pour les paiements transfrontaliers et le reporting, avec une phase parallèle portant sur les messages MT jusqu'en novembre 2025. Ce calendrier ouvre également la voie au scénario Relay. Ainsi, les banques qui prennent en charge le multibanking devront être passées au scénario Relay ISO 20022 d'ici 2025 au plus tard.

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

À travers le fouillis inextricable des certificats numériques

Savoir nécessaire
— Connaissances de base des méthodes de cryptage

Les certificats numériques sont devenus incontournables. Si leurs sigles TLS, HTTPS, CA, ECC et RSA peuvent paraître «cryptiques», ces certificats le sont eux aussi, si l'on s'en réfère à l'origine latine du mot: crypticus, ou «caché». Cachés et omniprésents derrière les connexions Internet qu'ils sécurisent en cryptant les données. Ainsi, les tiers non autorisés ne peuvent ni lire ni manipuler le trafic de données échangées entre le navigateur, le site Web visité et le serveur du site Web.

Un certificat numérique, également appelé certificat de clé publique ou certificat d'identité, n'est rien de plus qu'une clé cryptographique. Émis par une autorité de certification de confiance, le certificat prouve l'authenticité des informations de connexion d'une personne sur Internet ainsi que son identité. Il s'agit d'une sorte de badge de sécurité, qui garantit à la fois à la personne qui saisit les données et à celle qui les reçoit qu'elles sont transmises à une source de confiance.

Transport Layer Security (TLS)

TLS est le successeur du protocole Secure Sockets Layer (SSL), désormais obsolète. En pratique, il sert de méthode standard pour sécuriser la communication de machine à machine sous forme de certificats numériques.

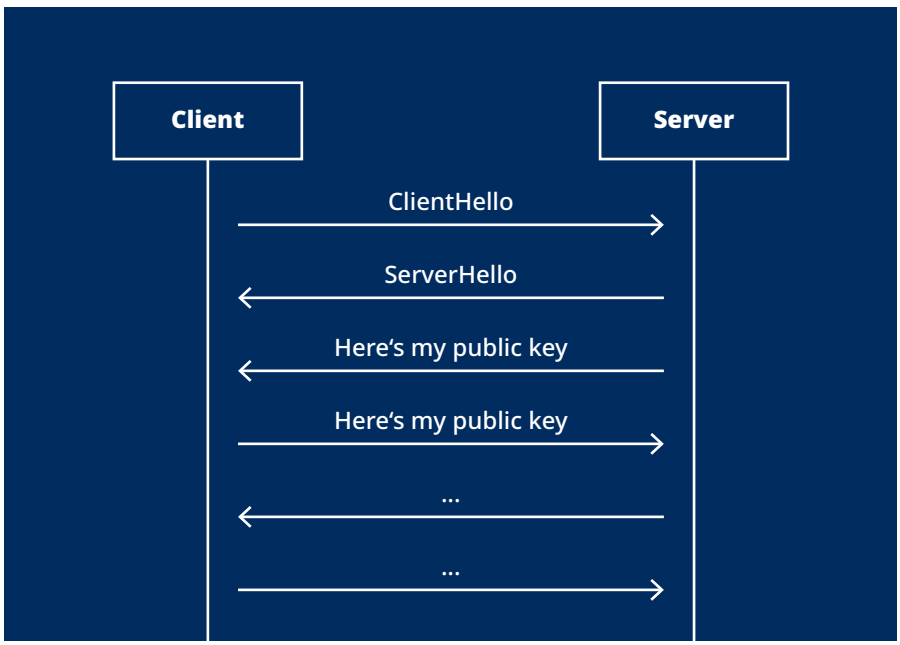
Les sites Web utilisent le plus souvent les certificats TLS. Ils sont les seuls permettant de garantir qu'un site Web applique le chiffrement HTTPS (indiqué par un petit cadenas dans la barre d'adresse) et que les données peuvent être transmises de manière sécurisée entre les sites Web, les navigateurs et les serveurs Web sans être interceptées ou modifiées. Il est ainsi possible d'authentifier l'identité d'un opérateur de site Web.

Fonctionnement du certificat TSL

Le certificat TLS établit une connexion chiffrée entre un site Web ou un serveur et un navigateur sans que la personne qui visite le site Web le remarque.

L'authentification a lieu en premier. Pour chaque nouvelle session que la personne démarre, son navigateur et le serveur de l'opérateur du site Web

Figure 4: Échange de clés avec TLS



échangent et valident leurs certificats TLS. Vient ensuite l'échange de clés.

Le serveur partage sa clé publique avec le navigateur, que ce dernier utilise ensuite pour générer une clé passe-partout (clé pré-maître). Enfin, le serveur décrypte ce passe-partout avec sa clé privée et établit une connexion sécurisée et chiffrée pour la durée de la session.

Les trois types de cryptographie

La cryptographie se préoccupe généralement de la sécurité de l'information et en particulier du cryptage et du décryptage de l'information. Un algorithme est utilisé pour crypter le texte en clair et le rendre illisible. Il est utilisé pour le chiffrement des données, l'authentification et les signatures numériques.

Le chiffrement symétrique appartient à la première catégorie cryptographique. Ici, l'expéditeur et le destinataire partagent une seule clé, à l'aide de laquelle l'expéditeur chiffre le texte en clair avant de le transmettre au destinataire. Ce dernier utilise ensuite la même clé pour décrypter le texte chiffré et restaurer le texte en clair de l'expéditeur.

La deuxième catégorie inclut la clé publique ou le chiffrement asymétrique. Deux clés sont liées entre elles: la clé publique et la clé privée. Alors que la clé publique peut être distribuée librement, la clé privée correspondante doit rester secrète. La clé publique est utilisée pour crypter les données qu'une personne veut envoyer. La clé privée utilisée pour décrypter les données est généralement conservée par le créateur de la paire de clés. Les algorithmes les plus couramment utilisés ici sont RSA (Rivest-Shamir-Adleman) et ECC (Elliptic Curve Cryptography); les certificats TLS utilisent souvent RSA. On augmente constamment la taille recommandée de ces clés (par exemple de 1024 à 2048 bits) pour maintenir leur efficacité. Sur le plan cryptographique, ECC est aussi efficace que RSA. Cependant, la taille des clés est beaucoup plus petite, ce qui réduit les frais de calcul et de stockage tout en augmentant la vitesse et la sécurité. L'inconvénient est que les applications basées sur ECC ne sont pas toutes interopérables avec les certificats TLS.

La fonction de hachage est la troisième catégorie cryptographique. Cet algorithme n'utilise pas de clé, mais compresse le texte en clair numériquement en fonction de longueurs fixes, de sorte que le contenu du texte en clair ne puisse plus être reconstitué. Les fonctions de hachage sont souvent utilisées par les systèmes informatiques pour crypter les mots de passe.

À quoi sert la signature numérique?

Une signature numérique, émise par des fournisseurs de services de confiance tels que SwissSign, est un certificat de signature lié cryptographiquement à un document par une infrastructure à clé publique (PKI). Les signatures numériques valident et authentifient l'identité du signataire et l'intégrité du document. Elles fournissent un niveau élevé d'assurance que la personne qui a signé le document l'a effectivement écrit et garantissent qu'aucune modification n'a été apportée au document. Les signatures numériques peuvent parfois être utilisées pour sécuriser l'accès à des données confidentielles ou dans le contexte de la cyberadministration, par exemple pour demander un passeport par Internet.

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

Phygital Banking: l'exemple des cartes de paiement

Le monde physique et le monde numérique fusionnent de plus en plus. Combinés, ils peuvent mener à de nouvelles expériences client passionnantes. Numériser des processus physiques, compléter le monde virtuel par des services physiques, telle est la quintessence du «phygital», contraction des mots «physique» et «digital».

Aujourd'hui, les particuliers attendent des options de paiement personnalisées, pratiques et sécurisées s'intégrant bien à leur vie physique et numérique. Les guichets classiques de transactions en espèces se transforment en zones de libre-service numérique, qui permettent en même temps de dispenser des conseils personnels.

Les cartes de paiement sont un bon exemple de Phygital Banking. Après l'ouverture d'un compte, l'émission d'une carte constitue la prochaine interaction importante entre la banque et la clientèle. Pour réduire le temps jusqu'à l'arrivée de la carte physique, la banque offre une carte virtuelle instantanément disponible qui permet aux clients de faire des achats en ligne. La banque envoie ensuite des mises à jour à la carte physique (par exemple, via l'état de livraison postale), que les clients peuvent consulter à tout moment via leur téléphone mobile. Les cartes physiques peuvent être sécurisées dans une app mobile, puis combinées à des outils numériques pour le suivi et la compensation du CO_2.

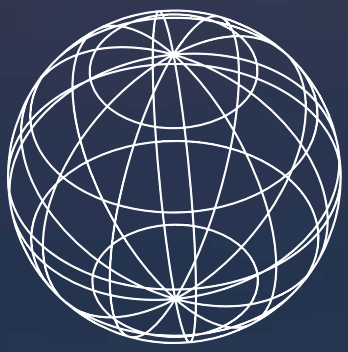
L'expérience de marque

La lettre servant de support physique à la carte peut également être phygitale: individualisée avec des contenus et codes QR, qui font de l'arrivée d'une nouvelle carte une expérience de marque pour la clientèle. Et la carte elle-même est personnalisée avec des images sélectionnées par les clients. Ou elle est fournie par des kiosques qui authentifient un titulaire de carte et émettent une nouvelle carte en quelques minutes. Les apps mobiles peuvent également prendre en charge l'activation de la carte sans que l'on ait à se rendre dans une succursale.

Dans son étude «Opportunités dans le paysage phygital», le groupe technologique Giesecke+Devrient a récemment examiné ce que cela signifie pour les banques et les prestataires de services financiers et quelles sont les énormes opportunités d'innovation qui s'offrent à eux. L'enquête menée auprès des prestataires de services financiers dans 15 pays a révélé la pertinence des cartes de paiement physiques en tant que lien important entre la banque et la clientèle. Les cartes agissent comme un élément de marque unique et servent d'ancrage physique pour les services numériques. Les offres phygitales aident les banques à rester pertinentes, avec des expériences utilisateur innovantes chez les néo-banques et les grandes entreprises technologiques.

GABRIELLE BUGAT,
MEMBRE DE LA DIRECTION DE GIESECKE+DEVRIENT ET RESPONSABLE DU DOMAINE CARD & DIGITAL PAYMENT

INFORMATIONS COMPLÉMENTAIRES



SWIFT Go: une nouvelle norme internationale pour les paiements de petits montants

Envoyer de l'argent partout dans le monde devrait être simple. Simple pour les petites entreprises qui font des achats à l'étranger. Et simple pour les familles qui veulent envoyer de l'argent à leurs proches à l'étranger.

L'introduction de SWIFT gpi a définitivement transformé le système de paiement transfrontalier de gros montants – il est devenu plus rapide, plus transparent et traçable. À la suite de cette expérience positive, SWIFT rend maintenant la même chose possible pour les paiements de petits montants.

En effet, le marché des petits paiements connaît une croissance rapide: McKinsey prévoit une croissance du marché de 10 % entre 2018 et 2023. Dans cette optique, SWIFT pose les bases d'une solution plus intelligente, fournissant aux banques les ressources dont elles ont besoin pour transformer leurs offres en matière de petits paiements.

Le marché continue de croître, tout comme les attentes de la clientèle. À mesure que les services deviennent plus rapides et plus intuitifs dans la vie quotidienne, les clients s'attendent à ce qu'ils le soient aussi dans des domaines plus complexes tels que le trafic des paiements. Les établissements financiers se doivent d'innover pour rester en phase avec ces attentes.

Sur une base solide

L'idée derrière SWIFT Go est simple: les banques doivent fournir à leurs clients un moyen rapide, facile et traçable d'envoyer de l'argent partout dans le monde directement à partir de leurs comptes bancaires. Les accords de niveau de service de SWIFT sont au cœur de cette solution et permettent exactement cela.

Lorsqu'une banque choisit SWIFT Go, elle clarifie tous les frais avec ses contreparties. Cela garantit que les prix des paiements sont compétitifs et que les clients connaissent le montant de leurs frais de virement avant de déclencher la transaction. La solution utilise les messages MT103 et est également transparente pour les banques effectuant le virement: elles peuvent intégrer les informations de suivi des paiements dans leur front-end pour accroître la prévisibilité.

Les banques s'engagent également à traiter les paiements dans les quatre heures et à ne pas effectuer de déductions supplémentaires. Cela garantit une circulation rapide de l'argent et donne aux particuliers l'assurance que leurs paiements arriveront à temps.

Les paiements SWIFT Go s'exécutent sur la même infrastructure et le même réseau que SWIFT gpi. Les banques et leurs clients peuvent donc compter sur le même niveau de sécurité et de disponibilité des services.

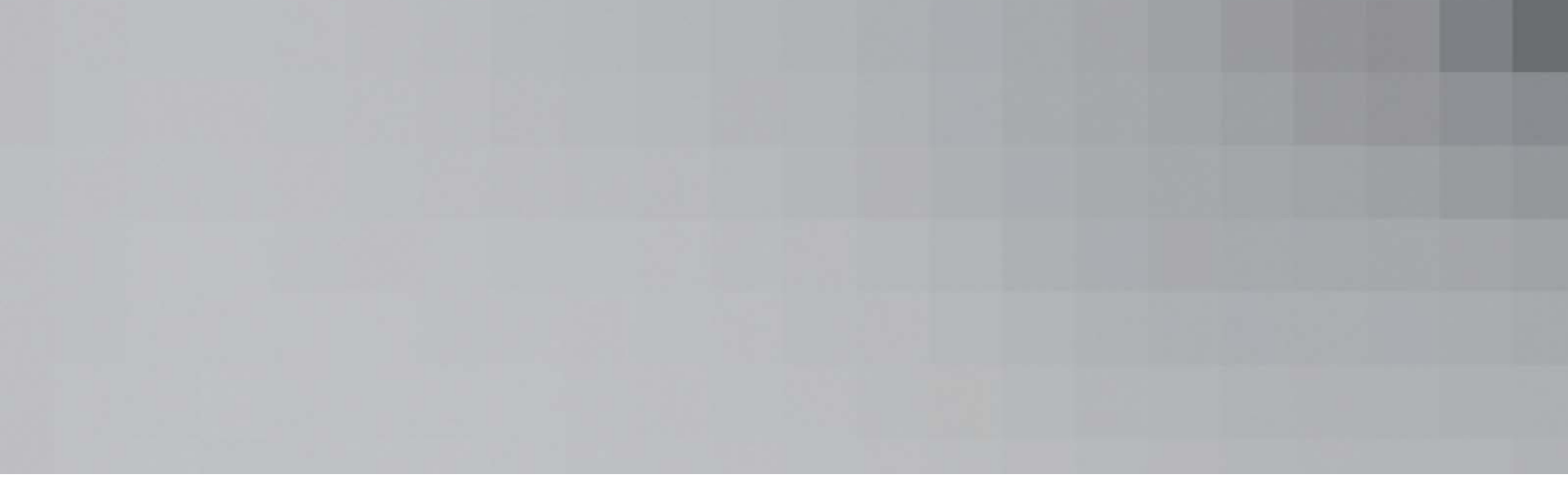
Une communauté en croissance rapide

SWIFT permet des transactions immédiates et sans heurts grâce à son réseau de plus de 11 000 établissements, qui connectent quatre milliards de comptes dans plus de 200 pays. SWIFT Go joue un rôle décisif dans ce domaine, car il permet une plus grande inclusion financière des PME et des consommateurs dans les pays en développement et émergents.

Plusieurs grandes banques correspondantes situées dans d'importants pays partenaires commerciaux de la Suisse ont déjà adhéré à ce service, notamment celles du Royaume-Uni, des États-Unis, de la Chine, des Émirats arabes unis et de l'Inde. Au total, il s'agit de plus de 250 banques dans 90 pays.

ROGER INDERBITZIN, RESPONSABLE DE SWIFT SUISSE ET LIECHTENSTEIN

INFORMATIONS COMPLÉMENTAIRES



Le prix est ce que l'on paye,
la valeur est ce que l'on obtient.

Warren Buffett (1930)