09 | 2018
Edition 76

«Know your enemy»

Interview avec Marc Hofmann, CISO SWIFT, sur la lutte contre les cyberrisques

Joyaux numériques de la place financière et cyberdéfense

Une harmonisation en chasse une autre

it
jet it

La revue suisse spécialisée en trafic des paiements

IMPRESSUM

EDITEUR
SIX INTERBANK CLEARING SA
Pfingstweidstrasse 110
CH-8005 Zurich
T +41 58 399 4747

COMMANDES/FEED-BACK
clearit@six-group.com

EDITION
Edition 76 – septembre 2018
Paraît régulièrement, aussi en ligne sur www.clearit.ch
Tirage en allemand (1300 exemplaires) et en français (400 exemplaires) ainsi qu'en anglais (sous forme électronique sur www.clearit.ch)

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

EQUIPE DE REDACTION
André Gsponer, ConUm AG; Gabriel Juri (responsable), Karin Pache, et Thomas Reske, SIX Interbank Clearing SA

TRADUCTIONS
Anglais: Word+Image AG
Français: Denis Fournier

PRESENTATION
Felber, Kristofori Group, agence de publicité

IMPRESSION
sprüngli druck AG

Vous trouverez d'autres informations sur les systèmes suisses de trafic des paiements sur le site Internet
www.six-interbank-clearing.com

PAGE DE TITRE
Marc Hofmann, Chief Information Security Officer chez SWIFT

Marco Menotti

Chères lectrices, chers lecteurs

En biologie, un «écosystème» désigne une communauté de plantes et d'animaux dans un habitat. Un arbre avec ses champignons et autres êtres vivants forme un écosystème. Avec la prairie environnante, qui représente à son tour un écosystème, il en résulte un ensemble plus vaste, gagnant encore en amplitude en conjugaison avec la forêt.

Il en va de même pour les écosystèmes d'entreprise. Le réseau de paiement mobile suisse déployé autour de TWINT, par exemple, peut être qualifié d'écosystème pour paiements (voir clearit 72, septembre 2017). En considérant que les paiements instantanés prennent de plus en plus d'importance, il est logique de placer cette solution P2P mobile dans le contexte du trafic des paiements interbancaires, où le déclenchement et le crédit de paiements sont traités en temps réel depuis des décennies. Un écosystème peut ainsi se confondre parfaitement dans un autre, à l'instar de l'arbre et de la prairie environnante.

Sous ma direction, SIX est en train de mettre sur pied et avant tout de développer le trafic des paiements en tant que nouvel écosystème en phase avec les besoins actuels et futurs de nos propriétaires, les banques. Il est essentiel que nous comprenions les écosystèmes d'aujourd'hui, que nous puissions interagir entre les différents écosystèmes et que nous exploitions le potentiel de synergies, notamment en termes de dynamiques technologiques ou réglementaires affectant de plus en plus le quotidien du trafic des paiements des banques.

Nous créons et utilisons un large écosystème de produits et de services incluant entre autres TWINT, eBill, LSV, QR-facture, DAB, cartes et SIC/euroSIC. Des avantages en termes de coûts, d'effets de réseau et aussi des innovations ciblées de SIX doivent être créés à l'intention des banques. A l'avenir également, SIX Interbank Clearing SA veillera sous forme réduite – avec l'IT Management et l'Operations Center – à l'exploitation de la plateforme RBTR suisse et assurera que la Banque nationale puisse exercer son influence conceptuelle sur le système SIC d'importance systémique. Tous les domaines non-clés de SIX sont incorporés dans la nouvelle organisation fonctionnelle de l'unité d'affaires, tout en mettant comme par le passé les services existants à la disposition de SIX Interbank Clearing. Viennent se joindre à la nouvelle unité d'affaires les activités d'émission, de traitement et d'exploitation ATM de SIX Payment Services. En font partie des extensions des domaines d'activités actuels, par ex. par le biais de nouvelles offres d'approvisionnement en numéraire («Ecosystème Cash»).

Et non des moindres, la «Swiss Corporate API» (voir clearit 75, juin 2018) implantée chez nous influera positivement, en tant qu'«écosystème Connectivity», sur tous les autres écosystèmes mentionnés, ouvrant de nouveaux champs d'affaires qui dépassent le cadre du trafic des paiements et créant de l'espace pour des services novateurs destinés à élargir et à compléter notre modèle d'affaires. L'arbre, la prairie et la forêt à eux seuls ne suffisent pas à notre aspiration stratégique. Nous nous concentrons sur l'élargissement des écosystèmes. En ce sens, notre revendication dans la réorganisation est la suivante: «Today we are payments – tomorrow we are Banking Services». Elle s'appliquera dès le 1er octobre à la SIX Business Unit Banking Services.

Marco Menotti
Head Business Unit Banking Services, SIX

Marc Hofmann,
Chief Information Security Officer chez SWIFT

Cyber-sécurité – une course contre la montre

«Know your enemy.» Développer des stratégies de détection et de défense, analyser les menaces, sensibiliser aux cyberrisques et promouvoir l'échange des expériences au sein de la communauté. Ce sont quelques-uns des aspects que Marc Hofmann, Chief Information Security Officer chez SWIFT, a abordé en interview.

«Pratiquement tout le monde est exposé à des risques informatiques sous une forme ou une autre», ont constaté des experts du FMI dans un document publié l'an dernier. Cela semble aussi banal que les mises en garde de la police sur les risques d'accident. Comment ce message vous interpelle-t-il personnellement, Monsieur Hofmann?

Je doute que les risques d'accident de la route se soient développés aussi fortement que les cyberrisques au cours des dernières décennies. Les hackers criminels sont aujourd'hui beaucoup mieux organisés qu'ils ne l'étaient il y a quelques années et disposent de multiples ressources. Ils agissent désormais comme une entreprise mondiale, changeant massivement la situation de danger. Un autre aspect est que l'exposition aux attaques s'est élargie: la numérisation, l'ouverture de nos réseaux à l'Internet – ceci est particulièrement vrai pour l'interface client-banque. Prenez l'open banking en tant que mot à la mode ou l'Internet des objets (Internet of Things), voire la réglementation avec la PSD2, qui utilise des API pour ouvrir l'interface client à des tiers.

> «La communauté SWIFT a un intérêt communautaire croissant à sa sécurité.»

Il y a deux ans, SWIFT a annoncé une série de mesures de sécurité en réponse au cyber-hold-up de la Banque centrale du Bangladesh et les a déployées sous le nom de «Customer Security Programme (CSP)» – un article est paru à ce sujet dans clearit 12/2017. A la fin de l'année dernière, tous les clients SWIFT devaient démontrer qu'ils respectent les contrôles de sécurité obligatoires. 89% l'ont apparemment fait. Qu'advient-il de ceux qui n'ont pas participé au mouvement?

Je suis ravi que plus de 90% de nos 12 000 clients aient maintenant terminé leur autocertification. Et ce nombre croît encore pendant que nous en parlons. C'est une bonne nouvelle. En regardant de plus près les chiffres, nous constatons également que ce chiffre couvre plus de 99% de tous les messages SWIFT FIN. Nous visons 100% d'ici la fin de 2018 et nous aiderons les clients restants à effectuer leur attestation CSP. En principe, nous enfonçons là des portes ouvertes, car la communauté SWIFT a un intérêt communautaire croissant à sa sécurité. Avec nos parties prenantes, nous mettons tout en œuvre pour atteindre cet objectif. Cela signifie également que nous signalons aux autorités de surveillance compétentes ceux qui ne respectent pas les exigences. .

En parlant de communauté: on pourrait s'attendre dans une telle communauté à ce qu'un échange animé d'informations et d'expériences ait lieu entre les différents membres. Selon nos informations, cela ne semble pas toujours être le cas. Pour le

moins, seules quelques banques seraient intéressées par le statut de «Security attestation» des contreparties. Quelle en est la cause?
Cela ne se recoupe pas avec mon observation personnelle. En fait, je vois le contraire: un intérêt beaucoup plus fort et croissant dans la sécurité des contreparties. Ce point ne concerne pas uniquement les contreparties et s'applique à toutes les relations avec des tiers – contrairement au passé, lorsque l'on se limitait principalement à sa propre sécurité. J'ai constaté dans de nombreuses banques que des réglementations et des processus avaient été mis en place pour garantir la sécurité chez les partenaires. Les demandes d'informations d'attestation augmentent également dans le monde entier. Bien sûr, comme nous sommes dans un processus d'apprentissage, nous avons encore de la marge pour des améliorations.

> «Tant que les attaquants espèrent pouvoir gagner de l'argent, ils n'arrêteront pas leurs activités.»

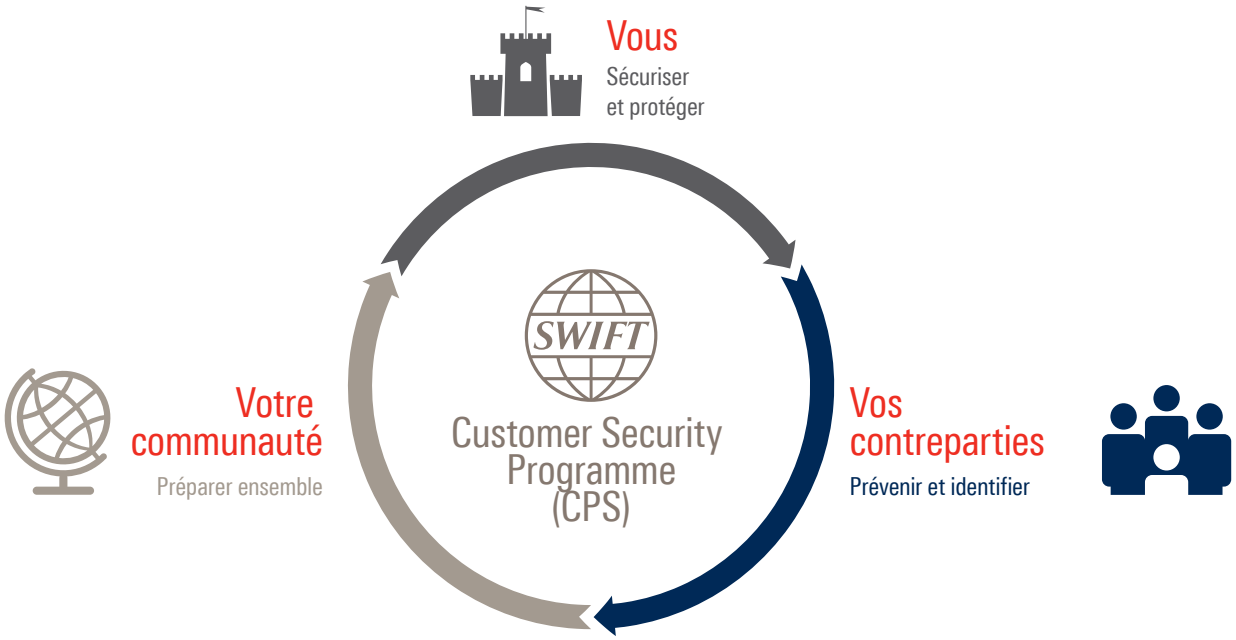
Combien de fraudes de quel montant total ont pu être évitées grâce aux activités CSP?
Nous avons en effet réalisé des progrès tangibles et mesurables dans la lutte contre la fraude. Je ne peux pas citer de chiffres, voire de dossiers individuels. Cependant, nous avons observé de nombreux cas où la fraude de paiement avait pu être évitée grâce à nos mesures. Un autre aspect important est que nos clients sont beaucoup plus conscients de leur propre sécurité et, comme je l'ai déjà mentionné, que les contreparties augmentent également leur capacité à identifier les menaces. Partant, nous nous améliorons. Cependant, j'observe que le nombre de tentatives de fraude ne diminue pas vraiment. C'est plutôt le contraire qui est vrai. Tant que les attaquants espèrent pouvoir gagner de l'argent, ils n'arrêteront pas leurs activités.

Y a-t-il des preuves que les hackers ont déplacé leurs activités criminelles vers d'autres canaux et domaines à cause du CSP?
Nous savons que les hackers criminels déploient de plus en plus d'efforts pour contourner les mesures de sécurité. Ainsi, peu importe ce que les établissements financiers ont introduit, les criminels essaient de trouver une solution de contournement. Avec la bien nommée Deception Technology, nous simulons entre autres de faux serveurs et comptes pour les piéger. Ils réagissent maintenant à cela et réagiront également face à d'autres mesures. Le CSP n'y fait pas exception. Qu'est-ce que cela signifie pour nous? En d'autres termes, nous ne devons pas nous reposer sur nos lauriers et constamment nous demander si nos mesures sont appropriées, pour logiquement toujours en rajouter une couche. Nous détectons très tôt de nombreuses tentatives de fraude avec notre outil de vérification d'intégrité, qui signale à quel moment un message est transmis de manière corrompue.

En parlant d'outil: avec le nouveau service «Payment Controls», SWIFT a mis en place un nouvel outil de protection contre la fraude: le dépistage en temps réel des paiements sortants. Pourquoi pas pour les ordres de paiement entrants?
Tout d'abord, il est du devoir de chaque entreprise de vérifier les messages sortants pour vérifier s'ils ne sont pas frauduleux. Et c'est pourquoi nous avons commencé de ce côté-là. La future extension au côté destinataire n'est ainsi pas exclue.

C'est l'une des prochaines étapes de la course disputée avec les criminels ...
Peut-être que oui. Le hic, c'est que vous devez pouvoir motiver toute la communauté en fin de compte. Il y a peu de choses qui fonctionnent sur simple commutation afin d'obtenir un effet pour toute la communauté. La plupart du temps, un effort collaboratif s'impose. Conclusion: avec nos clients, nous devons déterminer où sont nos priorités et où atteindre le meilleur effet au vu de notre exposition aux dangers actuels et anticipés.

La cybermenace est le revers de la numérisation. La politique, l'économie et la société semblent avoir pris conscience de la gravité de la situation. Pour ne citer que quelques exemples: les Etats membres de l'UE créent ensemble des cybertroupes de réaction rapide, le Conseil fédéral suisse s'adjoint un ou une «Mr./Mrs. Cyber Security». En Allemagne, le plus grand centre de recherche du monde pour la sécurité informatique (Cispa) sera créé avec une filière de master en cybersécurité. Comment SWIFT se met-elle en réseau dans la course à la sécurité avec les initiatives mondiales?
Tout d'abord, je pense que c'est un sujet extrêmement important promouvant la coopération dans la lutte contre le crime – et pas seulement avec les banques ou



nos clients, mais également avec les autorités chargées des poursuites pénales. Je crois que la coopération ou du moins l'échange d'informations sur le modus operandi des cybercriminels auprès des pouvoirs publics, mais aussi avec les universités, sera l'une des compétences critiques pour nous défendre efficacement. C'est pourquoi nous avons déjà entrepris de nombreuses démarches à cet égard et nous en prévoyons d'autres. Par exemple, nous travaillons avec des organisations telles que le Fonds monétaire international ou la Banque mondiale. Nous sommes par exemple dans le FS-ISAC, une organisation du secteur financier, qui approvisionne ses 7000 membres dans le monde entier en informations sur les cybermenaces. Récemment, son sommet annuel a eu lieu à Miami, où les Chief Information Security Officers des banques se sont entretenus et ont discuté franchement.

Cette collaboration est certes importante, mais l'est-elle aussi stratégiquement parlant?
Absolument, et cela pour différentes raisons: la plus évidente est la coopération en matière de renseignement. Donc, nous partageons à bref délai ce qu'on appelle des «Indicators of Compromise» – soit des données sur les menaces telles que des programmes malveillants ou des groupes d'auteurs – avec la communauté SWIFT, afin qu'elle puisse également ajuster sa défense à court terme. Ces données se nourrissent des expériences acquises par d'autres intervenants. Je pense qu'il est extrêmement important d'échanger de telles informations et que nous nous avertissions mutuellement contre d'éventuelles menaces. Et en effet, nous avons été en mesure de nous défendre avec succès contre certaines attaques – nous en avons parlé auparavant sous «Où étions-nous efficaces contre la cyberfraude?».

Un autre aspect stratégique est que nous voulons sensibiliser la communauté SWIFT dans ce contexte. Nous donnons des exemples du fonctionnement des attaques et de la manière dont les auteurs d'attaques procèdent; que certains d'entre eux font preuve d'une très, très grande patience, qu'après avoir pénétré dans le réseau d'une entreprise pendant des mois ou plus d'un an, ils espionnent sans être remarqués l'environnement et les activités des utilisateurs avant qu'ils ne frappent. Nous savons que les criminels frappent astucieusement les jours fériés ou les week-ends afin d'exploiter le comportement des opérateurs locaux. Nous devons partager ces informations et sensibiliser aux risques dans des situations spécifiques afin que les entreprises puissent investir là où c'est le plus pertinent. Nous ne devrions pas nous promener avec l'arrosoir et essayer en vain de tout protéger uniformément, mais plutôt là où le meilleur effet peut être obtenu, ce qui n'est vraiment efficace qu'avec l'aide de la communauté.

Le plan directeur de cybersécurité de SWIFT est articulé autour de quatre critères principaux. Le premier point dit: Know your enemy. Nous connais-

sons bien entendu le principe Know your customer. Mais comment et à quoi reconnaît-on un ennemi?
Tout d'abord, les analyses des menaces sont très importantes. Le deuxième aspect est la capacité des différents Security Operations Centers (SOC) à détecter les intrus. Et c'est un sujet difficile, car les pirates ne veulent pas être reconnus. Mais il existe un support technique, par exemple dans le domaine de l'analyse du comportement des réseaux (Network Behavior Analysis). Il est ainsi possible de détecter un comportement inhabituel dans le réseau pour en dépister les auteurs. Ce type d'analyse comportementale, à l'instar de la Deception Technology mentionnée ci-dessus, est un autre moyen de sensibiliser sur le côté technique de l'infrastructure.

Et puis, bien sûr, il y a le côté commercial. Il s'agit ici de la façon de découvrir par ex. une fraude de paiement. Nous avons brièvement abordé notre nouveau service «Payment Controls». Notre «Daily Validation Report» est un autre moyen de protéger les processus liés au rapprochement quotidien de transactions contre la fraude. Si je reçois un message à un moment inhabituel ou qu'il doit être envoyé à un nouveau bénéficiaire qui m'est inconnu, il est évident que quelque chose cloche. Et cela se résume simplement par «Know your enemy».

Cet été, une nouvelle version du CSP sera publié avec des modifications apportées à de nombreux contrôles de sécurité. Pourquoi le référentiel doit-il être adapté? La version actuellement valide a-t-elle ignoré des aspects importants?
Ce n'est pas le cas. Mais peu importe à quel point nous nous défendons intelligemment contre les cyberattaques, les criminels ne se reposent pas et développent des méthodes de plus en plus sophistiquées. Cela signifie que nous devons nous aussi progresser. Ce principe s'applique au même titre au CSP. Nous devons continuellement examiner et faire évoluer les contrôles pour ne pas perdre la course. Comme les risques et la situation de risque changent constamment, nous devons adapter le CSP en conséquence. En ce sens, il y aura certainement de nouveaux contrôles de sécurité obligatoires à l'avenir – certains finiront peut-être par disparaître. En tout état de cause, je m'attends à ce que le référentiel dans son ensemble soit encore mieux ciblé.

Peut-on conclure que le référentiel est pratiquement soumis à un cycle de release?
C'est ainsi. Nous remettons constamment les contrôles en question. Nous introduirons un tel cycle d'entente avec la communauté.

A la Banque centrale du Bangladesh, les pirates informatiques ont injecté des paiements frauduleux entre le système de back-office et SWIFT Alliance Access. Le contrôle le plus efficace contre une telle attaque est la sécurité des flux de données en back-office (Back-office Data Flow Security). Pourquoi ce point de contrôle n'est-il toujours que recommandé dans le nouveau référentiel et pas déclaré obligatoire?
Nous considérons qu'il s'agit d'un sujet important. C'est pourquoi il fait également partie du cadre de contrôle. Nous sommes convaincus que, à mesure que le référentiel évoluera, il y aura des glissements des «Advisory Controls» en «Mandatory Controls». Nous examinons régulièrement la signification et la pertinence de chaque contrôle, puis envisageons de passer à une mise à niveau en «Mandatory Control».

Et cela sera implémenté dans un prochain release ...
C'est ainsi.

Depuis deux décennies, SWIFT mise du fait de son importance systématique sur la stabilité du système financier mondial sous la supervision des banques centrales du G10. Comment SWIFT rend-elle compte de ses propres efforts de cybersécurité?
Bien entendu, le sujet de la cybersécurité est extrêmement important non seulement pour la communauté, mais surtout pour notre propre sécurité de statut. Cela signifie que nous accordons la plus grande attention à ce thème dans notre entreprise. Dans le même temps, nous avons – et nous continuons à le faire – considérablement investi dans notre infrastructure et notre stratégie cybernétique. Nous nous référons constamment aux normes internationales (par ex. ISO) ainsi qu'aux meilleures pratiques et recherchons où nous pourrions aller encore plus loin. Nous tenons le G10 au courant sur tout ce que nous faisons ici, afin de l'aider à assumer ses responsabilités en matière de gouvernance.

« *Nous savons que les criminels frappent astucieusement les jours fériés ou les week-ends.* »

Marc Hofmann

> **«Si je pouvais souhaiter quelque chose, ce serait que toutes les entreprises sans exception se tournent vers nous immédiatement en présence d'un soupçon d'abus, afin que nous puissions les aider.»**

Selon vous, quels sont en ce moment les principaux obstacles à la garantie de la cybersécurité dans la communauté SWIFT?

Même si ce n'est pas la majorité, beaucoup de nos clients appréhendent encore d'échanger des informations. Certains considèrent comme un avantage concurrentiel de les garder pour eux. Cela concerne en particulier les informations sur des incidents. Si je pouvais souhaiter quelque chose, ce serait que toutes les entreprises sans exception se tournent vers nous immédiatement en présence d'un soupçon d'abus, afin que nous puissions les aider. Ou que nous puissions communiquer des informations anonymisées par notre canal – bien entendu seulement après leur validation – afin d'éviter des dommages à d'autres entreprises. D'après mon expérience, malheureusement, de nombreuses entreprises ne sont pas en mesure d'agir avec nous en cas de suspicion. Tout d'abord, parce qu'elles ne savent tout simplement pas qui contacter en interne en termes de Legal & Compliance pour obtenir une approbation de l'échange d'informations. Et même si cette connaissance existe, cela prend parfois trop de temps pour l'approbation, peut-être des jours, soit parce que les responsables sont en vacances ou du moins pas consultables.

Le deuxième point est que les entreprises peuvent ne pas être en mesure de réagir techniquement. Dans quelques attaques, j'ai vu des criminels détruire une grande partie de l'infrastructure de l'entreprise (par ex. des serveurs, y compris ceux de messagerie) pour effacer leurs traces. Soit ils suppriment des entrées de bases de données, soit ils sont extrêmement destructeurs et chiffrent ou suppriment tout ce qui se présente à eux. En d'autres termes, les clients étaient techniquement incapables de réagir rapidement. En principe, les pirates veulent empêcher ou du moins retarder le rapprochement des paiements entrants et sortants. En dernière analyse, il s'agit d'une course contre la montre. Il n'y a rien de plus important que le temps dans la récupération de ressources. Les pirates le savent aussi et c'est pourquoi ils veulent brouiller les pistes et ralentir les velléités de réaction des lésés.

Interview:
Gabriel Juri & Karin Pache
SIX Interbank Clearing

SWIFT CSP SECURITY CONTROLS FRAMEWORK

Sécuriser le propre environnement	1	Restreindre l'accès à l'Internet
	2	Sécuriser les systèmes critiques envers l'environnement informatique général
	3	Réduire la surface d'attaque et les points faibles
	4	Sécuriser physiquement l'environnement
Connaître et restreindre l'accès	5	Prévenir la manipulation de données d'accès
	6	Gérer les identités séparément des droits
Identifier et réagir	7	Identifier les activités inhabituelles dans les protocoles de système et de transactions
	8	Planifier la capacité de réaction et l'échange d'informations

L’avenir de la sécurité des paiements

La sécurité dans le trafic des paiements préoccupe l’être humain au plus tard depuis l’introduction des pièces de monnaie comme moyen de paiement. A l’ère de la numérisation galopante, les menaces et les exigences de sécurité augmentent de façon exponentielle. De nouvelles stratégies, des outils et des éléments de sécurité sont essentiels dans la lutte contre la cybercriminalité.

Une véritable «course» entre les «bons» et les «méchants» façonne l’histoire de l’argent depuis près de 3000 ans, celle de la monnaie officielle contre la fausse monnaie. Et par conséquent, un peaufinage ad aeternam des éléments de sécurité. Pour la monnaie métallique, citons par exemple le matériel, la couleur, la tranche ou les dimensions. Pour les billets, il s’agit souvent de l’impression en taille-douce, de fils de sécurité (fil d’argent), de filigranes, hologrammes, micro-impression, fluorescence à la lumière UV et infrarouge. Bien que les éléments de sécurité soient de plus en plus sophistiqués, rien n’est si sûr à long terme qu’un faussaire ne puisse les imiter ou les déjouer.

On peut en dire autant de l’histoire de l’Internet: cybersécurité contre cybercriminalité. Les premières connexions informatiques numériques étaient déjà protégées par des mesures techniques et dotées d’éléments de sécurité. En dépit de cela, des attaques de pirates informatiques ont abouti. De nouveaux éléments de sécurité devaient alors être développés. Cela vaut aussi pour l’Internet: la concurrence ne se couche jamais. Non seulement la course se poursuit, elle s’accélère même depuis les débuts.

L’ampleur de la menace cybercriminelle ne cesse de croître à l’ère numérique croissante et de bout en bout. Toute entreprise, toute personne privée peut être la cible de prédilection des cybercriminels. La menace se retrouve dans le vol d’informations, la fraude et le sabotage de la chaîne d’activités. Elle emprunte différents canaux tels que les médias sociaux, l’e-mail, l’Intranet, l’Internet, le téléphone et la lettre. Et elle est le fait de groupes et d’individus très différents, d’initiés et de cybercriminels, de pirates informatiques, de syndicats du crime organisé, d’hacktivistes et d’attaquants à la solde d’un Etat étranger.

Sécurité informatique – combiner des mesures techniques et organisationnelles
Des mesures techniques peuvent réduire les risques d’infection par des logiciels malveillants et accroître la sécurité informatique dans le réseau d’entreprise. Ces mesures incluent la protection antivirus mise régulièrement à jour, la sauvegarde quotidienne de toutes les données, les filtres antispam, le pare-feu et le cryptage des données importantes.

Le maillon le plus faible de la chaîne n’est souvent pas la technologie, mais bien l’utilisateur. Ainsi, en plus des démarches techniques, des mesures organisationnelles s’imposent pour accroître la sécurité informatique. Les mesures d’organisation doivent permettre de définir les responsabilités en matière de sécurité informatique dans l’entreprise. De plus, les collaborateurs doivent être formés, les risques régulièrement examinés et une politique de mot de passe définie pour assurer la sécurité.

Nouveaux éléments de sécurité
Dans la course aux cybercriminels, il existe de nombreux nouveaux éléments de sécurité destinées à préserver l’avantage technologique et à accroître encore la sécurité informatique à l’avenir. Quelques exemples à ce sujet.

– **L’authentification à deux facteurs (2FA)** utilise la combinaison de deux facteurs différents et indépendants pour identifier un utilisateur. 2FA est considérée comme très sécurisée, mais présente l’inconvénient que le jeton correspondant (jeton matériel, carte bancaire ou clé) doit être transporté à tout moment. La **2FA sans jeton** a été développée en tant qu’amélioration et alternative. Cette nouvelle authentification à deux facteurs utilise les smart-

Chasser l'inhabituel en détectant les anomalies.

phones comme jetons. Si donc l'utilisateur veut s'authentifier, il utilise son accès personnel au smartphone et un mot de passe à usage unique (OTP) valide, dynamique et supplémentaire qu'il obtient d'une app ad hoc installée sur ce même smartphone. L'avantage avec cette méthode: un jeton supplémentaire est inutile, car le smartphone est un compagnon de toute façon fidèle de l'utilisateur. Google Authenticator et l'app UBS Access par exemple fonctionnent sur ce principe.

– **La signature électronique distribuée (SED)** sera indispensable dans le futur. Dans ce type de signature, les ordres de paiement sont transférés électroniquement à la banque par le service comptable ou de trésorerie, sans toutefois être comptabilisés dans un premier temps. Les signataires autorisés peuvent vérifier si les ordres de paiement disponibles pour validation sont corrects et quelles signatures ont déjà été fournies ou sont toujours manquantes. L'ayant droit peut désormais signer électroniquement les ordres à exécuter. Ce n'est que lorsque toutes les signatures nécessaires auront été reçues que la banque exécutera les ordres. Si les ordres de paiement empruntent de plus un canal séparé des signatures, la sécurité peut être augmentée à nouveau. Par exemple, l'ordre de paiement pourrait être transféré via EBICS à la banque et les signatures de validation effectuées via l'e-banking. Pour réussir, un cybercriminel devrait alors duper en même temps deux canaux déjà très sécurisés en soi.

– **SwissID – l'identité numérique.** Au quotidien, il est certes facile de prouver son identité en présentant un passeport, une carte d'identité ou un permis de conduire. Sur Internet en revanche, fournir cette preuve devient très compliqué. Une preuve d'identité électronique est ainsi nécessaire dans le monde virtuel, permettant par exemple aux portails en ligne d'identifier et d'authentifier une personne de manière univoque. SwissID est une solution efficace et largement soutenue d'identité numérique en Suisse. Le service gratuit est fourni par SwissSign, une coentreprise composée d'entreprises proches de l'Etat, de sociétés financières, de compagnies

MELANI

Le site Internet de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI (www.melani.admin.ch) géré par la Confédération suisse est destiné aux utilisateurs privés d'ordinateurs et d'Internet ainsi qu'aux petites et moyennes entreprises (PME) suisses. Il contient des informations sur les menaces actuelles et des cas fréquents, ainsi que des documentations, des newsletters et aussi un formulaire d'inscription.

d'assurances et de caisses-maladie. Avec SwissID, les utilisateurs se connectent simplement aux services en ligne suisses, s'identifient, achètent des produits, effectuent des paiements et signent en ligne.

– Un **système de détection d'anomalie (Anomaly Detection System, ADS)** aide à identifier les données anormales problématiques, en considérant par exemple des achats inhabituels ou des bénéficiaires inhabituels comme des transactions potentiellement frauduleuses. La détection des anomalies automatisée côté banque dans les ordres de paiement est une tâche complexe, impliquant des domaines tels que l'apprentissage automatique, les statistiques et l'exploration de données.

Plus de sécurité grâce aux paramètres personnels de paiement et de carte
Avec l'adaptation des paramètres personnels dans les paiements et des cartes, la sécurité des ordres de paiement augmente en supplément. Les clients doivent être en mesure de paramétrer eux-mêmes s'ils veulent être informés, au niveau des mouvements de compte, d'un montant qu'ils ont fixé via leur smartphone. Il sera également de plus en plus possible, dans les systèmes e-banking, de bloquer des paiements et des cartes pour les pays vers lesquels l'argent n'est jamais transféré (géoblocage). En outre, les clients pourront définir des limites de période pour les paiements. Si la limite est dépassée, aucun paiement ne peut plus être saisi dans la période définie. Avec plusieurs comptes, il sera possible de désactiver complètement certains comptes pour des paiements en ligne. Ces comptes seront alors fermés aux virements et transferts de compte à compte. Autre caractéristique se généralisant à l'avenir: les paiements à de nouveaux bénéficiaires devront d'abord être confirmés; en d'autres termes, un destinataire à qui de l'argent n'a encore jamais été transféré devra être confirmé à titre unique pour des raisons de sécurité. Les banques proposeront à leurs clients certaines de ces options en combinaison. Par exemple, il sera possible pour un client de définir que la confirmation des nouveaux bénéficiaires n'est nécessaire qu'à partir d'un certain montant.

eBill – payer les factures en toute sécurité
Avec eBill, les émetteurs de factures peuvent transmettre leurs factures électroniquement directement à partir du logiciel de facturation et les envoyer en toute sécurité et sans rupture de support à l'e-banking de leurs clients sous forme de facture eBill. Les payeurs n'ont plus besoin de saisir les informations de paiement et ne sont plus obligés de numériser les bulletins de versement. En conséquence, aucune erreur de saisie et en revanche un paiement des factures toujours fiable, sécurisé et transparent. Les émetteurs de factures évitent ainsi des dommages liés à la réputation, qui ne sont pas rares avec les factures par courrier électronique dus au spam et au phishing. Etant donné que l'eBill est exempte de ruptures de support et donc supérieure à la facture par courrier électronique, elle devrait probablement prévaloir à long terme en tant que facture numérique et sécure en Suisse.

Peter Ruoss
UBS Switzerland SA

SUR LA VOIE VERS L'E-ID

Le 1er juin 2018, le Conseil fédéral a adopté le projet de loi sur les services d'identification électronique (e-ID). Les utilisateurs d'une telle e-ID doivent pouvoir prouver dans les services en ligne d'entreprises et d'autorités (par ex. achats en ligne, dossier patient électronique, commande d'extrait de casier judiciaire, annonce à la commune, remplissage de la déclaration d'impôt, etc.) qu'ils sont une entité déterminée – et tout cela avec un seul login.

SwissSign Group SA, une coentreprise composée d'entreprises proches de l'Etat (CFF, La Poste Suisse, Swisscom), de sociétés financières (SIX, UBS, Credit Suisse, Raiffeisen, Zürcher Kantonalbank, Entris), de compagnies d'assurances (AXA, Baloise, Helvetia, La Mobilière, Swiss Life, Vaudoise, Zurich) et de caisses-maladie (CSS, SWICA), est dans les starting-blocks. Avec SwissID, elle offre une option simple et sans frais d'identification numérique répondant à toutes les exigences de protection des données et protégeant la confidentialité de ses clients.

Joyaux numériques de la place financière et leur cyberdéfense

La Swiss Value Chain constitue la colonne vertébrale de la place financière suisse. Le fonctionnement harmonieux et efficace de son infrastructure en réseau – qu'il s'agisse du commerce boursier, du traitement des transactions sur titres et du trafic des paiements – est tout aussi essentiel pour l'attractivité de la place financière que sa résilience face aux cyberattaques. En effet, la question n'est pas de savoir si, mais bien quand de telles cyberattaques vont se produire.

La question connexe est de savoir si SIX, l'exploitante de l'infrastructure des marchés financiers entièrement standardisée, automatisée et numérisée, est prête à faire face aux cyberattaques. Des mesures techniques seules – dans le cadre de la «Business Continuity Planning (BCP)» – ne suffisent pas à la tâche.

Ligne de défense proactive

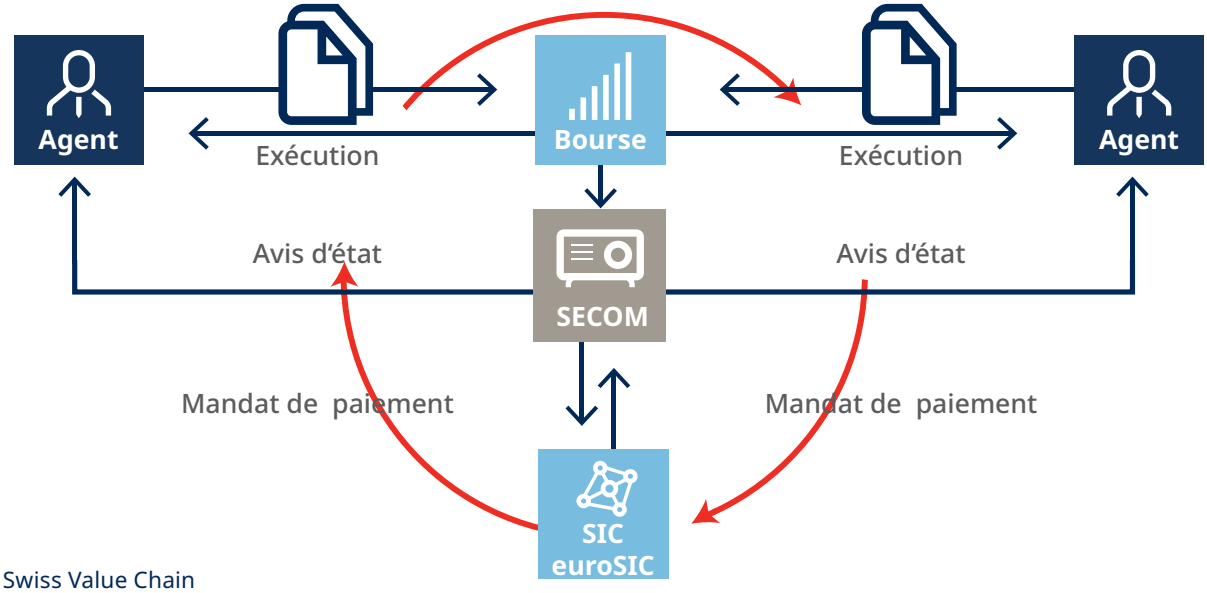
SIX est tenue d'optimiser en permanence les processus de sécurité existants (par ex. BCP, système de contrôle interne). En outre, elle identifie et évalue de nouveaux risques technologiques et, conformément aux meilleures pratiques et aux normes de sécurité mondiales du secteur financier, prend toutes les mesures nécessaires pour se protéger et protéger ses clients dans un environnement en constante évolution. Que le crime organisé ait déplacé ces activités dans le monde en ligne et y cause d'immenses dégâts en recourant à des cyberattaques de plus en plus sophistiquées, tout le monde en parle, mais la prise de conscience de la menace n'est pas encore chose faite au niveau national. Elle nécessite une culture du risque vécue qui ne se fait pas sans autre. SIX promeut proactivement cette culture dans l'entreprise depuis quelque temps déjà. Une connaissance adéquate des risques par chaque individu est indispensable si l'on considère qu'un courrier électronique suspect peut déjà devenir une menace d'importance.

Le premier Security Operations Center cognitif de Suisse

SIX s'est équipée en conséquence sur le plan organisationnel: en janvier 2018, le premier Security Operations

Processus SOC

- Incident management
- Vulnerability management
- Threat intelligence
- Penetration testing
- Forensic analyses
- Red teaming
- Monitoring & detection
- Compliance assurance
- Security analytics
- Use case development
- Security reporting
- Security awareness
- Roadmaps & architecture
- Ambition levels & requirements
- Continuous improvement
- Review & quality control



Swiss Value Chain

Center (SOC) de Suisse a été mis en service, se concentrant sur le Cognitive Computing – à savoir une technologie d'autoapprentissage. Les analystes de la sécurité travaillent ensemble avec l'Operation Monitoring sur place, par équipes 24 heures sur 24. Cela permet d'élargir considérablement les possibilités afin d'accroître durablement le niveau de sécurité, d'identifier les cybermenaces et de protéger ainsi SIX et ses infrastructures de marchés financiers. Sur les milliards de messages de journal, 30 menaces potentielles ou failles de sécurité sont actuellement examinées et traitées par jour.

La cybersécurité en tant que domaine d'activité
SIX accompagne désormais ses clients dans la lutte contre la cybercriminalité. Elle soulage les autres entreprises du développement coûteux et de l'exploitation permanente d'un SOC et fournit les analystes spécialisés requis dans la cybersécurité. En particulier, les petites et moyennes banques et les compagnies d'assurance ont accès à une solution de sécurité maximale que seules les grandes entreprises peuvent développer par elles-mêmes. Les données restent à tout moment chez le client – et toujours en Suisse – seuls les évènements sont transmis pour analyse. En outre, SIX lancera des programmes de formation et de formation continue et encouragera et simplifiera le partage de constatations sur la situation de menace entre tous les intervenants.

Thomas Koch
Head Corporate Security, SIX

MISE EN RESEAU ORGANISATIONNELLE

SIX est un membre actif des communautés de sécurité suisses et échange des notifications de risques ainsi que des informations avec d'autres participants financiers, et reçoit des retours protégeant contre les cybermenaces.

En outre, SIX a lancé cette année le SIX Cyber Hub, une initiative sectorielle, interdisciplinaire et multilatérale. Il est ouvert à tous les participants de la place financière suisse. Le SIX Cyber Hub vise à renforcer la résilience, la coopération, l'échange d'informations et la «confiance numérique» dans la cyberrésilience de la place financière suisse.

FAITS & CHIFFRES

- 1765 cyberintrusions ont été enregistrées dans des entreprises du monde entier en 2017
- 2,6 milliards d'entrées de données ont été volées à cette occasion
- 3,62 millions USD, c'est ce que coûte une cyberintrusion en moyenne à une entreprise
- 94 entreprises suisses ont été victimes d'une cyberattaque en 2017

Protection des données de l'UE aussi pour la place financière suisse

Le règlement général de l'UE sur la protection des données est en vigueur depuis le 25 mai 2018. Que contient-il? Qui concerne-t-il? Et quel impact a-t-il sur la place financière suisse et son trafic des paiements?

Le Règlement Général sur la Protection des Données (RGPD, ou en anglais: GDPR) a été adopté afin d'harmoniser les lois de protection des données des pays européens, d'affirmer la protection des données des citoyens de l'UE et d'assurer la transparence correspondante. Cela permet également de revoir la politique de confidentialité des entreprises et des organisations dans les Etats membres de l'UE.

Qui est concerné par le règlement?
Toutes les entreprises qui traitent des données personnelles de personnes physiques résidant dans l'UE (clients, employés, etc.) doivent mettre en œuvre le règlement indépendamment de leur propre localisation. Le règlement s'applique donc aussi aux entreprises domiciliées en Suisse pour autant qu'elles entretiennent des relations d'affaires avec des résidents de

Des détails sur le RGPD sont disponibles sous www.EUGDPR.org

l'UE ou leur propose des services, mais pas aux personnes domiciliées en Suisse avec des relations d'affaires en Suisse.

Des pénalités de taille
Le non-respect du RGPD peut entraîner des pénalités pouvant aller jusqu'à 4% du chiffre d'affaires annuel ou 20 millions d'euros (le montant le plus élevé s'appliquant).

Incidences sur le trafic des paiements
Le RGPD doit également être mis en œuvre dans le trafic des paiements chaque fois que des données personnelles sont traitées. D'une part, les droits selon le RGPD des personnes physiques doivent être assurés. D'un autre côté, il faut s'assurer que les processus et les systèmes sont conformes aux exigences de protection des données et qu'ils sont largement documentés. Cela concerne la conservation, le traitement et la transmission de données à caractère personnel dans des applications internes à la banque aussi bien que dans le cloud, ce qui implique généralement les activités d'e-banking ou les ordres de paiement et de bourse. Il convient de noter que des identifiants techniques qui ne permettent pas de tirer des conclusions sur des personnes spécifiques, sont appliqués dans les processus middle-end et back-end des banques déjà aujourd'hui.

Consentement implicite inadmissible
Même les prestataires de services et les employeurs qui travaillent uniquement dans la place financière suisse doivent se conformer à la directive de l'UE avec les clients et les employés résidant dans l'UE. Les consentements implicites ne sont pas autorisés. Le client ou l'employé doit accepter explicitement la gestion des données; la croix dans le champ correspondant doit être définie explicitement le cas échéant. L'offre de service ou l'emploi ne peut pas dépendre du consentement en matière de gestion étendue des données.

La loi suisse sur la protection des données est en cours de révision afin de s'aligner sur le nouveau RGPD et s'appliquera en conséquence probablement à tous les clients et employés des prestataires de services et des employeurs suisses.

Manuela Giordano & Alain Hiltgen
UBS Business Solutions AG

LES PRINCIPAUX ELEMENTS DU REGLEMENT REVISE

Protection des données «by design and by default»
Une entreprise traitant des données personnelles doit veiller à ce que la protection des données soit assurée à tous les stades du traitement au moyen de mesures techniques et organisationnelles. De même, une entreprise doit s'assurer que, par défaut, les données personnelles sont uniquement traitées dans le but commercial. Ceci s'applique à la fois au nombre de données collectées et à leur traitement ainsi qu'à la durée de conservation et à l'accès à ces données.

Les droits des personnes physiques
Le règlement confère aux personnes physiques la transparence et l'autorisation d'agir par rapport à leurs données personnelles.

Droit d'accès des personnes concernées
Toute personne a le droit de savoir si, où et dans quel but une entreprise traite des données personnelles. En outre, chaque personne concernée doit pouvoir accéder à une copie des données traitées, en format électronique.

Droit à la portabilité des données
Le RGPD donne aux personnes physiques le droit d'obtenir auprès d'une société les données personnelles qu'elles leur ont fournies dans le cadre de la relation d'affaires.

Droit à l'effacement
Toute personne a le droit d'exiger l'effacement de ses données personnelles et d'arrêter leur diffusion et éventuellement leur traitement par des tiers.

Notification à l'autorité de contrôle d'une violation de données à caractère personnel
Le RGPD exige le signalement des violations de données qui pourraient conduire à un risque potentiel pour les droits et la liberté d'une personne physique. Les personnes affectées doivent également recevoir une information. La communication doit intervenir dans les 72 heures.

Désignation du délégué à la protection des données
Les entreprises qui traitent de grandes quantités de données à caractère personnel dans le cadre de leurs opérations commerciales doivent désigner un préposé à la protection des données doté des pouvoirs appropriés.

Une harmonisation en chasse une autre

Une étape importante a été franchie: à la fin juin 2018, plus de 80% des entreprises suisses avaient converti leur trafic des paiements à la norme ISO 20022. La dynamique soutenue suggère que la conversion sera entièrement atteinte d'ici la fin de l'année. C'est également ce que souligne un sondage représentatif mené par gfs.bern au printemps. Selon ce dernier, 90% des entreprises interrogées ont déjà lancé un projet de conversion et l'auront achevé à la fin de l'année. Un pont est ainsi jeté vers la QR-facture qui sera introduite à la mi-2020.

Selon le sondage de gfs.bern, le succès de la conversion s'explique principalement par les avantages de la norme ISO 20022 en matière de performances, ainsi que par le travail d'information des banques et des entreprises de logiciels. Au cours des derniers mois, elles ont activement soutenu leurs clients dans le travail d'information et de conseil. Quelque 70% des entreprises concernées ont été soutenues par un partenaire externe, 90% ont reçu des informations de leur banque et, parallèlement, elles ont été très satisfaites ou plutôt satisfaites du soutien. Compte tenu de ces chiffres élevés, le travail d'information et l'assistance des banques et des entreprises de logiciels peuvent être considérés comme un facteur clé de succès pour un projet d'infrastructure de cette taille.

Les avantages en termes de performance ont marqué des points

La norme ISO 20022 s'est révélée être une base importante pour l'optimisation des processus financiers clés au cours des derniers mois. 60% des organisations associent la normalisation du trafic des paiements à des avantages. Ce chiffre dépasse nettement les 70% d'autant plus si les paiements sont effectués de manière régulière et fréquente et au fil des progrès du processus de transition. Parmi les avantages les plus fréquemment cités, nous mentionnerons la numérisation des processus d'affaires, la simplification des paiements suisses et étrangers et une moindre sensibilité aux erreurs dues à l'utilisation de l'IBAN. Nous pouvons en déduire que la norme ISO 20022 fait ses preuves dans la pratique. Il

Avantages de la QR-facture

- Faible risque d'erreur, gains d'efficience
- Saisie simple des factures/facturation
- Plus de numérisation, automatisation

60% des organisations voient déjà des avantages dans la QR-facture avant son introduction.

70% des organisations sondées ont entendu parler de la QR-facture.

Source: gfs.bern
Etat: fin juin 2018

Avantages d'ISO 20022

60% des organisations voient des avantages dans la normalisation du trafic des paiements.
Quelque 35% sont pour l'instant sans opinion et seuls 5% voient des inconvénients.

en % des utilisateurs moyennement à fortement concernés
Source: gfs.bern, état: fin juin 2018

ressort de tous les résultats de l'enquête qu'au fur et à mesure que l'expérience quotidienne augmente, les avantages sont perçus plus clairement que cela n'est le cas dans les organisations ayant démarré un projet.

Combler les brèches de conversion
La conversion peut par conséquent être accélérée par la médiation de valeurs de sondages et d'expériences positives. Il est essentiel que d'ici la fin de 2018, tous les clients entreprises aient achevé leur conversion vers la norme ISO 20022. Le respect de cette échéance est important, car le standard DTA en cours jusqu'ici n'est plus soutenu ou développé, voire documenté par SIX depuis début juillet 2018. Il incombe à chaque banque de combler les lacunes dans la migration de ses clients entreprises dans les temps utiles. A défaut de conversion généralisée, la QR-facture ne pourrait pas être introduite, alors qu'elle est déjà considérée comme un élément clé du processus global d'harmonisation.

Attentes élevées dans la QR-facture
70% des personnes interrogées par gfs.bern ont entendu parler de la QR-facture et environ 60% ne lui prêtent que des avantages ou plutôt des avantages déjà avant son introduction. Cette attitude positive consolide la place financière suisse dans ses efforts d'une introduction bien étayée de la QR-facture et d'intégrer dans la prochaine étape les précieuses réactions entrées de la part du marché. A cette fin, une procédure de consultation publique est menée depuis la fin du mois de juillet, dont les résultats seront communiqués à la mi-novembre 2018. Cette procédure garantit que les acteurs du marché peuvent contribuer, que la QR-facture est largement étayée et qu'elle pourra donc être introduite avec succès à partir du 30 juin 2020.

Gabriel Juri
SIX Interbank Clearing

Consultation sur les Implementation Guidelines QR-facture

Les Implementation Guidelines suisses QR-facture (version 1.0 du 27.04.2017) doivent être révisées sur les huit points suivants et adaptées aux besoins actuels du marché.
- Introduction d'une obligation de perforation pour les paiements sur support papier
- Introduction d'un récépissé
- Simplification dans les adresses structurées
- Pas d'indication d'informations structurelles de l'émetteur de factures
- Simplification des combinaisons possibles dans les références structurées
- Pour le moment, pas d'utilisation du champ «Bénéficiaire final»
- Pour le moment, pas d'utilisation du champ pour méthodes alternatives
- Introduction d'une police supplémentaire sans licence pour les utilisateurs non Microsoft

La procédure de consultation s'adresse en premier lieu également aux banques et aux réalisateurs de logiciels ERP qui développent leurs produits et services à partir des Implementation Guidelines suisses QR-facture.

ISO 20022 – introduction réussie

90%
des clients entreprises ont lancé un projet de migration.

Source: gfs.bern
Etat: fin juin 2018

80%
des clients entreprises ont terminé leur migration et transféré 80% du volume de transaction.

Source: SIX Interbank Clearing SA
Etat: fin juin 2018

POUR EN SAVOIR D'AVANTAGE:

Plus sur la cybersécurité
dans l'édition 73 du décembre 2017

Plus sur la Swiss Value Chain
dans l'édition 68 du septembre 2016

Plus sur la conversion vers la norme ISO & la
QR-facture dans l'édition 74 du mars 2018