وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ م إ

BULLETIN D'INFORMATION DES ACTUALITES INTERNATIONALES
DANS LE DOMAINE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

Bulletin d'information : Bon à savoir (n°41)

Cybercriminalité

En quelques mots

La cybercriminalité se définit communément comme toute action illicite visant l'intégrité d'un site informatique déterminé, ou bien menée à l'aide d'un outil informatique. Cette définition se décline selon l'utilisation faite du médium informatique. En effet, soit ce dernier est utilisé par le criminel comme outil d'un délit ou d'un crime conventionnel (escroquerie, menace…etc), soit l'ordinateur est la cible-même visée par le criminel (vol, utilisation frauduleuse ou encore destruction de données…etc).

Attaque de type conventionnel

Ce type d'attaque utilise comme support, les technologies associées aux réseaux d'information et de communication. Généralement, le but est de profiter de la crédulité des utilisateurs pour leur soustraire des informations confidentielles et s'en servir ensuite de manière illégale.

Il existe toute sorte d'infractions dites conventionnelles, et leur nombre augmente continuellement. Les plus classiques étant :

- extorsions de fond;
- fraude liée à la carte de crédit;
- menaces répréhensibles diverses, de type «vengeance»;
- fraude commerciale;
- abus de confiance et escroqueries diverses;
- détournements de mineurs;
- usurpation d'identités.

Il s'agit en effet de l'ensemble des crimes et délits « traditionnels » qui se transpose sur les réseaux numériques d'information et de communication.

Ces attaques sont essentiellement motivées par la cupidité (la recherche d'un gain quel qu'il soit : financier ou encore matériel) ou des comportements immoraux, malsains et maladifs (telle que la pédophilie, les réseaux de prostitution, le racisme, révisionnisme...etc).

Attaque de type technologique

Ce type d'attaque a fortement évolué depuis son apparition ; elle exploite essentiellement les nombreuses vulnérabilités de l'outil informatique. Les attaques les plus répandues sont :

- l'installation de programmes espions,
- l'installation de programmes pirates,
- les intrusions,
- les détériorations diverses,
- les destructions de sites,
- le vol d'informations,
- les dénis de service sur des sites,

- le rebond à partir de sites informatiques victimes…etc.

Une attaque de type technologique peut être fondée par l'une, ou la combinaison de plusieurs des motivations suivantes :

- stratégiques (vol d'informations sensibles classifiées),
- idéologiques (transformation de pensées prédominantes ou de courant d'idées en actes illicites),
- terroristes (visant à déstabiliser un ordre établi),
- cupide (recherche d'un gain financier ou matériel),
- ludique (pour s'amuser ou par loisir),
- vengeur (réaction à une frustration quelconque).

Elles visent soit la confidentialité, l'intégrité ou encore la disponibilité d'un système informatique (voire une combinaison des trois).

Pour déployer des logiciels malveillants, le pirate informatique se focalise généralement sur une des alternatives suivantes:

Attaque opportuniste

Les attaques opportunistes sont des attaques qui ne sont pas directement dirigées vers des gens ou organisations en particulier, mais dont le but est d'obtenir autant de victimes que possible quelles qu'elles soient. La plupart des gens et organisations sont soumis à cette menace.

Voici quelques étapes courantes de ce genre d'attaques:

La création ou l'achat d'un logiciel malveillant

Un logiciel malveillant donne à l'attaquant un outil de contrôle absolu sur les ordinateurs de ses victimes. De ce fait il constitue la pierre angulaire de beaucoup d'attaques opportunistes.

L'envoi ou location d'un service de SPAM

Atteindre une large population de victimes ne se fait pas sans une bonne distribution. Que se soit pour une arnaque ou pour l'infection d'ordinateurs il faut pouvoir atteindre un large public. L'envoi d'e-mails ou le SPAM sur réseaux sociaux peut-être une très bonne méthode.

La création de sites malicieux et l'infection de sites existants

Avoir une présence sur la toile n'est pas seulement important pour les organismes légitimes mais aussi pour les cybercriminels. Création de sites de phishing, publicités, arnaques, pages contenant un exploit qui infectera les ordinateur des internautes,...

Attaque ciblée

Les attaques ciblées peuvent être très difficiles à contrecarrer. Tout dépend de l'énergie et temps déployés par le groupe de malfaiteurs. En général une attaque ciblée bien organisée a de grandes chances de réussir quand l'attaquant se concentre exclusivement sur sa victime.

Ces attaques peuvent se dérouler en différentes étapes. Ci-dessous vous trouverez certaines étapes importantes de ce type d'attaque.

La récolte d'informations

Avant d'attaquer une cible particulière, le pirate procède généralement à un relevé de toute information pouvant mener à une cartographie (photographie détaillée) de l'organisation ou de l'individu qu'il vise. Une liste de numéros de téléphones ou d'e-mails publiée sur Internet peut être décisive dans l'attaque d'une organisation.

Le balayage du réseau

Parfois les pirates testent les systèmes cibles pour vérifier s'ils sont actifs, et déterminer s'il présentent des failles. Cette opération peut déclencher des alarmes et ne donne souvent pas de résultats probants; de ce fait elle est réservée à certains champs d'application bien précis uniquement.

L'ingénierie sociale

Souvent l'attaque sur les systèmes informatiques sera impossible car trop protégés. Dans le cas de l'ingénierie sociale ('social engineering'), plutôt que d'utiliser une faille technique du

système, le malfaiteur utilisera plutôt la crédulité de l'être humain. Il tentera par exemple de se faire passer pour quelqu'un d'autre, en relation avec l'utilisateur, afin d'avoir accès à des informations tel qu'un mot de passe par exemple. Ce scénario est devenu une pratique courante ; les pirates agissent souvent par pression psychologique sur un individu, ou en invoquent l'urgence, pour obtenir rapidement les renseignements souhaités.

Le fichier piégé

Souvent le malfaiteur tentera une attaque par e-mail piégé, contenant par exemple un « cheval de Troie » dans un programme quelconque, qui pourra lui permettre, une fois activé par l'utilisateur, de prendre contrôle à distance sur l'ordinateur de la victime.

https://www.cases.lu/cybercriminalite.html

La protection du SI : Un enjeu vital pour l'entreprise

Dans l'entreprise, la sécurité du système d'information s'appuie sur trois piliers : la disponibilité du système, l'intégrité des données et leur confidentialité. L'entreprise doit donc tout mettre en œuvre pour le protéger. Si son datacenter est connecté à un réseau d'opérateur, le trafic qu'elle reçoit est censé être sain, expurgé de menaces. En revanche, Internet est porteur potentiel de tous les dangers, puisque personne ne le contrôle. Dans le Cloud, c'est au prestataire de garantir la sécurité des données. Quelle que soit la configuration retenue, l'entreprise a donc tout intérêt à disposer de sa propre solution de protection pour faire face à toute éventualité.

Les moyens d'attaque du SI de l'entreprise ne manquent pas, qu'il s'agisse de son datacenter ou de son cloud privé. Il est donc nécessaire de :

- interdire l'accès aux personnes non autorisées ;
- surveiller le trafic en permanence, même si aucune anomalie n'est constatée ;
- recourir au chiffrement pour protéger la confidentialité des données, surtout dans le Cloud.

Contrôler les accès

L'une des briques essentielles de la protection du SI réside dans le contrôle d'accès. C'est l'IAM (Identity and Access Management). Son but est de restreindre l'accès au SI aux seules personnes autorisées, ce qui nécessite le stockage de leurs identités. Celles-ci sont souvent hébergées dans un annuaire tel que l'Active Directory de Microsoft ou une solution ouverte telle que LDAP (Lightweight Directory Access Protocol).

Parer aux attaques par déni de service

La disponibilité du SI peut être gravement compromise suite à des attaques par déni de service distribué (ou DDOS). À l'insu des utilisateurs, les cybercriminels prennent le contrôle de centaines, voire de milliers de PC, qui deviennent des PC zombies et lancent massivement des attaques qui submergent le réseau et des équipements (par exemple un site Web) ou même un serveur DNS (Domain Name Server ou annuaire d'Internet). L'entreprise peut se retrouver paralysée, par exemple s'il s'agit d'un site d'e-commerce. Ce type d'attaque basique est en constante augmentation. Ainsi, Akamai (société américaine spécialisée dans les serveurs de cache) a constaté qu'elles ont augmenté de 125% entre le premier trimestre 2015 et le premier trimestre 2016. Ces attaques intervenant souvent aux niveaux 3 et 4 du modèle OSI (réseau et transport), les pare-feu et les répartiteurs de charge sont en première ligne pour les contrer grâce à des règles de filtrage ; il existe en compléments des solutions spécialisées dans la lutte anti-DDOS qui s'applique au cœur du réseau de l'opérateur pour contrer les plus grosses attaques, ou sur Site pour endiguer les attaques DDOS pernicieuses dites « applicatives ».

Surveiller le trafic en permanence

Ce ne sont pas les seuls dangers qui guettent le SI. Sans s'attarder sur les risques que font courir à l'entreprise les utilisateurs eux-mêmes, par malveillance ou insouciance, les programmes pernicieux sont particulièrement dangereux. D'autant plus que certains sont inconnus des systèmes de protection (attaque 0 Day). Ils se glissent dans le trafic applicatif normal (parfois en plusieurs paquets), profitent de failles dans les systèmes d'exploitation ou dans les applications et infectent le SI. Les pare-feu de nouvelle génération, qui travaillent au niveau applicatif, sont en capacité de pouvoir les détecter et les bloquer. Mais ce n'est pas toujours suffisant. Aussi les fournisseurs de solutions de sécurité fournissent de nouveaux outils tels que les sondes applicatives (sonde IPS)**,** qui analysent constamment le contexte à la recherche de paquets, anodins pris individuellement, mais virulents lorsqu'ils se combinent. En cas de doute sur la dangerosité de certains paquets, il est possible de se tourner vers une base de connaissances mondiale que certains éditeurs mettent en œuvre et qui héberge tous les cas d'infections récemment détectés.

Chiffrer ses données

Le chiffrement est un allié particulièrement efficace pour garantir la confidentialité des données. Même subtilisées, elles restent inutilisables. Cette précaution vaut particulièrement dans le Cloud, non seulement lors des phases de transmission, mais même pendant le stockage. Aussi est-il recommandé que l'utilisateur crypte lui-même ses données. Un autre avantage de cette solution concerne l'effacement des données dans le Cloud. L'entreprise n'est jamais certaine que le prestataire ait effectué l'opération demandée. Si les données sont chiffrées, il suffit de détruire la clé de cryptage pour les rendre définitivement inutilisables.

https://www.sfrbusiness.fr/room/securite/protection-si-vital-entreprise.html

Le « Dark Net »

Lorsqu'on parle de Dark Net, on parle de menace mais aussi de moyen de communication utile.

Qu'est ce que le Dark Net?

Le Dark Net a été créé par le gouvernement américain il y a une dizaine d'années. À l'origine il avait pour objectif de sécuriser les conversations internes, mais par la suite le gouvernement s'est rendu compte que cela pouvait intéresser d'autres organisations en donnant la possibilité de protéger les libertés individuelles de chacun. On peut ainsi dire que la portée de cette invention a dépassé ses créateurs.

Le Dark Net est également appelé Deep Web, Internet profond, Internet clandestin, ou encore Internet parallèle. C'est un monde parallèle à notre internet classique, un monde où l'on peut tout acheter : armes, drogues, faux billets, vidéos pornographiques etc. L'internet clandestin, est une zone qui échappe à tout contrôle (on l'appelle la zone « libre ») étant donné qu'on y effectue ses recherches via des variations des moteurs classiques tels que Google, Yahoo etc. Pour accéder à cet internet libre, il est nécessaire de télécharger un programme.

Comment y accéder ? Quel en est l'intérêt ?

Pour accéder au Deep Web, il faut donc télécharger un logiciel nommé « TOR » (The Onion Router). Ce logiciel permet d'accéder aux sites contenus dans le Deep Web, et également de conserver un certain anonymat.

La conservation de cet anonymat est possible puisqu'en téléchargeant TOR on obtient des noms de domaines en .onion.

Une fois le logiciel TOR téléchargé il existe des « moteurs de recherches » (équivalent de Google Search) qui permettent d'accéder aux « Darks Net Markets » afin d'y acheter des produits (armes etc.) ou services (services de tueurs à gages, forums de recrutement pour des

braquages etc.). Il suffit de taper le nom du market sur lequel on souhaite aller, la méthode de recherche est la même que sur un moteur de recherche classique.
L'intérêt du Deep Web réside dans l'anonymisation de notre identité. En effet en passant par le programme TOR, notre connexion internet transite d'un serveur à un autre ce qui empêche toute localisation. De cette manière, si j'envoie un message de France, je peux être localisée comme résidant aux USA.

Par quel moyen est-il possible d'effectuer des achats de marchandises ou de services sur le deep web ?

Sur le Dark Net la monnaie ne peut pas être la carte bleue puisque, pour rester dans l'anonymat il faut une monnaie intraçable (or la carte bleue localise tout achat) telle que le Bitcoin.
La monnaie utilisée sur le deep web est donc le Bitcoin. Il s'agit d'une monnaie légale virtuelle qu'il est possible de se procurer sur des sites internet légaux spécialisés (équivalent aux bureaux de change). Les euros dépensés légalement sont retranscrits en Bitcoins. Cette monnaie permet l'accès à un portefeuille virtuel.
Il faut savoir que le Bitcoin permet de faire des achats légaux ET illégaux, et que cette monnaie est de plus en plus surveillée puisqu'elle est l'un des outils permettant de blanchir de l'argent (mais ceci est une autre histoire).
Il est également intéressant de noter qu'il est possible de garantir ses achats en souscrivant sur certains « markets sites » des « assurances », qui permettront de rembourser le produit ou une partie dans le cas ou celui-ci ne serait pas livré.
Le Deep Web est vu comme dangereux du fait de l'anonymat, de la population éclectique utilisatrice, et des variétés de transactions qui peuvent y être faites. En effet il n'y a pas de limite à ce que l'on peut acheter sur le Dark Web et c'est là tout l'aspect dérangeant de l'internet parallèle. Le problème est donc l'anonymisation totale de transactions qui peuvent être illégales. C'est la raison pour laquelle récemment, le gouvernement français a souhaité couper tout réseau WI-FI ouvert, bloquer l'accès aux réseaux d'anonymisation (empêcher le téléchargement de TOR), et la fourniture des clés de chiffrement des messageries sous couvert de la sécurisation face à l'accroissement des réseaux de terroristes sur le Deep Web.
En effet, cette volonté de sécuriser l'Etat français au détriment de nos libertés fondamentales s'est posée en raison des évènements récents liés au terrorisme. Récemment la gendarmerie s'est aperçue que certains groupes terroristes s'étaient formés via le Dark Net.
http://www.juristesdunumerique.fr/2016/01/25/le-dark-net/

Les nouveaux modes de cyber-escroquerie

Les attaques de systèmes informatiques par DDoS (saturation des serveurs) se multiplient. Quelle stratégie adopter pour éviter cette puissante cybecriminalité? Par Adrian Bisaz, Vice President Sales EMEA de Corero Network Security
« Allo ? Ici le commissariat, on vient de fracturer votre bureau, merci de venir vérifier si on ne vous a rien volé, toutes affaires cessantes ». Voilà une manœuvre de diversion classique, qui permet aux cambrioleurs de profiter de votre absence certaine pour pénétrer chez vous et faire main basse sur vos biens les plus précieux.
Un type d'attaque équivalent existe dans le cybermonde. Le DDoS (envoi à un serveur d'un grand nombre de requêtes pour le "planter") remplace le faux coup de fil en détournant l'attention des professionnels du réseau et de la sécurité qui se précipitent alors pour contrer l'attaque par déni de service.

Comment une attaque DDoS peut-elle masquer un vol de données ?

Utiliser le déni de service pour faire diversion est à la fois simple et redoutable. Pendant que l'entreprise est occupée à repousser l'attaque, les cybercriminels ont le loisir de contourner la sécurité affaiblie pour voler des informations monnayables ou stratégiques. Et les cas de diversion se multiplient, tant la méthode est efficace. Lorsqu'une entreprise est attaquée, tous les yeux et toutes les alertes se focalisent sur l'attaque. Il ne reste que peu de personnes et moins de ressources pour maintenir la protection du système d'information. L'attaque distrait les experts de la sécurité, occupe les systèmes de sécurité, différant ainsi l'examen de nouvelles alarmes. Les voleurs ou les pirates ont alors le loisir d'intervenir à partir de comptes à privilèges, par exemple pour détourner des fonds dans une banque, exfiltrer des données ou installer un système espion qui sera utilisé plus tard.

Surveiller les attaques par DDoS

Pour de nombreux observateurs, les outils étant faciles à obtenir sur le marché clandestin du piratage, ce type d'attaque va encore se développer dans les mois qui viennent. Pour les contrer, les entreprises doivent rester vigilantes et accroître leur protection.

L'an dernier, diverses attaques DDoS, dirigées contre les institutions financières ont servi de couverture à des fraudes. Plusieurs banques ont été victimes de virements non autorisés. Les cyber-malfaiteurs prennent le contrôle du système de transfert monétaire, faisant main basse sur les avoirs des clients ou détournant des ordres à leur profit. Une attaque par DDoS est alors lancée, avant ou après le transfert de fonds, empêchant que la banque puisse identifier rapidement la transaction frauduleuse.

Subissant un flot d'attaques, les institutions financières en pointe cherchent à accroître leur protection et unissent leurs efforts pour mieux endiguer le fléau. Face à l'ampleur des attaques par déni de service distribué, les banques n'ont en effet guère le choix. Elles doivent prendre des mesures vigoureuses.

Former le personnel de l'entreprise

C'est un fait malheureusement indéniable : c'est le plus souvent une erreur interne qui permet l'intrusion. Informer les salariés des ruses utilisées par les cyber-délinquants est donc essentiel. Le clic sur un lien ou l'ouverture de la pièce jointe d'un e-mail provenant d'une personne inconnue peut être le point de départ d'un processus qui sera difficilement maîtrisable. Le phishing est aussi un moyen efficace pour une personne mal intentionnée de placer un logiciel malveillant dans un système et de voler des informations. Il faut aussi sécuriser absolument toutes les connexions au réseau de l'entreprise et aux informations de du système depuis un ordinateur, une tablette ou un smartphone personnel...

Enfin, il convient de surveiller les comptes à privilèges, les connexions et les activités qui se produisent en dehors des heures de bureau. L'examen des journaux de sécurité permet de déterminer si des activités suspectes ont eu lieu avant, pendant ou après l'attaque. Mais il faut aller encore plus loin et mettre en place une solution anti-DDoS, contrant les attaques du réseau et éliminant le mauvais trafic avant qu'il n'atteigne d'autres parties de l'infrastructure .

Une première ligne de défense

Les solutions de sécurité traditionnelles comme les pare-feu et les IPS se révèlent malheureusement parfaitement inefficaces face aux cyber-menaces avancées. Elles sont d'ailleurs souvent elles-mêmes la cible d'attaques. C'est pour cette raison qu'il est nécessaire de déployer une première ligne de défense entre Internet et le réseau de l'entreprise, construite pour résister aux cyber-menaces modernes, assurant ainsi la continuité des activités et des services. Les interruptions ou blocages de service que provoquent les attaques peuvent avoir un coût très élevé selon le type d'activité en ligne. Elles occasionnent une perte de productivité mais altèrent aussi fortement l'image de l'entreprise.

La première ligne de défense offre une protection sans interruption contre les cyber-menaces qui évoluent en permanence. Elle arrêtera un large éventail d'attaques DDoS et de cyber-menaces de nouvelle génération, sans dégrader les performances de l'entreprise. Il faut en

effet une protection maximale des actifs informatiques critiques tout en autorisant un total accès pour les utilisateurs légitimes et aux applications. En écartant les menaces des DDoS, la sécurité du réseau répond aux exigences de protection de l'entreprise moderne et conserve le patrimoine numérique en évitant les fuites de données. Il est ainsi possible de contrer la cupidité des cybercriminels utilisant les attaques DDoS pour détourner des fonds ou dérober des informations monnayables ou des données sensibles.

La prévention est la vraie bonne méthode

Contrer une attaque identifiée, en analyser les effets, remettre le système affaibli en état de rendre à nouveau les services requis est indispensable, et c'est le rôle des équipes d'experts et de maintenance sécurité. Mais cette intervention technique s'effectue quand le mal est déjà fait, et le ver peut-être dans le fruit. La prévention par la formation, la protection par une ligne de défense qui agit avant que l'attaque n'atteigne son but, laissant aussi les pare-feu et les IPS jouer pleinement leur rôle, voilà sans aucun doute la méthode la plus appropriée. Pour qu'une simple attaque DDoS ne soit pas le début d'une cascade de phénomènes plus graves pour l'entreprise.

http://www.latribune.fr/opinions/tribunes/20140403trib000823519/les-nouveaux-modes-de-cyber-escroquerie.html

Le protocole bancaire SWIFT victime de cyber fraude

Suite à la récente cyber attaque la Banque du Bangladesh, l'organisme SWIFT vient de reconnaître que son logiciel a été utilisé pour cacher des preuves de transferts frauduleux.

SWIFT (Society for Worldwide Interbank Financial Telecommunication), le réseau financier mondial que les banques utilisent pour transférer des milliards de dollars chaque jour, vient d'avertir ses clients "d'un certain nombre de récents incidents de cybersécurité" sur son réseau : les attaquants ont utilisé son système pour envoyer des messages frauduleux.

Cette révélation intervient alors que les autorités du Bangladesh continuent leur enquête sur le vol de 81 millions de dollars en février dernier. Le transfert litigieux a transité d'un compte de la Banque du Bangladesh vers la New York Federal Reserve Bank. Un des enquêteurs, Mohammad Shah Alam, du Forensic Training Institute du Bangladesh, a déclaré à Reuters que la Banque du Bangladesh était une cible facile pour les cybercriminels car il n'y avait pas de pare-feu et que par ailleurs des commutateurs d'entrée de gamme étaient utilisés pour connecter les systèmes informatiques de la banque à SWIFT.

5 paiements frauduleux sur 35 ont été autorisés

Les chercheurs en cyber-sécurité qui travaillent sur ce hold-up ont expliqué le mois dernier qu'un logiciel malveillant avait été installé sur les systèmes informatiques de la Banque du Bangladesh. Ce malware a permis aux attaquants de se dissimuler avant de prendre l'argent. Un rapport interne de la Banque du Bangladesh mentionne que la Réserve Fédérale a été négligente : elle a validé les fausses transactions. Le rapport parle de «faute majeure». Il indique également que 5 paiements frauduleux sur 35 ont été autorisés (pour un total de 951 millions de dollars), et que des entités situées aux Philippines et au Sri Lanka ont reçu une partie des fonds volés. Et c'est une faute d'orthographe commise par les cybercriminels qui a empêché 20 autres millions de dollars de disparaître en plus des comptes de la Banque du Bangladesh.

Ce vol a provoqué la démission du responsable de la Banque du Bangladesh, Atiur Rahman, 64 ans. Il n'avait pas jugé bon d'informer le ministre des finances du Bangladesh, A M A Muhith, de l'incident. Ce dernier avait appris cet évènement dans la presse étrangère.

SWIFT a reconnu que l'attaque incluait la modification des logiciels SWIFT sur les ordinateurs de la banque pour dissimuler les preuves de transferts frauduleux. "SWIFT est au

courant d'un certain nombre d'incidents de cyber récents dans lesquels des personnes malveillantes dans l'entreprise, ou des pirates externes, ont réussi à envoyer des messages SWIFT depuis les back-offices, PC ou postes de travail des institutions financières connectées au réseau SWIFT" avertit l'organisme dans une message d'avertissement à ses clients.
L'avertissement, émit par SWIFT via une alerte confidentielle envoyée sur son réseau lundi, ne donne ni le nom des victimes ou le montant des sommes dérobées. SWIFT a également publié une mise à jour de sécurité pour le logiciel que les banques utilisent pour accéder à son réseau.

SWIFT : 3 000 institutions financières, 11 000 banques

Cette mise à jour doit sécuriser son système vis à vis du malware que les chercheurs de BAE Systems soupçonnent avoir été utilisé dans le hold-up de la Banque du Bangladesh. Les preuves collectées par BAE suggèrent que les pirates ont manipulé le logiciel Alliance Access de SWIFT, que les banques utilisent pour s'interfacer avec la plate-forme de messagerie de SWIFT, afin de brouiller les pistes. BAE a cependant mentionné ne pas pouvoir expliquer comment les commandes frauduleuses ont été créés et poussés à travers le système. SWIFT a cependant fourni des éléments sur la façon dont tout cela est arrivé. L'organisme explique que le modus operandi était similaire dans toutes les opérations frauduleuses. Les agresseurs ont obtenu des informations d'identification valides et ont pu créer et approuver des messages SWIFT.
SWIFT (Society for Worldwide Interbank Financial Telecommunication) est une coopérative détenue par 3 000 institutions financières. Sa plate-forme de messagerie est utilisé par 11 000 banques et autres institutions à travers le monde et est considéré comme un pilier du système financier mondial.
http://www.zdnet.fr/actualites/le-protocole-bancaire-swift-victime-de-cyber-fraude-39836064.htm

Soft law

La normalisation mondiale est rarement contraignante à ses débuts, c'est sans doute la raison pour laquelle les Français et les Européens continentaux, habitués à la force du droit positif, en tiennent trop peu compte» (Eric Dénécé et Claude Revel). Une soft law, désigne l'ensemble des textes de droit international non contraignants et pouvant être librement interprétés, mais qui s'appliquent sous la pression internationale, sous couvert de protection de l'intérêt général.
Le soft law, terme anglo-saxon aussi dit «droit mou», est un ensemble de règles dont la « juridicité » est discutée, le soft law consistant en des règles de droit non obligatoires. Néanmoins, l'on retrouve le soft law en droit international, notamment en droit de l'environnement, mais aussi dans les constitutions (la nature même des droits-créances) et les lois contemporaines. Un texte relève du soft law quand il se contente de conseiller, sans poser d'obligation juridiquement sanctionnée. Le soft law consiste donc en des textes de droit non contraignant et pouvant être librement interprétés par les Etats. La notion de soft law va donc à l'encontre de la conception du droit de Jean-Jacques Rousseau, pour qui la loi n'a de sens que si elle pose des obligations juridiques assurées. Le soft law laisse au juge la liberté de décider si une disposition est obligatoire ou non. L'aspect non juridique du soft law réside dans le fait qu'il repose sur des sources non législatives et non réglementaires telles que les déclarations de politique en matière d'éthique, les communiqués, les lignes directrices d'organismes professionnels ou para-gouvernementaux, mais aussi sur les programmes d'action ou les déclarations de principe de différentes organisations internationales.

Le soft law se voit souvent imposé par des organismes privés comme publics qui prétendent agir pour la préservation de l'intérêt général. Cet angle d'approche leur confère une certaine légitimité. Les organisations non gouvernementales peuvent être à l'origine de documents relevant du soft law. A titre d'illustration, l'on peut citer le Global Compact, également dit «Pacte mondial» texte qui défini notamment des mesures d'ordre environnementales et sociales, qui fut proposé à l' approbation aux entreprises multinationales en 2000 par le secrétaire général de l'Organisation des Nations Unies. L'adhésion aux principes du Global Compact relève d'une démarche volontaire des entreprises, qui peuvent par la suite améliorer leur image en arguant de leur engagement en faveur d'un développement plus équitable. Le soft law découle assez naturellement du common law anglo-saxon qui laisse une large place à l'interprétation et à la négociation, se différenciant ainsi du droit romain qui fixe un cadre précis aux décisions judiciaires et pratiques des affaires. Le caractère non contraignant du soft law pose problème dans la mesure où il s'étend aux organisations internationales, ce droit modulable est à la merci de l'interprétation de chaque Etat ou gouvernement. L'absence de dimension normative nuit à la fiabilité des mesures prises, notamment de traités, ou du Protocole de Kyoto. Certes, la liberté d'action des participants permet une plus grande universalité du projet, chacun s'impliquant suivant ses capacités. Cependant, il peut en résulter un manque d'efficacité et de cohérence.
https://portail-ie.fr/resource/glossary/90/soft-law

L'usage du *soft law* dans le système juridique international

L'usage du *soft law* dans le système juridique international et ses implications sémantiques et pratiques sur la notion de règle de droit
Cet article propose une réflexion autour du *soft law* et de son usage croissant dans les pratiques internationales. En vue de saisir les raisons du déploiement du *soft law*, l'idée d'une graduation de la « légalisation » au niveau international est mise en avant. Après avoir essayé d'identifier ces actes du *soft law*, l'attention se porte sur leur « juridicité atténuée » qui constitue leur principale spécificité sur le plan conceptuel. Les actes du *soft law* se distinguent des actes conventionnels à caractère contraignant du droit international par le fait qu'ils n'ont pas nécessairement ni immédiatement un caractère juridique, et par conséquent, ne sont pas forcément contraignants.
Le *soft law* se particularise aussi, du point de vue de la pratique, par les différents rôles qu'il remplit par rapport au droit dur. Son usage est favorisé par son caractère « allégé » sur le plan procédural et par sa faculté d'extension de la marge d'action gouvernementale au niveau international.
Enfin, la partie conclusive insiste sur les conséquences sémantiques que l'usage du *soft law* entraîne concernant la notion de la règle de droit. À la conception unifiée et hiérarchisée du droit se substitue une conception « éclatée » du droit où la contrainte n'est plus un élément constitutif, mais fonctionnel de l'ordre juridique international.

Gagner la guerre de la « soft law »

La création des règles de droit n'est plus l'apanage des seuls Etats. Elle se décide dans des enceintes discrètes où se retrouvent fonctionnaires, entreprises, ONG, experts, dans un jeu subtil d'influence.

La « soft law » – la « loi molle » ou « droit souple » – ce sont ces normes élaborées par consensus par des acteurs privés (ONG, grandes entreprises, organismes professionnels…) et qui s'imposent au monde entier par le poids économique ou technique de leurs auteurs. Ainsi, la Société financière internationale, filiale de la Banque mondiale, définit les normes environnementales et sociales auxquelles sont soumises les entreprises.
Et dans la guerre de la « soft law », l'Europe, et singulièrement la France, perd bataille sur bataille. L'Europe a reconnu l'une de ses défaites, sur les normes comptables, en 2010 (1). Mais elle est restée plus discrète sur son échec, dans les années 80, sur les normes de régulation des télécommunications (2). Pourquoi de telles défaites ? Pour les acteurs européens, et français plus encore, les normes ne sont pas des outils stratégiques mais seulement techniques qui appellent alors des propositions techniques. La défaite tient alors à un manque de profondeur de pensée. De plus, les acteurs français ne comprennent pas ces débats : pour eux, les règles de droit se décident dans des assemblées politiques, dans des débats conflictuels et non dans des enceintes privées, par consensus.
D'autres combats, incertains, sont en cours, comme celui de l'exception culturelle (3). Alors voici un modèle permettant d'agir demain avec efficacité :
– Première étape, s'atteler à la détection des signaux faibles qui permet, très en amont, de deviner l'émergence d'un possible débat de normes (4). Les institutions concernées (administrations, fédérations professionnelles, think tanks…) peuvent alors définir les objectifs à atteindre, puis les traduire en textes techniques (5). De quoi participer avec force à la configuration du débat.
– Deuxième étape, le choix des experts qui portent les textes. De très haut niveau et disponibles, ils affichent, certes, leur neutralité envers les positions de leur pays. Mais rien ne les empêche de ne pas perdre de vue la philosophie globale précédemment définie.
– Troisième étape, le pilotage des discussions en proposant des sujets bien ciblés pour se voir attribuer la présidence du groupe de travail chargé de les traiter.
Tout est donc une affaire de préparation en amont, d'information. Voilà ce qui permet de peser fortement dans ces enceintes discrètes de la « soft law » qui créent une part essentielle du droit économique international.
http://www.hbrfrance.fr/chroniques-experts/2015/07/7769-comment-gagner-la-guerre-de-la-soft-law/

Le Conseil d'État s'attaque à la "Soft law"

Par deux arrêts de l'Assemblée du contentieux en date du 21 mars 2016, n° 368082 et n° 390023, le Conseil d'État juge recevables les recours dirigés contre un communiqué de presse de l'Autorité des marchés financiers et une prise de position de l'Autorité de la concurrence. Cette évolution ouvre de nouvelles perspectives pour les praticiens du droit ainsi que pour les administrés, notamment les entreprises.
Traditionnellement, pour être recevable, le recours pour excès de pouvoir doit être dirigé contre un acte faisant grief. Un acte administratif est réputé faire grief lorsqu'il produit par lui-même des effets juridiques, qu'il modifie l'ordonnancement juridique, qu'il atteint les droits et obligations des administrés. Un acte qui ne présente aucun caractère exécutoire ne fait pas grief. Il en est de même de la décision qui n'intervient que dans le cadre d'une procédure d'élaboration d'une décision ultérieure, il s'agit alors d'un acte simplement préparatoire.
Première évolution, selon sa jurisprudence issue de la décision Institution Notre Dame du Kreisker du 29 janvier 1954, seules les circulaires à caractère réglementaires faisaient grief et étaient susceptibles de recours. Par sa décision Duvignère, le Conseil d'État a pu considérer

que font grief les circulaires comportant une interprétation impérative à caractère général (CE Section, Duvignères du 18 décembre 2002).
Autre jurisprudence à souligner, par décision du 11 octobre 2012, n° 357193, le Conseil d'État se prononce sur le régime des avis de l'autorité de la concurrence en jugeant que ces derniers sont susceptibles de constituer des actes administratifs faisant grief.
Ainsi, le Conseil d'État a construit progressivement une jurisprudence sur l'appréhension du droit souple par le juge administratif. Celle-ci tend à atténuer la rigueur du principe selon lequel seuls les actes créant des obligations sont susceptibles de recours, en admettant, dans un certain nombre d'hypothèses, que des instruments de droit souple soient regardés comme faisant grief au vu de leur formulation impérative ou de leurs effets.
Les décisions Formindep du 27 avril 2011 et Société Casino Ghichard-Perrachon du 11 octobre 2012, en particulier, esquissent ce que peut être l'office du juge à l'égard d'une autorité régulatrice agissant par la voie du droit souple
Les arrêts du 21 mars 2016 constituent la suite logique pour la haute assemblée de prendre en compte le droit souple définitivement, notamment produit par les autorités administratives indépendantes (AAI).
La haute assemblée pose la règle que "les avis, recommandations, mises en garde et prises de position adoptés par les autorités de régulation dans l'exercice des missions dont elles sont investies, peuvent être déférés au juge de l'excès de pouvoir lorsqu'ils revêtent le caractère de dispositions générales et impératives ou lorsqu'ils énoncent des prescriptions individuelles dont ces autorités pourraient ultérieurement censurer la méconnaissance ; que ces actes peuvent également faire l'objet d'un tel recours, introduit par un requérant justifiant d'un intérêt direct et certain à leur annulation, lorsqu'ils sont de nature à produire des effets notables, notamment de nature économique, ou ont pour objet d'influer de manière significative sur les comportements des personnes auxquelles ils s'adressent (...)"
Cette décision, qui s'inscrit dans le droit fil de ses réflexions sur le droit souple en 2013 (étude annuelle), est une décision d'importance, et ce, à plus d'un titre.
En premier lieu, au vu de la multiplicité d'AAI et d'autorités produisant des recommandations, ligne directrice ou d'instrument de droit souple qui produisent des effets sur les acteurs notamment économiques.
Mais plus largement, dans la mesure ou pour le Conseil d'État, dans son étude, le droit souple peut contribuer au renouvellement de l'action de l'État en élargissant la gamme de ses moyens d'action, à condition de s'inscrire dans une doctrine de recours et d'emploi bien définie.
De nouveaux champs de contentieux en perspective à investir pour les praticiens du droit.
https://www.lesechos.fr/idees-debats/cercle/cercle-155731-le-conseil-detat-sattaque-a-la-soft-law-1210471.php