FORUM INTERNATIONAL DE LA CYBERSECURITE 2020

Auteur : Corinne FRANCE – General Secretary EFCSE
29 Janvier 2020

Pour la douzième édition du Forum International de la Cybersécurité, cette année sur 3 jours, c'était grosse affluence, salles combles, plénières complètes et circulation entre les stands plutôt chargée, nous pourrions naturellement en conclure que la cybersécurité est un sujet important et porteur …

Confirmation, les enjeux sont magistraux sur la scène mondiale où les poids lourds du numérique, US et Chine en tête, donnent le ton face à une Europe qui s'organise pour peser au moins aussi lourd sur ce terrain.

La souveraineté européenne est en effet fondamentale en matière de numérique, comme l'a souligné Guillaume POUPARD, directeur général de l'ANSSI, lors de son intervention plénière ; il a également rappelé l'importance d'agir vite dans le domaine de la cybersécurité, illustrant son propos par un focus sur le secteur de la santé et les attaques (ransomware) subies en 2019, dont celle contre le CHU de Rouen. Outre les préjudices subis, ce sont de forts avertissements dont il faut impérativement tenir compte.

Selon le CLUSIF (Club de la sécurité de l'information français) les établissements de santé ont été une des cibles prioritaires des pirates en 2019 (réf. Panorama de la cybercriminalité 2019 / CLUSIF).

Il a été souligné que ransomware et attaques indirectes semblent poursuivre leur progression de façon importante (inquiétante), en août 2019, la société McAfee publiait déjà un rapport faisant état d'une augmentation de 118 % au 1er trimestre 2019, il semble que sur l'année complète, ces attaques aient doublé, 2019 ayant été spécifiquement marquée par un vent d'innovations et d'approches très ciblées de la part des pirates.

Actions concrètes : les exemples de la Gendarmerie Nationale

Sur cette édition du FIC, la gendarmerie, co-organisatrice du salon, nous a donné, entre autres, des précisions sur les retombées de la plateforme PERCEVAL mise en place par le centre de lutte contre les criminalités numériques (C3N) en juin 2018 pour signaler une fraude à la carte bancaire.

Christian RODRIGUEZ, directeur général de la gendarmerie a souligné l'importance du dispositif PERCEVAL qui, en 2019, a enregistré plus de 200 000 signalements de fraudes aux moyens de paiement.

En matière de cybersécurité, la Gendarmerie Nationale française est un acteur particulièrement actif, souvenons-nous qu'elle avait fait tomber en 2019, un énorme réseau international de bots malveillants, avec 850 000 ordinateurs infectés, pour ne citer que cet exemple.

L'année 2020 s'annonce déjà riche en initiatives opérationnelles, notamment avec la création d'une cellule spécifiquement dédiée à la lutte contre le détournement des objets connectés, nommé plateau d'investigations des objets connectés (PIOC), né de la fusion des compétences du C3N[1] et de l'IRCGN[2].

De l'électroménager à l'automobile en passant par les caméras de surveillance ou les capteurs médicaux, le terrain de jeu pour les hackers est de plus en plus vaste pour capter de la matière première pour leurs activités illicites, à savoir : l'information.

INTERROGEONS-NOUS SUR LES CONSEQUENCES DU PIRATAGE DES OBJETS QUI NOUS ENTOURENT …

Ecosystème

Lorsqu'on parle d'organiser l'écosystème il s'agit tout autant de structurer sérieusement un cyberespace de confiance et suffisamment stable, que de permettre l'émergence d'acteurs européens dans un contexte mondial où les super puissances du numérique ont pris une sérieuse avance.

Tant sur le plan de la sécurité que sur le plan économique, la cybersécurité s'invite de plus en plus fréquemment à toutes les tables de réflexion stratégique. La mise en place du RGPD a permis d'amorcer ou de renforcer ce travail de fond qu'est la protection de l'information.

Dans ce contexte, la donnée personnelle, noyau de toutes les valeurs du cyberespace, y compris du côté obscur avec le Dark Web, bien qu'elle suscite toutes les convoitises, commence à disposer d'écrins de protection de plus en plus structurés. Le RGPD a, là aussi, œuvré en ce sens et il est intéressant de noter que cette initiative fait des émules à l'international. En effet, au 1er janvier de cette année, dans l'état américain de Californie, le California Consumer Privacy Act (CCPA) est entré en application. L'initiative accorde un droit à la vie privée et à la confidentialité des informations personnelles.

Moins contraignant que le règlement européen, le CCPA s'applique exclusivement aux entreprises en activité dans cet état, il n'en reste pas moins une étape intéressante dans un pays où la circulation libre des données est culturellement une habitude, la donnée privée étant considérée comme un bien commercial comme un autre.

Les règles ne bloquent pas nécessairement l'innovation, elles permettent de créer des standards.

[1] C3N : Centre de Lutte Contre les Criminalités Numériques - Directrice, Lieutenant Colonelle Fabienne LOPEZ

[2] IRCGN : Institut de recherche criminelle de la gendarmerie nationale – Directeur, Colonel Franck MARESCAL

Focus sur l'IDENTITE NUMERIQUE

Dans les différentes interventions auxquelles nous avons assisté, il a régulièrement été souligné l'importance de placer la personne au centre du monde digital.

Dans un contexte d'efficience économique et de choix sociétal, le besoin de sécurité et la volonté d'une meilleure maitrise de ses données sont autant de critères qui concourent à accorder cette centralité à la personne tant morale que physique.

Sur ce schéma, il est important de garantir nativement la confiance grâce au Privacy by Design, qui est la prise en compte du volet privé dès la conception d'une solution. Placé au cœur du RGPD, cet élément n'est en aucun cas une option mais bien une obligation. Intrinsèquement lié à l'identité de la personne, quels sont les challenges à affronter ?

L'une des tables rondes[3] du FIC a permis d'aller plus loin dans la réflexion et sur les pistes potentielles à suivre sur cette problématique identitaire.

La gestion de l'identité ou plus exactement de l'identité numérique est bien évidemment liée à la confiance mais aussi (non exhaustif), à l'interopérabilité des systèmes, à la gestion de la vie privée et à l'expérience utilisateur (UX de l'anglais User eXperience).

Dans les écosystèmes digitaux, la difficulté est l'interaction sur chacun des maillons d'une chaine, sur le principe de la procédure de « connaissance client », KYC (Know Your Customer en anglais), cela permet de connaitre l'identité de la personne mais s'accompagne généralement d'une dégradation de la chaine de services car il y a plusieurs identifications à faire. En tant que personne, nous appartenons à des univers différents selon les services que nous consommons, c'est le concept de segment de clientèle et d'identification en correspondance (personnification).

Le challenge est donc bien de rendre plus fluide l'accès aux services numériques, ce qui sera possible grâce à de nouvelles technologies comme le souligne David MANSET.

> LA QUESTION EST : QUI A LE CONTROLE DE LA GESTION DE L'IDENTITE ?

Frédéric LAPORTE souligne que dans le monde numérique, une fois que j'ai prouvé mon identité souveraine (administrative, encadrée par l'Etat), je dispose de plusieurs identités d'usage.

1 identité = 1 usage (carte de transport, carte Vitale, carte d'abonnement cinéma, identifiants & mots de passe pour accéder à mes divers espaces personnels de service …),

La dématérialisation ajoute une couche de complexité dans la mesure où il n'y a pas de présence physique de la personne.

Pour Tjerk TIMAN, le monde du numérique étant contrôlé par de grosses entreprises (Google, Facebook, Alibaba, etc..), en tant qu'individu je dois être particulièrement attentif à qui j'ai donné mes informations / Lesquelles ? Quand ? Comment ?

Nous laissons de plus en plus de traces digitales, avec plus d'opportunités pour disposer de services adaptés à nos besoins (envies) mais aussi plus d'exposition à une exploitation non consentie de nos informations.

Pour les offreurs de services, l'équilibre opportunités commerciales / responsabilité de gestion de la masse d'informations du client est une équation sensible, d'autant plus avec la RGPD.

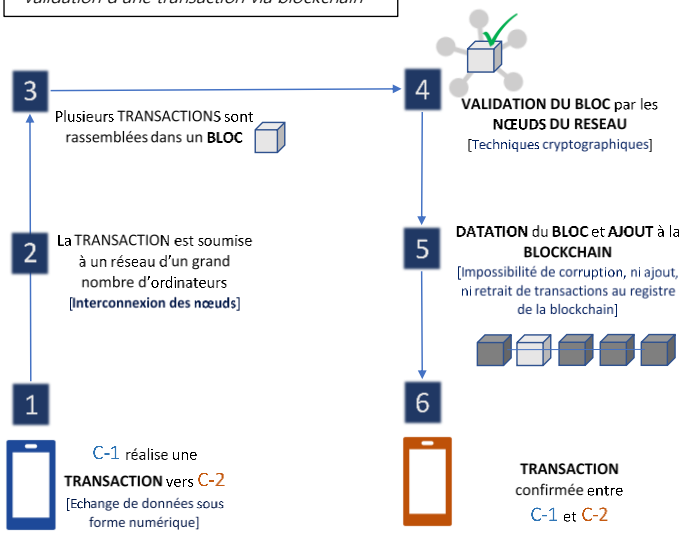
[3] Table ronde du 29/01 : Identité auto-souveraine, vers la conformité RGPD « by design » ? Animateur : Matthieu GUILLAUME, manager en cybersécurité et confiance numérique chez Wavestone ; Intervenants : Tjerk TIMAN, Strategy & Policy chez TNO – Frédéric LAPORTE, Directeur marketing & produit chez IN Group – David MANSET, Directeur Recherche & Innovation chez Be-ys Group.

LA TRANSPARENCE PORTEE PAR LE DIGITAL OBLIGE A RENFORCER LES PROCEDURES DE CONFIANCE.

L'identité souveraine, Self Sovereign Identity (SSI) en anglais, pose les bases d'une approche nouvelle pour la gestion de son identité dans la vie numérique.

Pour faire simple, il s'agit de valider l'information par l'ensemble d'un réseau, grâce à la technologie BLOCKCHAIN, au lieu de laisser ce soin à une seule autorité. Ceci permet à un utilisateur de garder la main sur ses données qui lui servent d'identité, de contrôler l'accès à n'importe quelle information, de la partager dans son intégralité ou en partie et surtout, d'annuler cet accès quand bon lui semble.

Schéma simplifié du processus de création / validation d'une transaction via blockchain



Le SSI va dans le mouvement de décentralisation pour la délivrance d'une identité, pour un écosystème numérique donné et replace la personne au centre, comme le précise David MANSET, qui attire cependant notre attention sur le fait qu'un certain nombre de problématiques sont encore à traiter, telles que : assurer un équilibre entre digitalisation et souveraineté, valider une identité sans présence physique, traduire des processus juridiques en informatique, assurer l'équilibre entre sécurité et confiance, respecter les organisations qui déterminent (délivrent) l'identité souveraine, imaginer comment les fédérer, imaginer quelle forme tout cela peut prendre pour les utilisateurs, autant de points qui, pour l'heure, sont à des niveaux variables d'avancement …

Tjerk TIMAN ajoute que dans des secteurs sensibles tels que le médical, la vérification d'identité via la bockchain est une solution (en théorie) dans la réalité c'est assez compliqué à mettre en place, question de confiance sur la phase de notarisation[4] par exemple, il existe quelques projets exploratoires dont certains très prometteurs,

- ✓ Corée du Sud : une blockchain partagée pour stocker les identités numériques (prévision du lancement commercial cette année) ;
- ✓ Canada et Espagne : projet d'authentification par blockchain avec des plateformes partagées dans le secteur bancaire.

En outre, comme la blockchain, par définition, ne peut pas être modifiée, il n'y est pas possible d'effacer l'information, il y a donc incompatibilité avec le RGPD et spécifiquement le droit à l'oubli. Cependant, pour le RGPD, la blockchain est capable d'apporter la preuve (notoriété).

A la question « qui est responsable du traitement de l'information » avec la blockchain, la réponse est difficile puisque c'est distribué sur l'ensemble d'une chaine.

Cependant, avec la qualification du business process dans les smart contrats[5] la blockchain pourrait être une solution pour la gestion de la SSI.

[4] Notarisation : phase de certification des étapes dans le cadre d'une transaction / échange entre 2 parties pour garantir un contenu, son origine, sa date et sa destination.

[5] Smart contrats : contrats intelligents, équivalent en informatique d'un contrat traditionnel mais sans l'intervention d'un tiers de confiance, pour

La piste du DLT[6] pourrait représenter une solution de réponse à la problématique de registre notarié et aller ainsi dans le sens d'une identité souveraine ; la blockchain représente un des types de structures de données qui peuvent être utilisés dans le cadre d'un DLT.

Le potentiel de succès du DLT se trouve probablement entre les mains des personnes qui sont passionnées (geek) de la PRIVACY ID !

Nous voyons que la distribution de l'identité auto-souveraine se heurte à des contextes contradictoires, si l'on y ajoute les problématiques d'extraterritorialité[7], nous sommes dans un environnement que l'on peut vraiment qualifier de complexe …

L'identification numérique nécessite d'avoir une infrastructure dimensionnée, de vraies expertises (compréhension des technologies) et des utilisateurs avec une éducation numérique.

Sur ce sujet, l'Europe a une dette à la fois structurelle (ses organisations) et numérique.

Il existe cependant des projets très prometteurs au niveau de l'UE, tels que My Health My Data (MHMD), action de recherche et d'innovation du programme Horizon 2020 pour un changement fondamental de partage des données sensibles.

MY HEALTH MY DATA

MHMD est destiné à devenir un véritable marché de l'information, basé sur de nouveaux mécanismes de confiance et des relations directes, fondées sur des valeurs entre les citoyens de l'UE, les hôpitaux, les centres de recherche et les entreprises.

En conclusion, s'agissant de cybersécurité, c'est bien sur la scène internationale, dans le cyberespace, que tout se situe, que l'on soit acteur public ou privé, une des clefs fondamentales est la COOPERATION.

S'il est souvent fait référence au point faible que représente l'humain au cœur de ce nouveau monde immatériel, ancré dans un monde très matériel, c'est que nous avons encore du chemin à parcourir …

L'évolution de nos habitudes (mauvaises ?) dans nos vies numériques passe forcément par une prise de conscience des enjeux, pour aujourd'hui et pour demain.

[6] DLT : Registre Distribué ou Partagé (en anglais distributed ledger ou shared ledger) il est simultanément enregistré et synchronisé sur un réseau d'ordinateurs, il a la capacité à évoluer à la suite de l'addition de nouvelles informations, préalablement validées par la totalité du réseau et ne pouvant jamais être supprimées ou modifiées. Pour faire simple, c'est un protocole informatique géré par du code informatique qui s'appuie sur la technologie blockchain.

[7] Extraterritorialité : se référer au Cloud Act made in US qui permet aux forces de l'ordre ou agences de renseignement américaines d'obtenir des informations stockées sur les serveurs des opérateurs télécom ou des fournisseurs de services de cloud, tant sur le sol américain qu'à l'étranger. Cloud Act : Clarifying Lawful Overseas Use of Data Act", loi fédérale américaine du 23 mars 2018 /