L'entreprise face à la criminalité

Avril 2020

La souveraineté numérique
Cybercriminalité
Les mafias
Malveillance anarchiste
La montée des tensions politiques et sociales
Sécurité privée
Activisme actionnarial
Contrefaçon

La souveraineté numérique :

Pierre Bellanger est le fondateur et président de Skyrock. Il est l'auteur d'un ouvrage sur « La souveraineté numérique » en 2014 (Stock) et revient sur le sujet dans le numéro 209 de mars-avril 2020 de la revue « Le Débat » dans un article titré « Trois empires et un garde-manger ».

L'auteur nous cite deux exemples, Adobe avec le Venezuela et Huawei avec la Chine pour attirer notre attention sur le fait, que dans le cadre d'une tension entre puissances, l'une d'entre elles peut frapper l'autre en utilisant l'arme de la dépendance technologique. Du jour au lendemain, les logiciels, les systèmes d'exploitation, les processeurs et les autres équipements informatiques d'une nation peuvent être suspendus par une autre.

Il nous alerte également sur le fait qu'en France par exemple, 80 % du trafic national part aux Etats Unis par l'intermédiaire du « cloud » et que les échanges sur Internet transitent par quelques centaines de câbles sous-marins. Une coupure de trafic est une interruption de nation.

Facebook et Google s'apprêtent à déployer des câbles sous-marins en Afrique et il faut savoir que la « neutralité » du Net ne s'applique pas au trafic sous-marin. L'Algérie en 2015, la Guinée et le Liban ont eu à souffrir d'interruption de trafic.

La souveraineté numérique consiste à pouvoir contrôler ses données, ses logiciels, ses protocoles, ses adresses, ses chiffrements et tous ses processeurs, de manière à être souverain sur le réseau.

Actuellement, le cyber-empire américain règne et deux autres prétendent accéder à ce statut, le chinois et le russe.

D'ici à 2022, l'administration chinoise devrait avoir supprimé tous les logiciels étrangers et les forces armées travaillent à se doter de leur propre système d'exploitation pour remplacer Windows.

La Russie, également, avec plus de difficultés, veut se prémunir d'une coupure agressive et garantir le fonctionnement de son réseau. Dans ce cadre, elle établit un système d'adressage alternatif, se substituant à l'Américain, rapatrie toutes ses données sur le territoire russe et centralise les interconnections des fournisseurs d'accès nationaux.

L'Europe, par contre, est restée sidérée par le développement du réseau et a compris trop tard qu'Internet ne venait pas s'ajouter au monde que nous connaissons, mais qu'il le remplaçait. L'auteur indique que 80 % des entreprises du CAC 40 en France et du DAX allemand utilisent Amazon Web Service. Il insiste sur le fait que cette subordination volontaire, ou par défaut, est incompatible avec notre souveraineté numérique.

De plus, souligne l'auteur, toute donnée collectée par un opérateur privé est à la disposition de son pays d'origine et toute information recueillie par un agent public, ou sous contrat, est communiquée aux entreprises de sa nation en compétition à l'étranger.

Il conclut en assurant qu'il faut fonctionner avec trois monnaies, une monnaie de long terme : la sécurité nationale, une monnaie immédiate : la donnée financée par le renseignement et enfin le marché qui s'intercale utilement entre les deux et il déplore l'absence d'un géant de l'Internet européen.

Cyber criminalité

Dans la revue Atlantico, publiée le 27 avril 2020, le criminologue Xavier Raufer attire l'attention sur une attaque cyber de grande ampleur concernant la ville de Marseille. En effet, dans la nuit du vendredi 13 mars 2020, les serveurs de Marseille, la ville et la communauté urbaine, ont été infectés par un virus qui a crypté environ 90 % des données.

Tous les services de la municipalité ont été gravement handicapés. Plus grave, les sauvegardes ont été également cryptées par le virus. Le virus « Mespinoza-

Pyza » qui sert à rançonner des villes et des entreprises serait connu depuis la fin de l'année 2018.

Selon le criminologue et malgré les recherches qu'il a entreprises, il ne semble pas que des explications aient été données, 40 jours après l'événement.

Ce n'est pas la première fois que des municipalités sont attaquées. En novembre 2019, les administrations des villes de Nuits-Saint-Georges et de l'intercommunalité de Gevrey-Nuits avaient été infectées par un virus. Une demande de rançon de 0,31 bitcoins (soit 2 200 €), avait été émise.

Un mois avant, en octobre 2019, c'est l'agglomération de Grand Cognac (Charente) qui avait été également touchée par une attaque informatique et des milliers de fichiers avaient été contaminés. La rançon demandée était de 180 000 €.

Comme l'a précisé l'ANSSI concernant la ville de Marseille, ce phénomène n'est pas nouveau. Il est cependant très alarmant et mériterait d'être pris en considération.

Un autre criminologue, Alain Bauer, souligne que la guerre d'internet continue pendant la crise épidémique et, pour lui, la prochaine épreuve de souveraineté dépassera en ampleur celle des masques. Il note que l'on assiste à une diffusion exponentielle des rançongiciels et prise de contrôle des équipements informatiques et des stocks de données et pense que nous sortirons de la crise sanitaire, mais que nous allons entrer dans la crise cyber. Notre monde y est extrêmement dépendant et n'est guère préparé.

Pour lire la suite de la veille Aconit, il est nécessaire, pour s'abonner, d'adresser un mail à jean.lucat@aconit.eu en mentionnant les informations suivantes :

Société Adresse
Téléphone Nom de la personne responsable
Adresse mail :
Prix de l'abonnement : 480 € à l'année TTC.
Dès la réception de ces informations, vous recevrez une facture correspondante.