De l'importance d'une stratégie collective en matière de cybersécurité

En 2020, en pleine crise sanitaire, le nombre de cyberattaques contre les collectivités locales a augmenté de 50%. La métropole Aix-Marseille-Provence, la région Grand Est, le Conseil départemental d'Eure-et-Loire, les villes de Marseille, Vincennes, Angers, la Rochelle, Annecy, Alfortville entre autres ont toutes été victimes de cyberattaques organisées. En mars 2020, l'AP-HP a fait face à une attaque par déni de service (DDoS), les salariés en télétravail étant coupés de leurs accès à distance. En décembre 2020, le Centre hospitalier d'Albertville-Moûtiers a été lourdement impacté : nombre d'équipements, logiciels, serveurs ont été paralysés, ainsi que les systèmes de deux EHPAD et Unités de soins. En février 2021, le Centre hospitalier de Dax (Landes) et l'hôpital de Villefranche-sur-Saône ont aussi été ciblés et leurs services impactés.

La gravité du sujet n'est pas à démontrer, en particulier lorsque les cyberattaques visent des secteurs essentiels à l'économie du pays et que peuvent être en jeu la vie de milliers de personnes.

L'attaque informatique peut consister à rendre les données indisponibles (atteinte à la disponibilité des données), à voler les données (atteinte à la confidentialité des données), voire à s'introduire dans un système d'information de manière frauduleuse pour les modifier (atteinte à l'intégrité des données). Le chiffrement des données suivi d'une tentative d'extorsion de fonds est la technique employée la plus courante (rançongiciel).

Quel cadre normatif en matière de cybersécurité ?

Juridique_ Marie-Hélène Gostiaux

Un cadre normatif vise à renforcer la cybersécurité dans le secteur public et le secteur privé pour les activités les plus sensibles, avec notamment :

- La loi de programmation militaire de 2013: elle a imposé aux opérateurs d'importance vitale (OIV) le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent ;
- La directive sur la sécurité des réseaux et des systèmes d'information de 2016 (dite aussi directive Network and Information System Security « NIS ») : elle a été une des premières mesures à l'échelle de l'UE pour renforcer la coopération entre les États membres en matière de cybersécurité, en instaurant des obligations pour les Opérateurs de services qui sont essentiels au fonctionnement de l'économie et de la société (OSE) – dans des secteurs critiques tels que l'énergie, les transports, la santé ou la finance – et des Fournisseurs de service numérique (FSN) tels que marchés en ligne, moteurs de recherche et services dans le cloud ;
- Une loi de transposition de la directive NIS : la loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'UE dans le domaine de la sécurité et le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique ;
- Le règlement (UE) 2019/881 du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications.

La directive NIS est en cours de révision (« NIS 2 ») pour tenir compte de l'évolution des menaces et de la mutation numérique accélérée par la crise de la COVID-19, la Commission européenne ayant fait une proposition en ce sens en décembre 2020.

Fin mars 2021, le Conseil de l'Union européenne a adopté des conclusions sur la stratégie de cybersécurité de l'UE, avec un plan d'actions pour la décennie à venir, consistant notamment à accélérer l'adoption des normes clés de sécurité internet, le chiffrement fort, la coopération avec les organisations internationales et les pays partenaires, la mise en place d'une unité conjointe de cybersécurité, etc.

Le facteur humain, facteur clé de la stratégie cyber

En dépit de tous les moyens matériels et techniques consacrés à renforcer la sécurité, le risque zéro n'existe pas. La sécurité informatique passe avant tout par l'humain, par le biais d'une sensibilisation et d'une vigilance accrue de la part des agents et collaborateurs.

Juridique_ Marie-Hélène Gostiaux

A cet effet, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ne cesse de sensibiliser les acteurs privés comme publics aux mesures de sécurité et à l'hygiène numérique. A titre individuel, le dispositif gouvernemental Cybermalveillance.gouv.fr offre une assistance à toute victime d'actes de cybermalveillance. En mars 2020, suite à plusieurs attaques ciblant des collectivités, l'ANSSI a publié des recommandations de sécurité à destination des collectivités territoriales. En février 2021, l'ANSSI a présenté la stratégie française pour la cybersécurité dans le cadre de France Relance, laquelle prévoit de mobiliser un milliard d'euros pour notamment développer des solutions souveraines de cybersécurité, former aux métiers de la cybersécurité ou encore soutenir l'adoption de solutions cyber par les entreprises, les collectivités et l'Etat.

Marie-Hélène Gostiaux