Pourquoi la cybersécurité devient partout une question de sécurité nationale ?

Les cybercriminels s'attaquent de plus en plus aux infrastructures sensibles voire même à des services vitaux. Aujourd'hui aucun pays n'est épargné. Partout des infrastuctures critiques, des hôpitaux, des chaînes d'approvisionnement (supply chain) sont ciblées, et nous l'avons vu pendant la crise du COVID-19, la distribution des vaccins a également été impactée. Il est temps de poser une limite. Alors que les lignes s'estompent au niveau des cyberattaques, une chose apparaît de plus en plus évidente : la cybersécurité est une question de sécurité nationale pour toutes les Nations.

Les PDG de 24 entreprises de technologie, fournisseurs d'infrastructures critiques, banques, compagnies d'assurance et établissements d'enseignement de premier plan ont récemment rencontré à la Maison-Blanche le président américain Joe Biden et ses conseillers sécurité.À l'issue de la réunion, la Maison-Blanche a annoncé plusieurs initiatives audacieuses.

En effet, les Etats-Unis ont été particulièrement touchés, et ont donc rapidement pris des mesures. A titre d'exemple, le National Institute of Standards and Technology (NIST) collaborera avec des partenaires du secteur privé pour développer un cadre visant à améliorer la sécurité et l'intégrité de la chaîne d'approvisionnement. L'Initiative de cybersécurité des systèmes de contrôle industriel a également été élargie au-delà des services d'électricité pour inclure les gazoducs.

Les principales entreprises de technologie ont également accepté de participer à diverses initiatives. Apple améliorera la sécurité de la supply chain, Google étendra les programmes Zero Trust, Microsoft accélérera ses efforts pour intégrer la cybersécurité dès la phase de conception des systèmes et Amazon mettra sa formation interne de sensibilisation à la sécurité gratuitement à la disposition du public.

En conséquence de cette rencontre, des initiatives ont également été créées pour renforcer l'éducation et la formation. L'objectif étant d'enseigner les bases de la cybersécurité aux étudiants et de combler le manque de compétences en cybersécurité, par le biais de nouveaux programmes de certifications plus courts, ou encore de bourses d'études plus accessibles.

Investir et collaborer plus et mieux

Ces décisions prises par les Etats-Unis vont dans le bon sens. Les attaques contre SolarWinds, suivie des attaques HAFNIUM contre les serveurs Microsoft Exchange vulnérables, et les attaques massives de ransomware contre Colonial Pipeline et JBS Meat Packing ont aussi démontré que les secteurs public et privé doivent impérativement coopérer pour contrer les cybermenaces. Il est temps de cesser de s'appuyer sur des technologies archaïques conçues pour se protéger des menaces qui existaient il y a 20 ans et d'investir dans des solutions de prévention, de détection et de résilience de pointe.

Nous devons par ailleurs lutter contre la montée en puissance du cyberespionnage et des cyberattaques perpétrées par les États en introduisant une réglementation financière du bitcoin et des autres cryptomonnaies pour lutter contre les ransomwares et limiter la possibilité de monétiser la cybercriminalité. Nous devons revoir la législation pour mettre à jour les sanctions associées à la cybercriminalité, travailler avec les pays alliés à la révision des traités d'extradition des

cybercriminels et favoriser la coopération mondiale pour pouvoir riposter.

La condamnation de la Chine par les États-Unis et l'Union européenne pour l'attaque de Microsoft Exchange Server a envoyé un signal fort aux États « ennemis », leur signifiant qu'à l'avenir, les cyberattaques contre des cibles mondiales ne seront pas sans conséquences. Davantage de condamnations sont nécessaires ainsi que l'établissement de règles d'engagement claires pour les opérations offensives.

Le collectif doit être une valeur fondamentale. Nous sommes confrontés à un paysage de menaces en constante évolution et en expansion, de même qu'à des attaques de plus en plus sophistiquées qui brouillent les lignes entre cyberattaques et cyberespionnage. Un effort de collaboration entre nations, fournisseurs des secteurs privé et public et administrations publiques est nécessaire pour échanger des renseignements et des connaissances afin d'améliorer notre capacité à lutter contre ce déferlement de cybercriminalité avancée.

La cybersécurité est aujourd'hui une question de sécurité nationale et si ça n'est pas encore le cas, cela devrait clairement le devenir pour toutes les Nations.