Photo by Aziz Acharki on Unsplash

La France prévoit 1 milliard d’euros pour aider à la création de 20 000 emplois en cybersécurité

Face à la multiplication des cyberattaques, visant notamment des hôpitaux, Emmanuel Macron annoncera ce 18 février la stratégie française en matière de sécurité informatique. Un milliard d'euros va être engagé.

La multiplication des attaques informatiques à destination des hôpitaux en France et dans le monde inquiète. Ils sont devenus des cibles privilégiées des cyberattaques au rançongiciel. Face à cette situation, Emmanuel Macron présentera ce jeudi 18 février la stratégie française en matière de cybersécurité, après un échange par visio-conférence avec les directeurs des hôpitaux de Dax et Villefranche-sur-Saône, récemment victimes de rançongiciels, a annoncé l’Elysée. Le chef de l’Etat annoncera une enveloppe d’un milliard d’euros, dont 720 millions de fonds publics, pour renforcer la filière et tripler son chiffre d’affaires à 25 milliards d’euros en 2025. L’exécutif veut créer un « *écosystème de la cybersécurité* » en renforçant les liens entre recherche publique et privée, afin de réduire la part des acteurs étrangers qui représentent 30 à 40% du marché français.

Au coeur de cette ambition, le futur « Campus Cyber » qui réunira sur 20 000 m2 à La Défense une soixantaine d’acteurs-clés du secteur – grands groupes,

startup, acteurs publics, organismes de formation, acteurs de la recherche et associations. L'objectif est de doubler les effectifs de la filière, à 40 000 emplois, et de faire émerger au moins trois « *licornes* » (startup dont la capitalisation
dépasse un milliard de dollars). Parmi les sociétés les plus prometteuses, la présidence cite Vade Secure, Gatewatcher ou CybelAngel. Les effectifs de l'Anssi (Agence nationale de la sécurité des systèmes d'information), qui aide les institutions à renforcer leur sécurité, devraient également passer à 600 personnes fin 2021 contre 400 en 2017.

À lire aussi

Covid-19 : Comment CybelAngel a neutralisé une escroquerie visant un fabricant de vaccins

Les cyberattaques contre les organisations ont quadruplé en 2020, une tendance qui touche « *tous les acteurs et tous les pays*« , souligne l'Elysée. En témoignent l'attaque de grande ampleur contre des géants du numérique et des agences nationales aux Etats-Unis ainsi que celle contre l'Agence européenne du médicament. Des entreprises françaises ont également été la cible d'une cyberattaque majeure entre 2017 et 2020.

Même si leurs auteurs restent souvent inconnus et difficiles à arrêter, une action policière coordonnée des Etats-Unis, de la France, d'autres pays de l'UE et de l'Ukraine ont réussi en janvier à démanteler le réseau du logiciel malveillant Emotet. Autre succès, l'arrestation de membres du groupe de rançongiciel Egregor qui a frappé ces derniers mois le groupe Ouest-France, entre autres. Comme l'ont montré les exemples de Dax et Villefranche-sur-Saône ces derniers jours, les hôpitaux français sont particulièrement vulnérables. Ils ont fait l'objet de 27 cyber-attaques majeures en 2020, a indiqué mercredi le secrétaire d'Etat à la Transition numérique Cédric O.

Ni le centre hospitalier de Dax ni celui de Villefranche-sur-Saône ne verseront un sou. Les hôpitaux « *ont pour consigne stricte de ne jamais payer* » les rançons exigées, a rappelé le directeur général de l'Anssi, Guillaume Poupard, ajoutant qu'il espérait pouvoir récupérer les données bloquées par
les pirates, grâce aux systèmes de sauvegarde. Selon le secrétaire d'Etat, 110 hôpitaux français ont été « accompagnés dans des audits de sécurité » grâce au soutien de l'Anssi et « *11 d'entre eux sont accompagnés au jour le jour*« .

Article écrit par MADDYNESS AVEC AFP