Je suis convaincue que l'hyper automatisation est clé aujourd'hui face aux menaces les plus fulgurantes.

Elena Poincet, après douze ans dans l'armée et quatorze à la DGSE, est aujourd'hui CEO de l'éditeur de logiciels Tehtris, expert en cybersécurité. Cet entretien a été publié le 3 juin 2022.

1/ Votre expérience dans les services vous confère-t-elle une spécificité dans la manière d'envisager le métier de la cybersécurité ?

Dès la création de TEHTRIS, nous avons mis notre culture offensive au service du défensif en réalisant nous-même des intrusions dans les entreprises, lesquelles se pensaient alors sécurisées. Notre capacité à entrevoir les possibilités et la connaissance de la cybercriminalité confèrent une spécificité à la technologie XDR que nous avons créée avec Laurent Oudot, co-fondateur de TEHTRIS : **nous avons imaginé un système hyper automatisé qui opère en tout temps et en tous lieux, comme si nous exercions en temps de guerre.**

La TEHTRIS XDR Platform a ainsi été conçue pour détecter et neutraliser les cyber attaques en temps réel et sans aucune intervention humaine. En opérant 24h sur 24 et 7 jours sur 7, elle est au service de la protection des entreprises et des administrations. **Je suis convaincue que l'hyper-automatisation est clé aujourd'hui face aux menaces les plus fulgurantes.**

2/ La France donne l'impression de se réveiller dans un monde hostile animé par des acteurs beaucoup plus soucieux de leurs intérêts que nous ne le sommes. Serait-ce une vue de l'esprit, et le cas échéant, pour quelles raisons ?

Entre 2012 et 2017, avec Laurent Oudot, lorsque nous alertions les entreprises du CAC40 sur l'arrivée des ransomware, personne ne nous croyait…

Pour moi, ce n'est pas une vue de l'esprit, c'est très clairement le cas. Les raisons sont diverses : la peur de changer, la peur de prendre des risques, la peur de perdre, etc.

Depuis deux ans, la donne change effectivement : nous avons pris conscience de nos dépendances. **Sur la cybersécurité, si la confiance envers les solutions européennes est difficile à obtenir, un changement s'opère, ça commence à venir. De plus en plus de RSSI sont soucieux de recourir à des solutions françaises car ils comprennent les conséquences que cela implique de recourir à des solutions étrangères.**

Au sein de TEHTRIS, nous n'avons pas attendu pour innover. Nous nous plaçons toujours dans une logique prospective où l'innovation fait partie de notre quotidien. Cette approche permet de proposer à nos clients des technologies à la pointe.

3/ Du point de vue de votre métier, est-il parfaitement sûr de recourir à des logiciels américains ?

Non. Nos données constituent notre patrimoine et doivent être protégées du cyber espionnage. **Si vous recourrez à des solutions américaines, comment être certains que ces acteurs étrangers protègent vos données ? Peut-être les utilisent-ils à des fins d'espionnage industriel ou commercial ? Les lois extraterritoriales comme de Sécurité Intérieure permettent un degré d'intervention difficilement contrôlable.**

Pour nous, les seuls logiciels sûrs sont les nôtres. Nos logiciels, développés en France et dont les données sont hébergées en Europe, sont « secure & ethics by design ». **Contrairement aux logiciels américains, nous garantissons l'inviolabilité du contenu des fichiers protégés, auxquels nous n'accédons pas.** Nous nous positionnons ainsi en tiers de

confiance européen. C'est la raison d'être de TEHTRIS qui est de lutter contre le cyber espionnage et le cyber sabotage.

4/ Face à la menace clandestine que fait peser la cybercriminalité, ne trouvez-vous pas que les acteurs de la sécurité jouent un peu "à jeu ouvert", en communiquant à profusion sur leurs ressorts, méthodes et outils ?

Les acteurs de la sécurité communiquent sur leurs solutions, c'est certain – les budgets marketing de nos concurrents américains et israéliens sont d'ailleurs colossaux. Les méthodes et outils restent, en revanche, relativement peu documentés dans les détails. Il y a un risque de surenchère sur les réseaux sociaux chez certains acteurs, qui permettent de nourrir l'ingénierie sociale des cybercriminels. Par exemple, **chez TEHTRIS, nous avons fait le choix il y a plusieurs années de ne pas afficher nos références clients, à de rares exceptions, afin de protéger nos clients, en ne les mettant pas dans la lumière. Nous sommes très précautionneux et ne mettons pas nos clients en danger pour en acquérir de nouveaux !**

Au sein de TEHTRIS, nous communiquons de façon « utile ». Cela signifie que nous partageons les informations qui peuvent contribuer à arrêter « la course » des cybercriminels. Par exemple, **dès que nous détectons une menace virulente, nous partageons l'information avec les autres acteurs de l'écosystème.** TEHTRIS est notamment membre de la Cyber Threat Alliance, une organisation à but non lucratif qui permet l'échange d'information de haute qualité et en temps quasi réel sur les menaces. Nous partageons, dans ce cadre, nos marqueurs uniques à forte valeur ajoutée pour contribuer à offrir un monde numérique plus sûr.

5/ L'IOT, c'est un vrai cauchemar pour des professionnels de la cybersécurité : une myriade de petits chevaux de Troie, n'est-ce pas ?

Les menaces liées aux IOT deviennent une cible privilégiée pour les cybercriminels. Ces derniers s'introduisent sur un de ces appareils non protégés pour accéder à l'ensemble du réseau d'une entreprise. Il est estimé que 75 milliards d'appareils seront en ligne en 2035.

Les entreprises doivent et devront donc s'adapter à l'utilisation croissante des IOT et comprendre que leur parc mobile est un vecteur de risque.

Je dirais que le cauchemar est donc surtout pour les entreprises qui doivent protéger leurs IOT avec des technologies adaptées. **Nous leur recommandons donc trois technologies : l'EPP (antivirus nouvelle génération), l'EDR (agent qui détecte et neutralise les menaces connues et inconnues) et le MTD (protection des périphériques mobiles, tels que les smartphones et tablettes).**

6/ La souveraineté technologique est devenue un thème central dans la vie politique. Quelle mesure prendriez-vous, qui en favorise le recouvrement pour notre nation ?

Je préfère parler d'autonomie stratégique, plus que de souveraineté technologique. Si je devais prendre une mesure pour protéger nos données, notre patrimoine, il s'agirait de recourir maintenant à des solutions françaises et/ou européennes de cybersécurité pour que, demain, l'Europe dispose de leaders de la cybersécurité.

La cybersécurité, c'est maintenant et non dans 10 ans. C'est un appel à faire confiance à nos solutions et à oser recourir à nos technologies. Certains RSSI le font déjà mais il faudrait que ce soit systématique.

Soutenir la commande publique et privée est essentiel. Si l'on regarde de l'autre côté de l'Atlantique, les PME innovantes et start-ups américaines se sont développées grâce au Buy American Act et au Small Business Act. Ces dispositifs d'achats et d'aides publiques volontaristes, qui datent depuis

plus de 50 ans, ont permis l'émergence de grands acteurs américains qui sont aujourd'hui largement présents en Europe et dans le monde.

S'il est inutile de rappeler que nous avons du retard, il est crucial de souligner que c'est maintenant qu'il faut un patriotisme économique en Europe.

7/ Au regard des enjeux de la cybersécurité pour le pays tout entier, pourquoi ne pas considérer que vous exercez une mission de service public, avec les moyens de puissance publique qui vont avec ?

Notre raison d'être est d'œuvrer pour la cyberpaix dans le monde et faire que le cyberespace devienne un environnement de confiance et d'avenir. Cette raison d'être est actée dans nos statuts puisque **TEHTRIS est désormais la seule entreprise de cybersécurité à avoir adopté le statut de société à mission.**

En ce sens, on exerce bien une mission de service public en protégeant les citoyens et en œuvrant pour l'intérêt général.

Si nous partons de ce principe que nous exerçons une mission de service public, il faudrait effectivement disposer de moyens de puissance publique efficaces. Les solutions de cybersécurité utilisées sur le marché français sont actuellement très majoritairement non-européennes.

Les acteurs publics pourraient-ils commencer par s'imposer à eux-mêmes l'utilisation de solutions françaises ? Assumons le fait que nous avons des technologies de cybersécurité à la pointe ! Assumons le fait de communiquer sur nos forces ! Nos concurrents américains et israéliens disposent de forces marketing considérables.

Je le redis la commande publique et aussi privée est essentielle pour nous, et plus globalement pour les acteurs de la filière.

8/ Notre droit pénal vous semble-t-il suffisamment sévère en matière de cybercriminalité ?

La cybercriminalité est une délinquance protéiforme et sans frontière. Les auteurs et les victimes sont des entreprises, des administrations, des particuliers, nous tous.

L'ampleur de la cybercriminalité est complexe à évaluer. Selon les estimations, les pertes sont estimées à 6 000 Mds USD en 2021, soit 7% du PIB mondial et l'équivalent de la 3ème économie mondiale…

Dans ce contexte, il est essentiel que le droit pénal soit à la hauteur de ces enjeux. La cybercriminalité impose une coopération judiciaire internationale qui se développe. Il existe des pôles de cybercriminalité, par exemple, dans les tribunaux. Nous avons tous intérêt à réduire le nombre de cybercriminels.

La sévérité pénale dépend surtout de l'ampleur des dégâts causés…l'internationalisation et la coopération inter-Étatique requise, comme l'anonymat et la distance physique que le numérique permet de maintenir, laissent à penser au cybercriminel que ses victimes ne sont pas des personnes incarnées et qu'il est à l'abris de la Justice. Diverses opérations policières dans les deux dernières années nous ont démontré qu'il ne l'était pas !

Rappelons que la question n'est pas de savoir si l'on risque d'être attaqué mais quand et comment il est possible de limiter ce risque. Assurer la sécurité des systèmes d'information et garantir la disponibilité, l'intégrité et la confidentialité des données est clé. Comment ? La première recommandation est de recourir à des outils hyper automatisés qui détectent et neutralisent en temps réel et sans aucune intervention humaine les cyberattaques.