

Cybersécurité : Face aux risques, l'urgence de former

Dans le cadre de l'opération « Tribune d'été », organisée par la rédaction de Maddyness, nous nous sommes rapprochés de celles et ceux qui ouvrent une fenêtre sur le futur des entreprises et de la société. Tribune proposée par Valérie Poulain de Saint Père et Axel Dreyfus, fondateurs de l'École 2600.

Temps de lecture : minute

14 août 2023

Ces dernières années, les entreprises et les institutions françaises ont significativement renforcé leurs efforts en matière de cybersécurité. Pourtant, elles restent, dans une large mesure, vulnérables et frappées par des cyberattaques de plus en plus nombreuses et souvent fatales.

Les chiffres ont de quoi préoccuper. D'après le baromètre du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), plus de la moitié des entreprises françaises ont été attaquées en 2022. Pour certaines, les conséquences sont lourdes. Une entreprise perdrait en moyenne 27 % de son chiffre d'affaires annuel à la suite d'une cyberattaque. 70 % des PME ne s'en relèveraient pas, contraintes de cesser leur activité dans les 18 mois suivants.

Former davantage et massivement

Ce bilan, déjà préoccupant, a peu de chances de s'atténuer dans les années qui viennent. Nos entreprises françaises sont insuffisamment préparées face aux cyberattaques et peinent encore à déployer les moyens nécessaires pour se protéger. Un enjeu majeur pour leur survie,

mais aussi pour la confiance de leurs clients et partenaires de plus en plus attentifs à l'exposition aux risques cyber.

De plus, le développement du télétravail, le recours à de nouvelles technologies comme l'intelligence artificielle, le cloud computing ou l'internet des Objets (IoT), créent sans cesse de nouvelles formes de menaces auxquelles il faut s'adapter. En face, les cybercriminels se multiplient, se professionnalisent et usent, sans surprise, de techniques de plus en plus sophistiquées pour exploiter ces vulnérabilités.

Au regard de la rapidité avec laquelle ces technologies évoluent, on ne peut que parler d'urgence. Le premier enjeu de notre secteur c'est d'abord celui de former plus, mieux et plus massivement des experts en cybercriminalité pour protéger les entreprises et les institutions de notre pays.

On déplore aujourd'hui 15 000 postes vacants, faute de profils qualifiés, et 37 000 emplois nécessaires dans la cybersécurité à horizon 2025, lesquels ne seront probablement pas pourvus si on ne change pas de paradigme rapidement. Or le modèle pédagogique standardisé centré sur la formation initiale proposé actuellement en France ne répond plus aux besoins concrets des entreprises en matière de cyberdéfense.

Vers un nouveau modèle d'évaluation ?

Il est impératif de proposer, en complément d'un modèle basé sur la formation initiale structurellement insuffisante, un modèle plus équilibré qui mise davantage sur la formation continue et qui rassemble un public plus large. Nous savons désormais que pour rester performant, les compétences en cybersécurité doivent être très régulièrement réévaluées et mises à jour pour tenir compte de l'évolution des menaces.

Il faut ainsi passer d'une approche standardisée des formations, qui prend

mal en compte les spécificités des métiers cyber, à une approche d'hyper personnalisation des parcours d'acquisition des compétences pour mieux répondre aux besoins des entreprises et des institutions. Pour cela, l'évaluation précise du niveau des apprenants en amont du début de parcours de formation est cruciale.

Enfin, il faut s'affranchir d'un modèle qui valorise les diplômes génériques au détriment de la certification des compétences cyber. La validation efficace et rapide des acquis est essentielle pour mesurer l'adéquation entre les qualifications de l'apprenant et les besoins de l'entreprise.

Les enjeux sont vertigineux mais nous avons, en France, la chance d'avoir toutes les ressources et la diversité des talents pour relever ces défis. En nous préparant, en éduquant, en nous mobilisant autour d'objectifs communs, entreprises, écoles, État, institutions, pourront construire ensemble une cyberdéfense souveraine, solide et pérenne.



À lire aussi

L'École 2600 lève 6 millions d'euros pour lancer une formation

continue dans la cybersécurité



MADDYNEWS

La newsletter qu'il vous faut pour ne rien rater de l'actualité des startups françaises !

JE M'INSCRIS

Article écrit par Valérie Poulain de Saint Père et Axel Dreyfus