Communiqué de Presse

AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 vloquet@alx-communication.com

Le CESIN et Advens révèlent les résultats d'une grande enquête inédite sur le stress des Responsables Cyber

Le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) et la société Advens ont conduit une étude avec le concours de spécialistes, portant sur le stress des Responsables en Cybersécurité. Elle met au jour une profession éprouvante, soumise à un niveau élevé de stress.

Paris, le 15 septembre 2021 - Les résultats de cette enquête inédite portent sur un échantillon de 330 répondants, dont 60% de RSSI (responsables sécurité des systèmes d'information) et 20% de Directeurs Cybersécurité. Membres du CESIN, ils sont issus d'entreprises française (tous secteurs et tailles d'entreprises) et d'organismes publics.

Des niveaux de stress préoccupants

Conçue par le CESIN et Advens, avec le concours d'un coach et d'un médecin oncologue, tous deux spécialisés dans la gestion du stress et du burnout, l'étude s'appuie sur un questionnaire en deux parties. La première vise à évaluer le niveau de stress, et la seconde les facteurs propres aux métiers de la Cyber et susceptibles de contribuer au stress.

L'évaluation du niveau de stress se base sur un modèle de mesure reconnu (la PSS, *Perceived Stress Scale*), dont l'objet est la détermination du niveau de stress ressenti. Avec l'échelle PSS utilisée, donnant une évaluation allant de 0 à 40, le stress est jugé positif ou stimulant si le niveau est inférieur à 16. Entre 16 et 24, il existe des sentiments d'impuissance occasionnels et des perturbations émotionnelles. Au-delà de 22, l'individu se situe en « zone rouge », accompagnée de risques accrus pour la santé physique et mentale, et un sentiment de menace et d'impuissance.

La mesure du niveau de stress auprès des 330 répondants a conduit à établir un niveau moyen de 18,4 : cela traduit un niveau collectif de stress élevé. 130 personnes (soit 39% des répondants) se situent dans la zone verte, tandis que 61% des répondants sont en zone orange (33%) ou rouge (28%), et subissent donc un stress aux effets négatifs. Sur les 92 personnes qui se trouvent en zone rouge, 62 personnes sont en risque de burnout. Parmi celles-ci, 22 personnes sont même dans une zone à risque de dépression clinique, avec un score supérieur à 28 sur 40.

Un stress élevé peut être supportable sur une durée courte. Mais dans la durée, il peut impacter sérieusement la santé mentale. Ce stress peut impacter la performance des responsables Cyber et, in fine, la performance des dispositifs de Cybersécurité.

Concernant les causes du stress, les questions posées ont été organisées suivant une typologie de 8 familles de facteurs : coercition et surveillance, complexité et évolutivité, transversalité, combat et adversité, incertitude et inconnu, gestion de crise, communication et conviction, responsabilité et culpabilité.

Parmi les facteurs les plus contributifs du stress, se trouvent notamment le contexte d'adversité, la difficulté à déconnecter, la relation à la responsabilité et la culpabilité et le sentiment d'incertitude et d'imprévu au quotidien. A cela s'ajoutent les évolutions permanentes de la fonction et de son contexte.

Les personnes les plus touchées par le stress éprouvent un sentiment d'impuissance et de découragement devant la puissance des attaques cyber. Autre élément notable : la majorité des répondants estiment qu'un incident majeur pourrait leur faire perdre leur poste.

Plus précisément, **82% des répondants confirment le contexte d'adversité, face à des ennemis souvent invisibles, 52% des répondants se sentent en permanence sur le qui-vive, près d'un quart des répondants ne se font pas aux aléas et imprévus du métier et 28% se sentent découragés devant l'augmentation de la fréquence et de la puissance des cyberattaques.**

38% des répondants déclarent que leur métier souffre « encore » d'un a priori plutôt négatif, 47% se sentent encore incompris, voire jugés parfois excessifs et 54% estiment qu'une crise majeure pourrait leur coûter leur poste. Ce dernier chiffre passe à 65% pour les répondants de la zone rouge.

Alain Livartowski, oncologue à l'Institut Curie, participant à l'enquête, déclare : *« En tant que médecin, j'observe que le pourcentage de personnes en situation de stress est élevé, avec pour certains probablement une souffrance. La question du stress des responsables Cyber ne peut pas être occultée et une prise de conscience est nécessaire. Un des moyens de l'éviter est déjà de le reconnaître et de soutenir les RSSI dans l'entreprise. »*

Certaines composantes du métier de Responsable Cyber sont manifestement génératrices d'un stress, qui peut parfois devenir négatif. Si certains facteurs semblent difficiles à maitriser, comme l'intensité des attaques ou leur caractère aléatoire, certains paramètres peuvent être travaillés.

Une prise de conscience à suivre de près, des mesures à mettre en œuvre

Les résultats de cette enquête sont préoccupants et incitent à poursuivre la démarche. Le CESIN, avec le concours de la société Advens, mettra en place divers travaux et dispositifs, ainsi qu'un baromètre annuel pour suivre l'évolution de cette étude. Il est essentiel de comprendre si ces résultats sont inscrits dans la durée, de les mesurer à distance de la situation pandémique actuelle qui a tendance à majorer le stress pour un grand nombre de professions. Celles de la Cyber sont plutôt soumises à une aggravation des menaces, depuis le début de la pandémie, et l'isolement forcé lié aux phases de confinement peut avoir accentué la sensation d'impuissance et de découragement devant les menaces.

Mylène Jarossay, présidente du CESIN, commente : « *Cette étude confirme qu'il était urgent de se pencher sur la charge mentale des professionnels de la Cyber, afin d'identifier des pistes pour prendre soin de ceux qui assurent, chaque jour, un travail de défense complexe et exigeant. L'ambition est que les Responsables Cyber se sentent pleinement en accord avec les valeurs et les spécificités de ce métier singulier. Le CESIN est pleinement engagé dans cette démarche.* »

En réponse, plusieurs pistes sont examinées et portent soit sur la modification des causes du stress, soit sur l'atténuation des conséquences. Ces pistes peuvent s'inscrire dans le cadre de communautés telles que le CESIN, à travers des ateliers de « résilience face au stress », des séminaires ad hoc ou la réalisation de portraits plus complets de professionnels de la Cyber pour mieux comprendre le sujet du stress dans ce métier, avec différents parcours.

Au-delà des communautés, la prise en compte du stress doit être faite par l'employeur. Elle doit commencer dès l'élaboration de la fiche de poste, être intégrée au parcours de formation et s'appuyer sur des échanges avec les autres métiers de l'entreprise pour une meilleure

connaissance et compréhension du métier – ce qui, au passage, ne peut qu'accroitre la sensibilisation aux risques Cyber et le niveau collectif de préparation face à une attaque. Le monde académique a également un rôle à jouer dans l'identification et l'intégration des aspects liés au stress dans l'éducation des professionnels et futurs professionnels.

Rendre la filière plus apaisée et plus attractive

Comprendre et adresser le sujet du stress chez les professionnels de la Cyber est une démarche doublement gagnante. Il est important d'assurer enthousiasme, épanouissement et équilibre des populations concernées. Mais traiter le stress est une aussi approche qui fera gagner en performance.

En travaillant sur les causes du stress, la cybersécurité progressera. D'une part les personnes qui la pilotent se sentiront mieux armées et mieux soutenues, d'autre part ce sujet stratégique sera mieux intégré dans la vie numérique de l'entreprise, avec des responsables Cyber correctement reconnus et dotés des bons leviers pour exercer leur fonction.

Benjamin Leroux, directeur Marketing et RSSI de la société Advens, ajoute : *« Les problématiques identifiées par cette étude doivent nous permettre de rendre la filière Cyber plus apaisée, et donc plus attractive. C'est un challenge clé pour renforcer et diversifier les équipes de Cybersécurité, en profonde pénurie de ressources à l'heure actuelle. »*

Ressources : pour télécharger l'étude complète

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la cybersécurité. Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la cybersécurité et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'ANSSI, la CNIL, la BEFTI, la Gendarmerie Nationale, l'ARJEL, le Cercle Européen de la sécurité, ACYMA (cybermalveillance.gouv.fr), l'AFAI, l'EBG, le CyberCercle ou encore l'EPITA. Le CESIN compte plus de 700 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

www.cesin.fr

A propos d'Advens

Avec 300 collaborateurs à Paris, Lille, Lyon, Bordeaux, Toulouse et Nantes, Advens est le premier pure-player de la cybersécurité et le leader du SOC-as-a- Service en France. Advens propose une offre globale de cybersécurité qui combine des prestations à haute valeur ajoutée et un modèle innovant de Security-as-a-Service pour répondre aux besoins croissants des entreprises, quels que soient leur spécificité sectorielle ou leur métier. Advens œuvre pour la protection de plus de 300 clients en France et à l'international. Advens a pour ambition de devenir un leader de la cybersécurité en Europe tout en ouvrant une nouvelle voie au travers d'un modèle d'entreprise vertueux dans lequel performance économique et performance sociétale se nourrissent l'une de l'autre.

www.advens.fr