Le nouveau rapport Cyber Readiness de Trellix dévoile l'état de préparation des agences gouvernementales et des fournisseurs d'infrastructures critiques en France, en Allemagne et au Royaume-Uni.

Trellix, le spécialiste de la cybersécurité et pionnier dans la détection et la réponse étendues (XDR), publie aujourd'hui son Cyber Readiness Report, qui évalue l'adoption des technologies et le positionnement des gouvernements par rapport aux normes de cybersécurité, ainsi que la coopération entre les secteurs privé et public.

Le rapport de Trellix révèle que 87 % des répondants basés en Allemagne, en France et au Royaume-Uni, tous des pays de l'OTAN, estiment que les mesures officielles prises par le gouvernement peuvent jouer un rôle important dans le renforcement de la protection nationale contre les cybermenaces. Dans ces pays, les répondants considèrent que les partenariats avec le gouvernement gagneraient à être améliorés dans des domaines tels que la coordination de la cyberdéfense, le partage des informations sur les menaces et l'intégrité de la chaîne d'approvisionnement logicielle.

« *Au vu des tensions internationales et des incidents liés à la cyberguerre en Ukraine, la préparation des gouvernements et des infrastructures critiques fait l'objet d'une attention accrue* », explique Bryan Palma, PDG de Trellix. « *Notre rapport évalue la progression des nouvelles implémentations technologiques telles que le XDR. Il identifie également des points d'amélioration pour renforcer les partenariats public-privé, où une meilleure nous permettra de conserver une longueur d'avance sur nos adversaires.* »

L'enquête, basée sur une étude internationale menée par Vanson Bourne, repose sur l'avis de 900 professionnels de la cybersécurité issus d'organisations employant au moins 500 collaborateurs, dont 200 professionnels basés dans trois pays de l'OTAN : l'Allemagne, le Royaume-Uni et la France.

Adoption des technologies de cybersécurité. En Allemagne, la modernisation de la cybersécurité dans le cloud est considérée comme prioritaire dans le processus d'implémentation. Parmi les répondants, 40 % déclarent avoir entièrement implémenté la technologie la plus avancée du domaine. Cependant, seuls 27 % affirment avoir mis en place les fonctionnalités EDR-XDR (détection des terminaux et détection et réponse étendues).

Parmi les répondants du Royaume-Uni, 37 % déclarent avoir intégralement mis en œuvre la solution EDR-XDR et entrepris de moderniser la cybersécurité dans le cloud, des priorités qui sont passées devant l'authentification à facteurs multiples (MFA) et l'approche Zero Trust.

Côté français, 47 % des répondants affirment avoir entièrement déployé l'authentification à facteurs multiples, se plaçant ainsi devant leurs pairs britanniques et allemands.

Risque de la chaîne d'approvisionnement logicielle. La majorité (82 %) des professionnels interrogés dans le monde estiment que la gestion des risques de la chaîne d'approvisionnement logicielle est d'importance élevée ou critique pour la sécurité nationale.

Au Royaume-Uni, 76 % des personnes ayant répondu au sondage considèrent ces politiques et processus comme extrêmement ou très difficiles à mettre en œuvre. En conséquence, seuls 39 % déclarent les avoir entièrement implémentés.

En Allemagne et en France, 63 % et 58 % des répondants mettent respectivement en cause la difficulté de ces politiques et processus. Ainsi, seuls 40 % des professionnels allemands et 36 % des professionnels français confirment avoir mis en place la totalité de ces mesures.

Dans l'ensemble, les répondants européens s'accordent à dire que les normes de sécurité logicielle bénéficieraient de la mise en place par le gouvernement de normes officielles plus sévères. Cependant, seuls 56 % des répondants allemands, 51 % des répondants britanniques et 48 % des répondants français se déclarent favorables à des obligations légales en matière de cybersécurité dans l'ensemble du secteur des logiciels.

Les compétences en cybersécurité au cœur des enjeux. Si les obstacles identifiés sont nombreux, la question de la rareté des talents est mise en évidence dans les trois pays. En Allemagne, au Royaume-Uni et en France, ce sont respectivement 48 %, 41 % et 35 % des répondants qui reconnaissent dans le manque de compétences en interne un obstacle de taille aux efforts d'implémentation. De même, près d'un tiers de l'échantillon évoque le manque d'expertise en matière d'implémentation comme un défi majeur. En écho à ces résultats, des lacunes similaires sont constatées aux États-Unis et en Asie Pacifique, où les compétences en cybersécurité font également défaut.

Palma ajoute : « *Nous savons déjà qu'il existe des lacunes à combler en matière de cyber-compétences, mais ce rapport révèle qu'elles sont également un frein à l'implémentation des dernières innovations. Les avantages que les États-Unis et leurs alliés nous prêtent en matière d'innovation ne valent plus rien si nous ne sommes pas en mesure de mettre en place ces solutions. Nous devons étudier la façon dont sont formés les meilleurs talents afin de reproduire le processus à grande échelle*. »

Partenariats public-privé. Dans le domaine de la cybersécurité, 95 % des répondants allemands et français, et 86 % des répondants britanniques trouvent que les partenariats entre les entreprises et leurs gouvernements respectifs pourraient être encore améliorés.

Au Royaume-Uni, en Allemagne et en France, 52 %, 46 % et 35 % des répondants, respectivement, se déclarent favorables à une formule combinant notification des incidents et assurance responsabilité afin de faciliter le partage des données sur les cyberattaques entre les acteurs concernés : organisations, partenaires gouvernementaux et audiences du secteur. De même, 44 % des répondants britanniques et 41 % des répondants français et allemands aspirent à une coopération plus étroite en matière de gestion des cyberincidents lorsque des attaques et campagnes sont lancées.

Concernant le type de données que le gouvernement devrait partager pour aider les organisations à mieux se protéger, près de deux tiers (60 %) des professionnels britanniques souhaitent recevoir plus de données sur les campagnes de cyberattaques en cours. De leur côté, près de la moitié des

répondants allemands expriment le souhait de recevoir plus d'informations sur les différents groupes d'acteurs malveillants et les auteurs de cybercrimes. Chez les répondants français, 88 % déclarent préférer les données sur la vulnérabilité de la cybersécurité à tout autre type de données.

Pour plus d'informations, veuillez consulter les ressources suivantes :

- *Kit média du Cyber Readiness*
- *Rapport Cyber Readiness* de Trellix – préparation, perception et partenariats
- Blog récapitulatif des résultats en Europe (Allemagne, Royaume-Uni, France)

À propos de Trellix

Trellix est une entreprise internationale tournée vers le futur, qui réécrit l'avenir de la cybersécurité. Sa plateforme ouverte et native XDR, développée pour la détection et la réponse étendues, aide les entreprises à consolider la protection et la résilience de leurs opérations face aux menaces avancées qu'elles rencontrent aujourd'hui. Les experts en sécurité de Trellix s'appuient sur un large écosystème de partenaires pour accélérer l'innovation technologique grâce au machine learning et à l'automatisation, afin d'accompagner plus de 40 000 entreprises et clients gouvernementaux. Pour en savoir plus, rendez-vous sur https://trellix.com.