ARMIS®

L'ÉTAT DE
CYBERGUERRE

RAPPORT ARMIS SUR L'ÉTAT DE CYBERGUERRE ET LES TENDANCES : 2022-2023

ANALYSE PAYS PAR PAYS

FRANCE

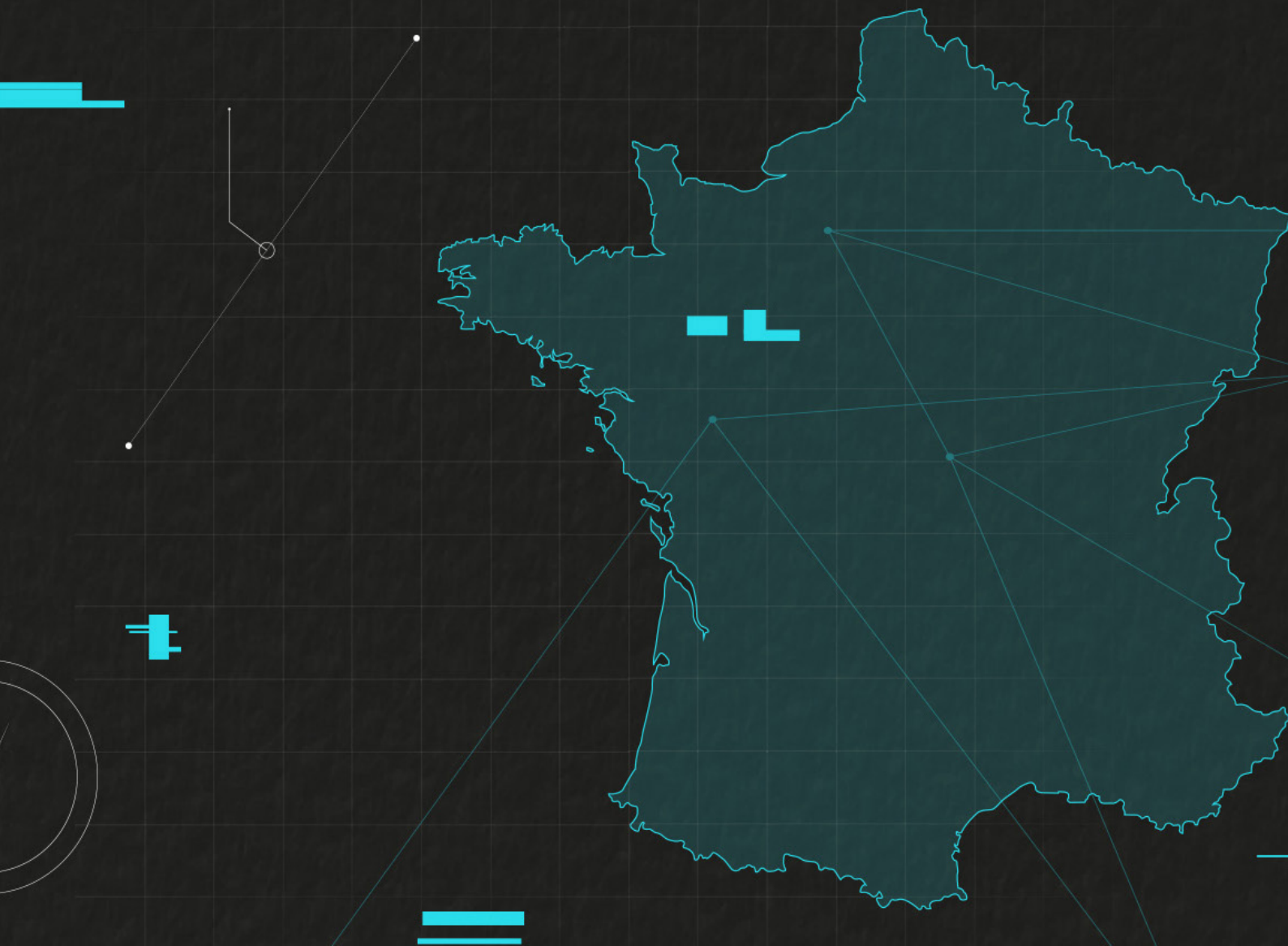


TABLE DES MATIÈRES

INTRODUCTION

Si vous avez lu le **Rapport Armis sur l'état de cyberguerre et les tendances à l'échelle mondiale : 2022-2023**, vous savez qu'il est essentiel pour les chefs d'entreprise et leaders IT de comprendre l'évolution du paysage des menaces dans un contexte de cyberguerre, afin qu'ils puissent améliorer leur posture de cybersécurité pour se défendre contre ces attaques. Pour préparer ce rapport, Armis a commandé une étude menée auprès de 6 021 professionnels de l'informatique et de la sécurité dans le monde entier afin de décrypter les tendances mondiales concernant les sentiments des professionnels de la sécurité sur la cyberguerre, les modèles d'attaque, les dépenses liées à la cybersécurité, etc. Les réponses ont été recueillies entre le 22 septembre 2022 et le 5 octobre 2022.

Armis a utilisé les données de sa plateforme primée Asset Intelligence and Security Platform pour analyser les résultats de l'enquête par rapport aux tendances des données du monde réel. Les données exclusives de la plateforme Armis recueillies entre le 1er juin 2022 et le 30 novembre 2022 ont confirmé que les cyberattaques n'ont pas ralenti, mais se sont plutôt aggravées. Les menaces contre la clientèle internationale d'Armis ont augmenté de 15 % entre septembre et novembre par rapport au trimestre précédent. En outre, Armis a identifié que les menaces visant des organisations essentielles représentent le pourcentage le plus élevé, les établissements de santé se plaçant au deuxième rang des entreprises les plus ciblées par rapport aux autres secteurs d'activité.

Outre ces conclusions à l'échelle mondiale, Armis a préparé des conclusions par zones géographiques et une analyse pays par pays afin d'offrir un éclairage unique et localisé, plus pertinent pour chaque lecteur en fonction de sa localisation géographique et des pays dans lesquels son entreprise opère. **Pour cette analyse pays par pays, nous allons nous concentrer sur les résultats de notre enquête menée auprès de 501 personnes basées en France et travaillant dans des secteurs tels que la santé, la fabrication, la vente au détail, les services financiers, etc.**

RÉSUMÉ DES CONCLUSIONS

Dans l'ensemble, Armis a dégagé quatre tendances clés lors de l'analyse des réponses des professionnels de l'informatique et de la sécurité d'entreprises françaises par rapport à d'autres participants à l'échelle internationale (EMEA, États-Unis et APJ). Ci-dessous, nous poussons plus loin l'analyse de ces résultats et des tendances qu'ils dessinent.

Le contexte géopolitique mondial et la récente crise sanitaire ont souvent mis en lumière le manque de préparation de certains gouvernements de pays industrialisés en matière de gestion des questions de cybersécurité. Plusieurs organisations, insuffisamment préparées ou inconscientes des vulnérabilités de leurs infrastructures informatiques, ont été victimes de tentatives d'extorsion qui peuvent prendre plusieurs formes. Aucun secteur n'a été épargné par ces attaques, à commencer par les activités dites stratégiques ou cruciales pour le bon fonctionnement des entreprises. La France n'y a pas échappé ces dernières années et continue de subir des attaques à répétition ciblant des organisations publiques et privées. Globalement, le pays doit faire face à une crise de confiance dans la capacité des autorités à protéger les équipements. Armis a interrogé les professionnels de l'informatique et de la sécurité sur le degré de confiance qu'ils accordent au gouvernement et 8 % ont déclaré n'avoir aucune confiance dans la capacité des autorités à protéger les équipements. En revanche, 16 % affirment avoir une confiance totale dans le gouvernement. Alors que l'UE s'apprête à adopter des réglementations plus strictes en matière de cybersécurité, il est clair que les avis diffèrent grandement quant au niveau de confiance envers le gouvernement. Le rapport révèle également que les entreprises françaises ne sont peut-être pas tout à fait prêtes à adopter ces nouvelles réglementations.

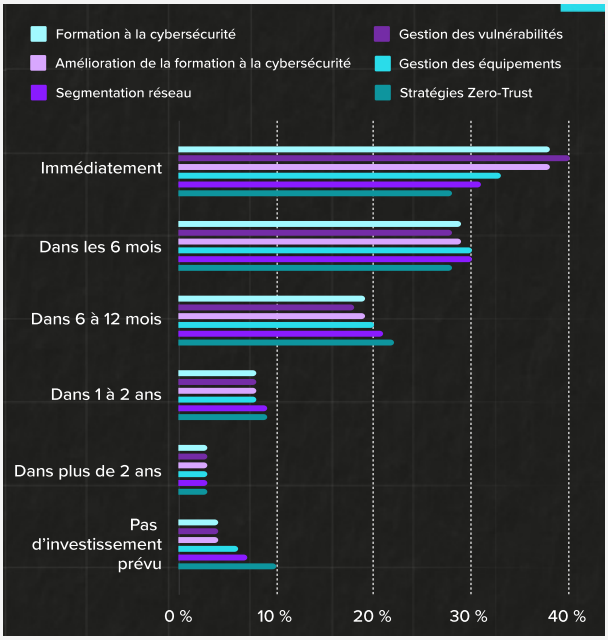
EMEA

En 2022, la région EMEA a assisté avec consternation à l'invasion de la nation souveraine d'Ukraine. Du fait de l'instabilité géopolitique liée à la guerre conventionnelle et à la cyberguerre, les conséquences du conflit se propagent comme des ondes de choc dans toute la région. L'imprévisibilité de l'approvisionnement en denrées alimentaires, la pénible crise énergétique et la vague de cyberattaques dirigées contre les fonctions les plus stratégiques de la société sont autant de facteurs qui contribuent à revoir les dépenses et les priorités dans de nombreux secteurs d'activité. Le rapport confirme l'augmentation des cyberattaques, mettant en évidence que près de 3 entreprises sur 5 (58 %) ont déjà connu au moins un incident de cybersécurité. Parmi les personnes interrogées, 25 % ont confirmé que le nombre de menaces pesant sur leur entreprise s'est multiplié.

Des mesures sont prises pour garantir une bonne protection, mais à ce jour, moins de la moitié (44 %) des professionnels de l'informatique et de la sécurité s'accordent à dire que leur organisation a mis en place des programmes et des pratiques pour contrer les menaces de la cyberguerre. Les personnes interrogées ont fait état du manque de préparation de leur entreprise, dans la mesure où plusieurs problématiques restent à traiter.

- Seuls 46 % des professionnels de l'informatique et de la sécurité de la région EMEA sont tout à fait d'accord pour dire qu'ils savent qui contacter en cas d'activité suspecte.
- Seuls 76 % des professionnels de l'informatique et de la sécurité de la région EMEA ont indiqué collaborer avec d'autres acteurs du secteur lorsqu'il s'agit de partager des informations sur les menaces, un chiffre inférieur au pourcentage moyen aux États-Unis et dans la région APJ. Même si ce pourcentage est élevé, il indique néanmoins qu'il reste encore des efforts à faire si l'on souhaite protéger tous les domaines contre les cyberattaques.
- Seuls 33 % des professionnels de l'informatique et de la sécurité de la région EMEA ont rapporté aux autorités un acte de cyberguerre, un chiffre inférieur à celui enregistré aux États-Unis (63 %) et dans la région APJ (61 %).
- Près de 2 professionnels de l'informatique et de la sécurité sur 10 (18 %) dans la région EMEA ont déclaré que leur organisation n'avait prévu aucun plan d'urgence en cas de détection d'une cyberguerre.
- Un tiers seulement (33 %) des professionnels de l'informatique et de la sécurité disposent d'un plan de cyberguerre validé avec des bonnes pratiques établies et la mise en place de mesures appropriées et proportionnées.
- En outre, moins de la moitié (49 %) des entreprises recourent à la formation des collaborateurs ou à la restriction des droits d'administration du réseau (40 %) comme pratique courante. Elles sont encore moins nombreuses à avoir mis en place des pratiques de cybersécurité, par exemple, la création d'une culture d'entreprise axée sur la sécurité (37 %), l'investissement dans une assurance cybersécurité (31 %) et la mise en œuvre d'un cadre de gestion des cyber-risques (31 %).

Il existe un décalage entre la confiance dans le niveau de préparation face aux attaques de cybersécurité (84 %) et la réalité : des investissements sont nécessaires pour combler ce fossé, tant au niveau des outils que des services. Invités à préciser sous quel délai des investissements seront réalisés sur certains aspects, les professionnels de l'informatique ont donné les réponses suivantes :



DES RÉGLEMENTATIONS RÉSOLUMENT TOURNÉES VERS L'AVENIR

Les gouvernements, les services de sécurité et les autorités compétentes concernées continuent de mettre l'accent sur la nécessité d'améliorer la posture de cybersécurité et le besoin impératif de mettre en place une stratégie davantage cyber-résiliente. La récente loi de l'UE sur la cyber-résilience s'appuie sur l'actuelle directive européenne sur la cybersécurité de 2016, actualisant ainsi les exigences du bloc européen pour une cybersécurité renforcée de la part des États membres. Avant cette loi de l'UE sur la cyber-résilience, la pression en matière de cybersécurité était exercée principalement sur les utilisateurs des produits, tant les entreprises que les particuliers. Désormais, le fabricant partagera lui aussi une part plus importante de cette responsabilité. Ce partage des responsabilités peut grandement contribuer à l'amélioration de l'ensemble de la situation. L'UE a également publié la directive NIS2, qui met en lumière de nombreux autres secteurs et prévoit des amendes, des sanctions et des pénalités en cas de mauvaise gestion des risques, d'absence d'hygiène informatique de base et de retards excessifs dans la mise en place de mesures correctives.

L'émergence de réglementations est un excellent moyen de lancer le débat et contribuera certainement à combler les déficits d'investissement dans certains outils et à hiérarchiser leur importance, mais il reste encore un long chemin à parcourir pour sécuriser les vulnérabilités critiques introduites par la prolifération exponentielle des équipements connectés. 37 % des personnes interrogées s'accordent à dire que les appareils connectés sont une priorité absolue en cas d'attaque de cyberguerre.

Au-delà des efforts internes, les professionnels de l'informatique estiment que l'Union européenne et ses États membres devraient également renforcer la coopération avec d'autres alliés dans le monde. Plus de la moitié (61 %) ont déclaré qu'ils seraient favorables à la création d'une ligue de cyberdéfense si leur pays était entraîné dans un conflit de cyberguerre.

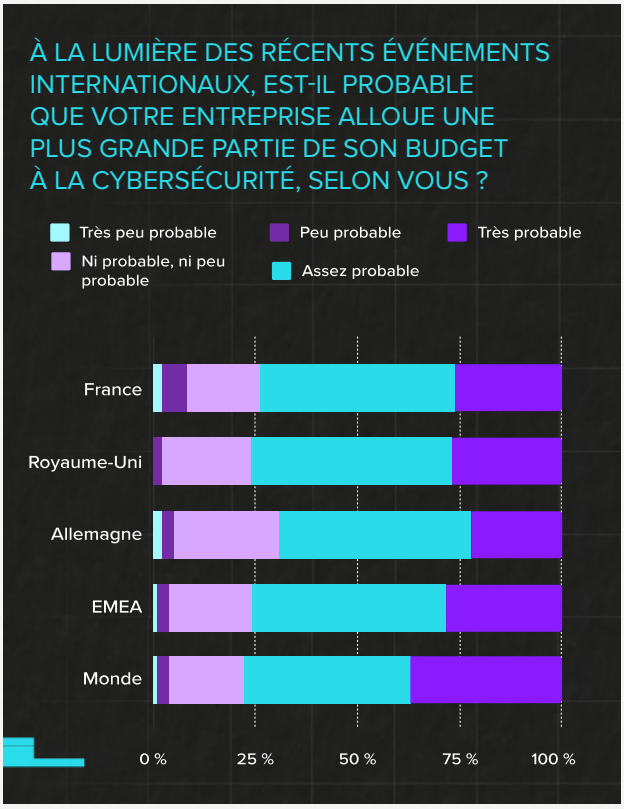
CYBERSÉCURITÉ : CRISE DE CONFIANCE DES ENTREPRISES FRANÇAISES À L'ÉGARD DU GOUVERNEMENT

RÉGLEMENTATIONS PROCHAINEMENT EN VIGUEUR ET NIVEAU DE PRÉPARATION

Plus de 4 personnes interrogées sur 5 (84 %) sont d'accord pour impliquer le secteur public et le secteur privé dans l'établissement des politiques publiques en matière de cybersécurité, à l'instar de ce qui a été décidé lors du Grenelle de l'environnement en 2007. Même si ces pourcentages élevés semblent montrer qu'il y aura un renforcement de la réglementation et une plus grande implication des entreprises dans les politiques publiques, seules 53 % ont mis en place la sauvegarde des données comme pratique de cybersécurité au sein de leur organisation. Elles sont encore moins nombreuses à utiliser des logiciels anti-malware et des pare-feu (48 %), à crypter les données (46 %) ou à mettre en œuvre un cadre de gestion des cyber-risques (41 %). Cela pourrait suggérer qu'elles ne sont pas prêtes à adopter une réglementation plus stricte.

LES INQUIÉTUDES DES ENTREPRISES COMPTE TENU DU CONTEXTE GÉOPOLITIQUE SONT-ELLES FONDÉES ?

On aurait pu penser que les événements récents auraient incité les organisations sensibles à la conjoncture à accroître leurs efforts et leurs investissements en matière de cybersécurité. S'il est vrai que l'actualité internationale actuelle et récente va pousser 74 % des entreprises à augmenter leurs investissements en matière de cybersécurité, 18 % des personnes interrogées en France ne seraient toutefois pas en mesure de dire si leur entreprise prévoit d'allouer un budget plus important à ce poste, et près de 2 % pensent qu'il est très peu probable que leur organisation le fasse. Ces chiffres diffèrent de ceux enregistrés dans d'autres zones géographiques, comme le Royaume-Uni, où 22 % des personnes interrogées n'en ont aucune idée. En Allemagne, 26 % ne sont pas en mesure de se prononcer et 2 % ont de sérieux doutes quant à l'affectation d'un budget plus important. Étonnamment, certaines organisations ne tiennent pas compte des indicateurs sociaux et économiques lorsqu'elles décident de leurs orientations budgétaires.



LE SECTEUR DE LA SANTÉ SOUS PRESSION, MAIS PEU TOUCHÉ PAR LES ATTAQUES

Le secteur de la santé en France a été victime d'attaques récurrentes pendant et après la

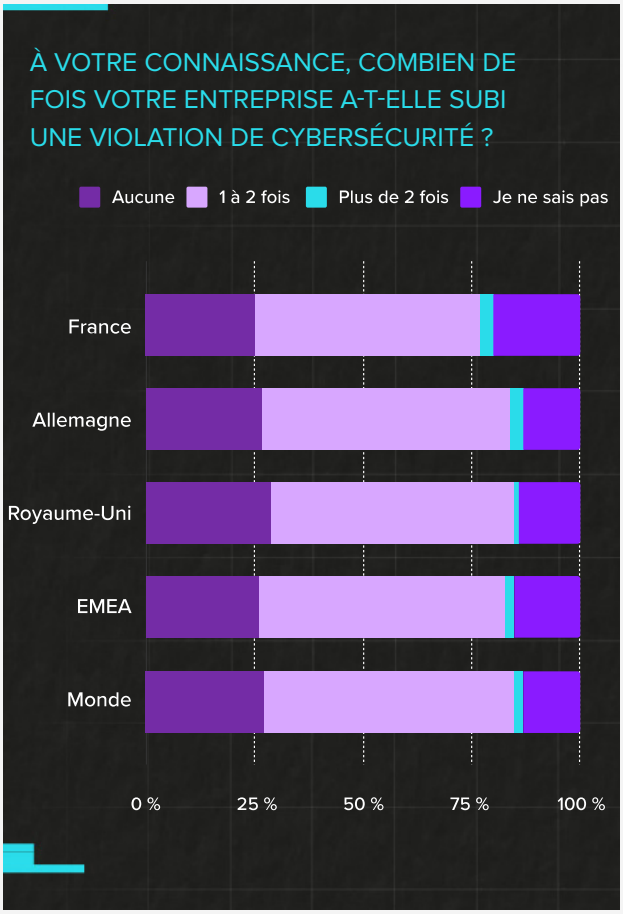
pandémie. Cependant, malgré un contexte particulièrement difficile et les conséquences de ces attaques sur la continuité des soins, on constate que le secteur semble peu inquiet. 22 % des personnes interrogées ne sont pas très inquiètes, tandis que 9 % ne le sont pas du tout. En revanche, 45 % se disent assez inquiètes et 13 % très inquiètes. Nous en déduisons que les attaques ne sont pas encore perçues comme un facteur pouvant influencer directement les personnes interrogées. Devons-nous attribuer ce manque d'intérêt au caractère répété des attaques, les rendant habituelles, au point qu'elles ne méritent plus d'attention ?

Cette attitude typiquement française du « je ne me sens pas concerné » ne se retrouve pas dans les autres pays, ou alors dans une moindre mesure. En Allemagne, par exemple, 53 % des personnes interrogées ont déclaré être inquiètes et 0 % ont déclaré ne pas l'être du tout. Seules 11 % des personnes interrogées ne sont pas du tout préoccupées par cette menace. De l'autre côté de la Manche, l'approche est également différente : au Royaume-Uni, 17 % ne se sentent tout simplement pas très inquiètes, 3 % ne se sentent pas du tout inquiètes et 49 % font part d'une certaine inquiétude.

QUELS ENSEIGNEMENTS TIRER DE L'OPACITÉ OU DE LA COMMUNICATION DES ENTREPRISES SUR LES CYBERATTAQUES ?

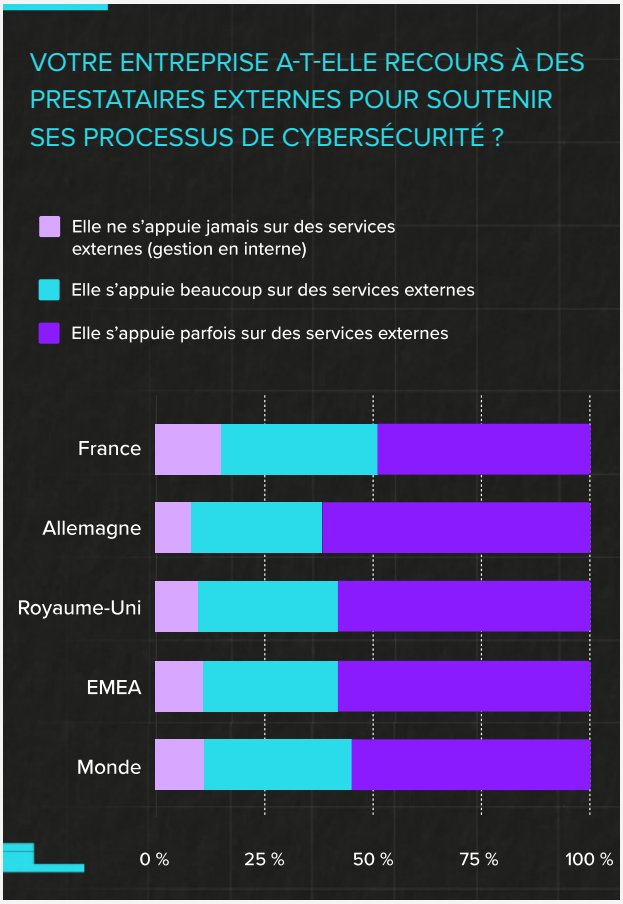
Les organisations doivent avoir une stratégie à la fois réactive et proactive en matière de cybersécurité. Et si le nombre d'attaques ne diminue pas, la question suivante se pose : quelles leçons en tirer et comment aider l'écosystème lorsque son organisation en a été victime ?

Afin de préserver leur image de marque et de limiter l'impact sur leur activité, de nombreuses entreprises ne communiquent pas sur les attaques subies. Il s'agit pourtant de précieuses informations qui peuvent être utiles pour comprendre les processus utilisés par les cybercriminels. Une mauvaise communication autour des attaques peut aggraver les conséquences. Malgré cela, 20 % des Français interrogés disent ne pas savoir si leur entreprise a déjà été touchée par une cyberattaque. Et seulement la moitié (52 %) disent avoir été informés que l'entreprise a été victime d'une attaque 1 ou 2 fois. Chez leurs voisins allemands, par exemple, seuls 13 % disent ne pas être tenus informés du tout, contre 57 % qui disent avoir été informés que l'entreprise a été ciblée par une attaque 1 ou 2 fois. Du côté des Britanniques, 13 % n'ont pas eu connaissance d'attaques qui les auraient ciblés, et 56 % savent que l'entreprise a déjà été touchée par une attaque à 1 ou 2 reprises. Quels enseignements pouvons-nous en retirer ? Les organisations sont peut-être plus touchées que nous ne le pensons et il y a aussi des efforts à faire dans ce domaine.



RESSOURCES INTERNES OU SOUS-TRAITANTS : À QUI SE FIER ?

Quel rôle les fournisseurs informatiques jouent-ils dans la mise en place de protocoles de sécurité ? Il est vrai que les entreprises subissent de plein fouet les attaques à répétition. 15 % des personnes interrogées déclarent que leur organisation n'a jamais fait appel à un prestataire pour la cybersécurité, mais qu'elle s'appuie plutôt sur les équipes en interne. 49 % ont recours ponctuellement à un prestataire de services. Là encore, nous comprenons qu'elles ont réalisé un diagnostic pour évaluer les vulnérabilités existantes ou qu'elles ont été victimes d'une attaque et dans l'incapacité d'y répondre en interne. En Allemagne, 8 % disent ne pas s'appuyer sur les compétences d'un prestataire informatique externe, tandis que 61 % disent s'appuyer sur les compétences d'un prestataire de services extérieur à l'organisation. Au Royaume-Uni, près de 10 % ont déclaré ne pas utiliser les compétences d'un prestataire de services, tandis que 58 % ont déclaré y avoir parfois recours.



EN QUOI CES CONCLUSIONS SONT-ELLES IMPORTANTES ?

Nous sommes conscients que le chemin à parcourir dans la lutte contre les cyberattaques s'annonce long. Nous observons que malgré le contexte géopolitique instable, les entreprises ne semblent pas tirer les leçons des événements macroéconomiques. Du côté des collaborateurs, soit certains ne sont pas informés des attaques visant leur organisation, soit leur employeur a recours à des prestataires de services pour pallier le manque de ressources internes. La lutte contre les cyberattaques doit donc passer par une prise de conscience générale et bien sûr un investissement massif dans la formation des collaborateurs ou le recours à des partenaires disposant de l'expertise nécessaire.

> *« Aujourd'hui, nous avons suffisamment de recul pour dire que si la crise sanitaire récente a accéléré les cyberattaques contre les organisations privées et publiques, elle a également montré que les infrastructures informatiques sont vieillissantes et inadaptées face aux nouvelles menaces. Notre étude révèle que nous n'avons malheureusement pas su tirer les leçons du passé. En effet, les dirigeants continuent de ne pas faire de la protection des équipements une priorité : l'augmentation des budgets dédiés à la refonte des infrastructures n'est pas au cœur des débats, le recours à des prestataires experts en cybersécurité reste rare et se limite à des audits ponctuels, sans continuité, et le contexte géopolitique et économique ne semble pas avoir une forte influence dans la prise de décision des entreprises. Sans vouloir brosser un tableau trop négatif de l'état de la cybersécurité dans la région EMEA, nous sommes confrontés à une forme de paralysie de la cybersécurité, renforcée par des crises successives, ce qui nuit à la performance. »*
>
> **JEAN-MICHEL TAVERNIER**
> DIRECTEUR FRANCE CHEZ ARMIS

QUE PEUT FAIRE VOTRE ENTREPRISE POUR SE PROTÉGER ?

Alors, que peuvent faire les organisations pour se protéger ? La détection précoce et la surveillance continue sont le meilleur moyen d'améliorer la posture de sécurité d'une organisation et de corriger rapidement les problèmes. Après tout, vous ne pouvez pas corriger un problème dont vous n'avez pas connaissance et vous ne pouvez pas protéger un équipement sur lequel vous n'avez pas de visibilité. C'est là qu'Armis peut vous aider.

PLATEFORME ARMIS ASSET INTELLIGENCE

La **plateforme Armis Asset Intelligence** offre une visibilité unifiée et la sécurité pour tous les types d'équipements, y compris IT (technologies de l'information), IoT (Internet des objets), OT (technologies opérationnelles), IoMT (Internet des objets médicaux), Cloud, et IoT cellulaire, managés et non managés. Déployée sous forme de plateforme SaaS (software-as-a-service) sans agent, la solution Armis s'intègre facilement dans les piles informatiques et de sécurité existantes afin de fournir rapidement les renseignements contextuels nécessaires à l'amélioration de votre posture de sécurité, sans perturber les opérations ou les flux de travail en cours. Armis aide ses clients à se protéger contre les risques opérationnels et les cyber-risques invisibles, gagner en efficacité, optimiser l'utilisation des ressources et à innover en toute sécurité avec de nouvelles technologies afin de développer leur activité, que la menace soit liée à la cyberguerre ou autre.

Inscrivez-vous dès aujourd'hui à une **évaluation de la sécurité et des risques** pour découvrir quels équipements sont les plus vulnérables. Utilisez ces informations pour établir vos priorités en matière d'atténuation des risques et garantir une conformité totale avec des cadres réglementaires qui vous obligent à identifier et à hiérarchiser toutes les vulnérabilités.

Pour demander une démonstration personnalisée. d'Armis, consultez la page : armis.com/demo.

Pour approfondir les résultats du rapport Armis sur l'état de cyberguerre et les tendances : 2022-2023 à l'échelle mondiale, consultez la page : **armis.com/cyberwarfare.**

L'ÉTAT DE
CYBERGUERRE

À PROPOS D'ARMIS

Armis, leader de la sécurité et de la visibilité sur les équipements, fournit la première plateforme d'intelligence des équipements unifiée du secteur, conçue pour gérer la nouvelle surface d'attaque étendue que créent les équipements connectés. Les sociétés classées au Fortune 100 font confiance à notre protection continue et en temps réel pour voir tous les équipements managés, non managés dans des environnements IT, Cloud, IoT, IoT des appareils médicaux (IoMT), des technologies opérationnelles (OT), des systèmes de contrôle industriel (ICS) et la 5G, le tout avec un contexte complet. Armis offre une gestion passive des cyberéquipements, la gestion des risques et la mise en application automatisée. Armis est une société privée dont le siège social est situé en Californie.

armis.com

info@armis.com

20230110-1

ARMIS®