SOPHOS

Le puzzle impossible de la cybersécurité

Résultats d'une enquête indépendante réalisée pour Sophos auprès de 3 100 responsables informatiques

Livre blanc Sophos Juin 2019

Sommaire

Le puzzle impossible de la cybersécurité

Résultats d'une enquête indépendante réalisée pour Sophos auprès de 3 100 responsables informatiques

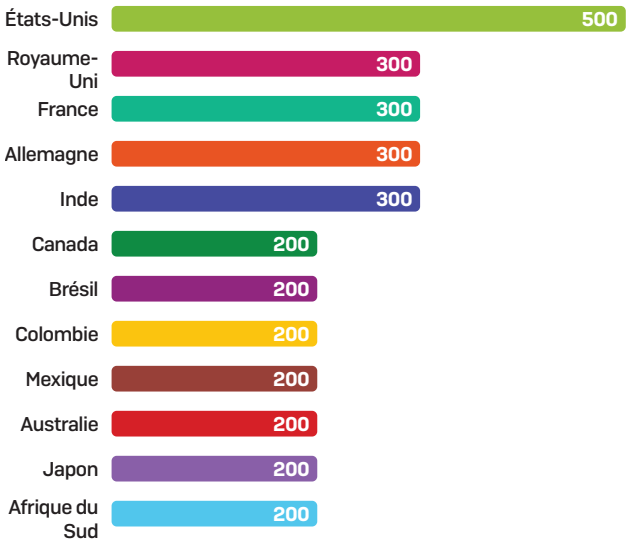
Force est de constater que la cybersécurité n'est aujourd'hui pas plus simple qu'hier. Les technologies de protection sont sans cesse améliorées, mais les cybercriminels continuent de les contourner à un rythme soutenu. Réussir à surmonter les menaces toujours plus complexes est une lourde tâche pour les équipes informatiques déjà bien occupées.

Pour comprendre ces défis, Sophos a commandé une enquête indépendante sur les expériences de 3 100 responsables informatiques dans 12 pays différents. Conduite par le cabinet de recherche Vanson Bourne, cette enquête a révélé des informations précieuses sur les niveaux et les types d'attaques subies, et les difficultés rencontrées pour gérer la cybersécurité.

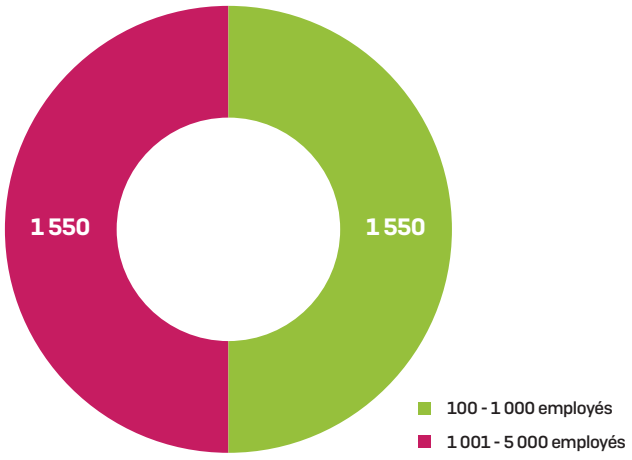
L'enquête

Le cabinet d'études britannique Vanson Bourne a interrogé 3 100 décideurs informatiques entre décembre 2018 et janvier 2019. Afin de fournir une répartition par taille représentative dans chaque pays, les participants ont été classés de manière équitable entre des entreprises allant de 100 à 1 000 utilisateurs et de 1 001 à 5 000 utilisateurs.

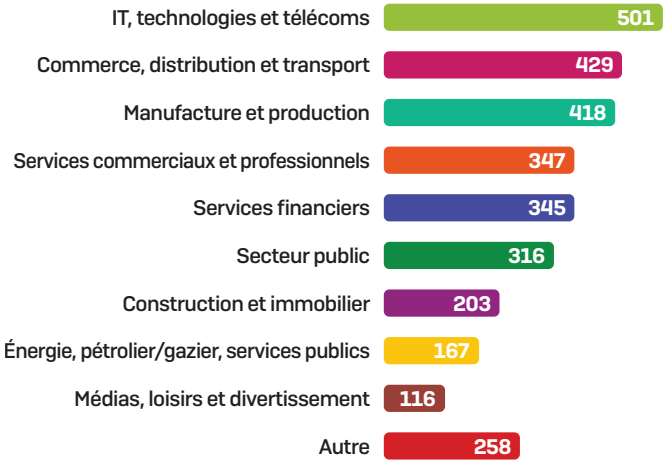
Nombre de participants par pays



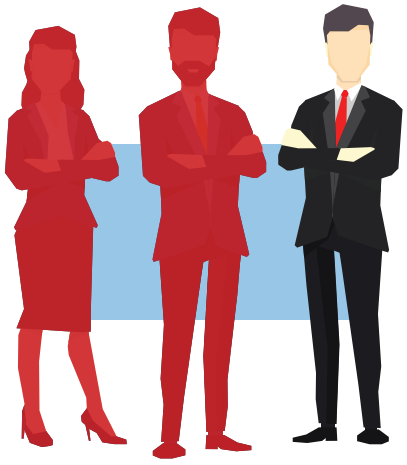
Répartition des participants par taille d'entreprise



Répartition des participants par secteur



Deux tiers des entreprises ont été victimes d'une cyberattaque en 2018



Il a été demandé à tous les répondants s'ils avaient été victimes d'une cyberattaque au cours de l'année passée ; c'est-à-dire ayant subi une attaque qui les a empêchés d'accéder à leur réseau ou leurs systèmes endpoint. 68 % ont répondu oui. Le nombre d'attaques subies par ces entreprises était en moyenne de 2, mais 10 % d'entre elles ont été la cible de 4 attaques ou plus.

Un élément préoccupant est que 9 répondants sur 10 (90,5 %) ont déclaré avoir en place une cyber protection à jour au moment de l'attaque ; ou pour les entreprises ayant subi plusieurs attaques, au moment de l'attaque la plus significative. Parmi les pays interrogés, les répondants en France étaient les plus nombreux à avoir une protection à jour en place (97,5 %), tandis que ceux en Colombie étaient les moins nombreux avec seulement 7 répondants sur 10 (70,9 %).

91 % des entreprises avaient une sécurité Endpoint à jour au moment de l'attaque

Cela démontre que, malgré les meilleures intentions et pratiques, les menaces parviennent à leurs fins. Cela peut être dû à des faiblesses de la cybersécurité, ou à des failles de sécurité non protégées ou une protection non exhaustive. Par exemple, ce n'est pas parce qu'une entreprise avait une protection Endpoint à jour que tous les autres appareils étaient sécurisés.

Les cyberattaques génèrent de nombreuses préoccupations

Les risques de cyberattaque génèrent de nombreuses préoccupations pour les responsables informatiques, notamment :

Perte des données La principale préoccupation exprimée par les répondants. 31 % l'ont classée en tête de leurs préoccupations et plus des deux tiers (68 %) l'ont placée dans leur top 3.

Coût Pour 21 % des répondants, le coût (financier et temps/efforts investis) du traitement de la question constitue leur principale préoccupation.

Préjudice pour l'entreprise Plus de la moitié des responsables informatiques (56 %) ont classé cette préoccupation dans leur top 3 et 21 % l'ont classé en première position.

Curieusement, l'informatique apparait comme un sport d'équipe, où les responsables font passer le bien-être de leur département avant leur situation personnelle. Pour 13 % des répondants, leur plus grande préoccupation était le ternissement de l'image de l'équipe informatique au sein de l'entreprise, presque le double (7 %) de ceux ayant placé la sécurité de l'emploi personnel en haut de la liste.

Pourquoi les entreprises peinent toujours à réduire les cyber risques

Comme le montrent les résultats, malgré les investissements dans des technologies de sécurité, la norme est désormais d'être touché par une cyberattaque. L'enquête a révélé 3 raisons principales expliquant pourquoi les entreprises peinent toujours à réduire les cyber risques.

N° 1 Les attaques viennent de toutes les directions

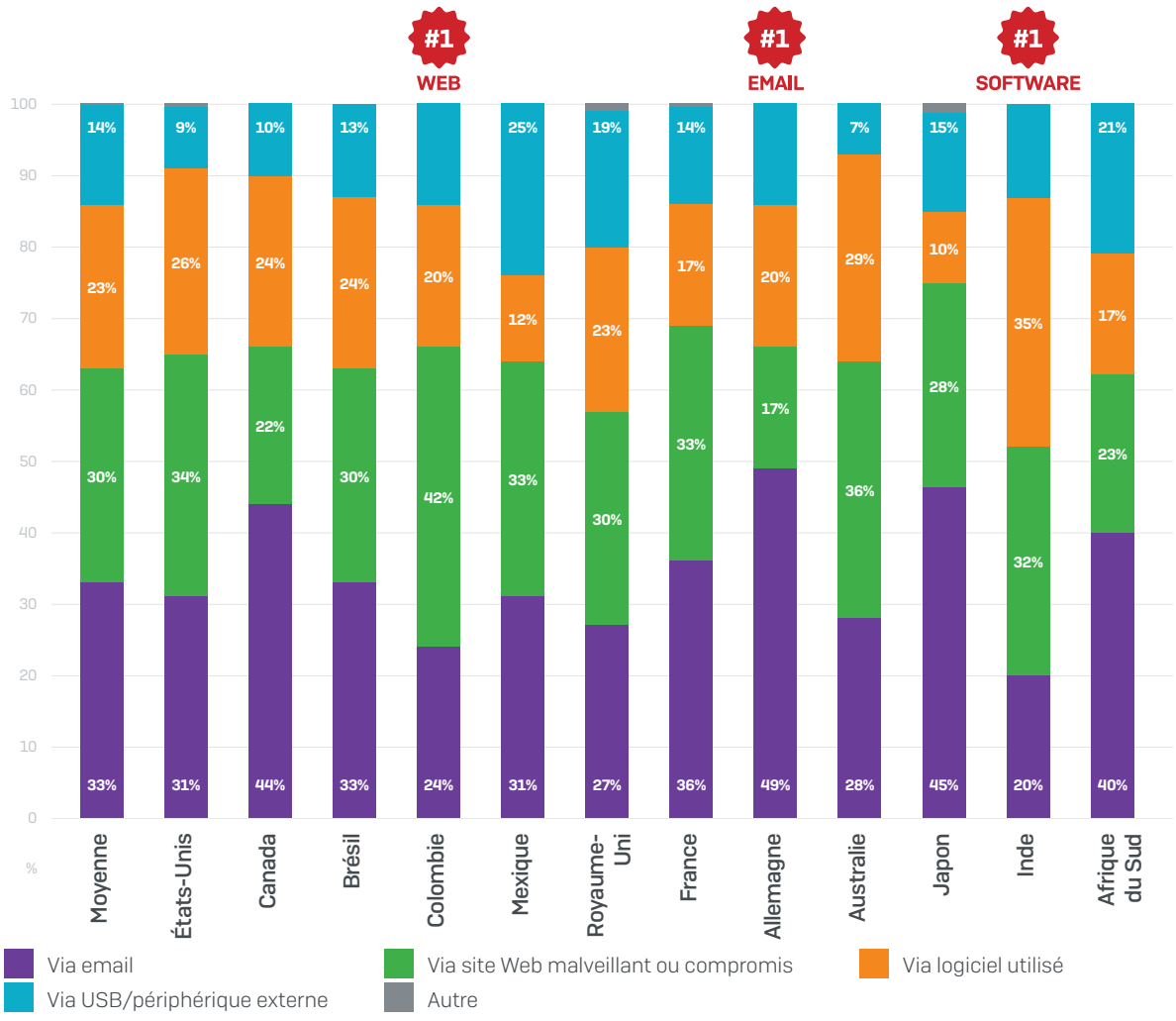
Il a été demandé aux répondants victimes d'une attaque au cours de l'année passée la manière dont la cyberattaque la plus grave était entrée dans leur environnement. Les résultats ont révélé que, lorsque les répondants ont identifié le point d'entrée d'une attaque, les emails en sont le principal vecteur et représentent 33 % des attaques. Étant donné la prévalence des attaques de phishing, cela n'est pas surprenant (nous y reviendrons plus loin). Le Web est également un vecteur majeur, identifié dans 3 attaques sur 10. Ensemble, les emails et le Web sont responsables de près des deux tiers des attaques.

Mais les responsables informatiques ne doivent toutefois pas se concentrer uniquement sur les emails et le Web. 23 % des attaques sont survenues grâce à une faille logicielle, et 14 % par une clé USB ou un périphérique externe. De plus, 20 % des responsables informatiques n'ont pas identifié l'origine de leur attaque la plus grave. Et malheureusement, si vous ne savez pas quelle porte est restée ouverte, vous ne pourrez pas la refermer facilement.

Comment la cyberattaque la plus grave ayant touché votre entreprise au cours de l'année passée est-elle entrée dans votre environnement ? (arrondi au nombre entier le plus proche) ***Base :*** *Répondants ayant identifié l'origine d'une attaque (1 685)*

En passant les données à la loupe, il apparaît que les vecteurs de menaces varient énormément à travers le monde. Le Web est un vecteur d'attaque courant en Colombie, tandis que les emails et les failles logicielles sont le premier vecteur respectivement en Allemagne et en Inde. Les clés USB/périphériques externes sont la source de 1 attaque sur 4 au Mexique.

Cela soulève une question intéressante : cette variation est-elle le résultat de mauvaises personnes utilisant différents vecteurs d'attaques dans différents pays, ou de différentes failles de sécurité dans toutes les régions géographiques étudiées ?



*Comment la cyberattaque la plus grave ayant touché votre entreprise au cours de l'année passée est-elle entrée dans votre environnement ? **Base :** Répondants ayant identifié l'origine d'une attaque (1 685)*

En matière de cybersécurité, les équipes informatiques doivent gérer un large éventail de risques. Nous avons demandé aux répondants ce qu'ils considèrent être le plus grand risque de sécurité. Étant donné les vecteurs d'attaque que nous venons de passer en revue, il n'est pas surprenant que le phishing (nº 1) et les exploits de logiciels (nº 2) arrivent en tête.

Cependant, en troisième position apparaît le facteur humain, c'est-à-dire le personnel de l'entreprise, les contractuels et les visiteurs. Nous autres humains sommes classés comme la troisième menace de sécurité par 44 % des répondants. Cela représente sans nul doute un autre type de défi de cybersécurité pour les équipes informatiques.

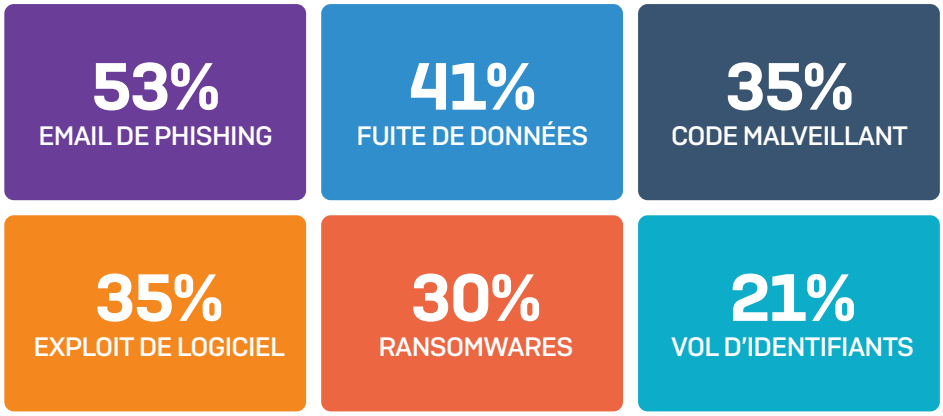
La sécurité du Wi-Fi préoccupe également les responsables informatiques avec plus d'un tiers (36 %) la plaçant dans leur top 3, suivie de près par les appareils inconnus, qui sont une préoccupation majeure exprimée par 3 répondants sur 10 (31 %).

Que considérez-vous comme un risque majeur de sécurité — combinaison de réponses classées en 1re, 2e et 3e position :

1. Emails de phishing **50 %**
2. Exploits de logiciel **45 %**
3. Humains (personnel, contractuels, visiteurs) **44 %**
4. Réseau Wi-Fi non sécurisé **36 %**
5. Appareils inconnus **31 %**

Nº 2 Les cyberattaques sont complexes, coordonnées et combinées

Les répondants dont les entreprises ont été touchées par une cyberattaque ont révélé avoir subi tout un éventail d'attaques au cours de l'année passée.



*Quels types de cyberattaques ont touché votre entreprise au cours de l'année passée ? **Base :** répondants au sein d'entreprise ayant été victime d'une ou plusieurs cyberattaques au cours de l'année passée (2 109)*

En additionnant ces chiffres, on dépasse les 100 %, ce qui montre que les attaques complexes à étapes successives sont devenues la norme. Par exemple, un email de phishing peut installer du code malveillant qui ensuite exploitera une faille dans un logiciel pour installer un ransomware. Ces chiffres élevés confirment également l'ampleur du défi que doivent relever les équipes informatiques.

Phishing : la cyberattaque la plus répandue

Sur les 2 109 entreprises touchées par une cyberattaque en 2018, plus de la moitié (53 %) ont été victime de phishing. En effet, le phishing est l'attaque la plus répandue dans tous les pays interrogés, à l'exception de la Colombie, où il arrive en seconde position. Sur l'ensemble des 3 100 répondants, plus d'un tiers (36 %) ont été victimes d'un email de phishing.

Exploits de logiciel : impact variable selon les pays

Parmi les entreprises touchées par une cyberattaque, il s'agit dans plus d'un tiers des cas (35 %) d'un exploit profitant d'une faille dans un logiciel. La propension à être touché par un exploit varie considérablement d'un pays à l'autre. Au Mexique, plus de la moitié des entreprises ont été victimes d'un exploit (51 %). C'est deux fois plus qu'au Brésil (22 %) et qu'en Afrique du Sud et au Japon (tous deux à 23 %).

Ransomwares : toujours là et aussi actifs

Malgré les rumeurs de disparition des ransomwares, ils sont bien toujours là et aussi actifs. 3 entreprises sur 10 (30 %) ont été touchées par un ransomware. Cependant, cette moyenne globale masque quelques variations régionales :

- La moitié (49 %) des répondants japonais ont déclaré avoir été touché par un ransomware, suivi par 43 % des Britanniques.
- Seulement 5 % des répondants mexicains ont été touchés par un ransomware, et seulement 13 % des Colombiens.

Nº 3 Pénurie de technologies, de personnel compétent et de temps

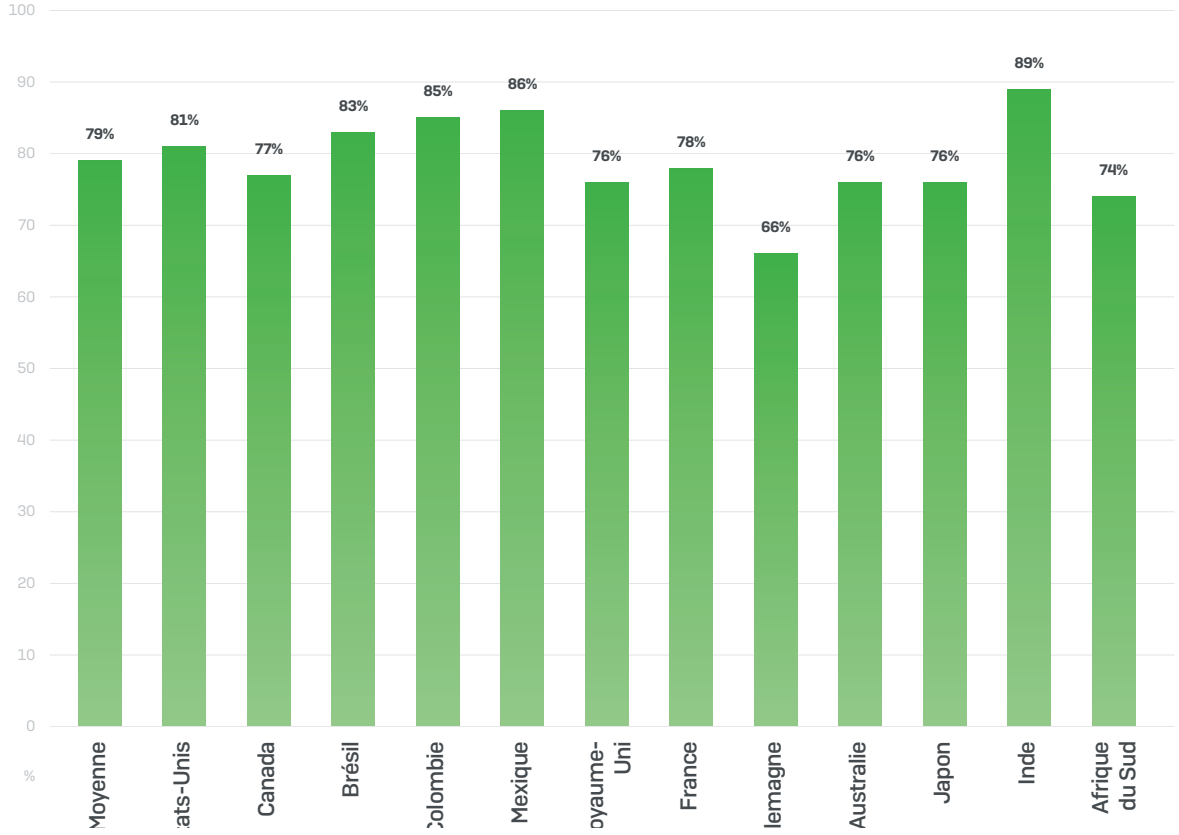
Comme nous l'avons vu, les entreprises font face à un large éventail d'attaques et doivent se protéger contre de nombreux vecteurs de menaces. Notre enquête a révélé que, en moyenne, les équipes informatiques passent 26 % de leur temps à gérer la cybersécurité.

Les entreprises indiennes y passent le plus de temps (32 %) et les équipes japonaises le moins (19 %). Les entreprises ayant été touchées par une cyberattaque ont tendance à consacrer plus de temps à la sécurité informatique (28 %) que celles n'ayant jamais été touchées (23 %).

Étant donné la grande variété et complexité des menaces, il n'est pas surprenant que 86 % des répondants déclarent avoir besoin de plus de personnel compétent en cybersécurité dans leur entreprise. Les entreprises ayant subi une attaque ont davantage besoin d'expertise en cybersécurité que celles qui ne l'ont pas été (89 % contre 79 %). Cela peut s'expliquer par le fait qu'elles ont plus de lacunes de sécurité à combler, ou par une prise de conscience accrue de la complexité des attaques d'aujourd'hui.

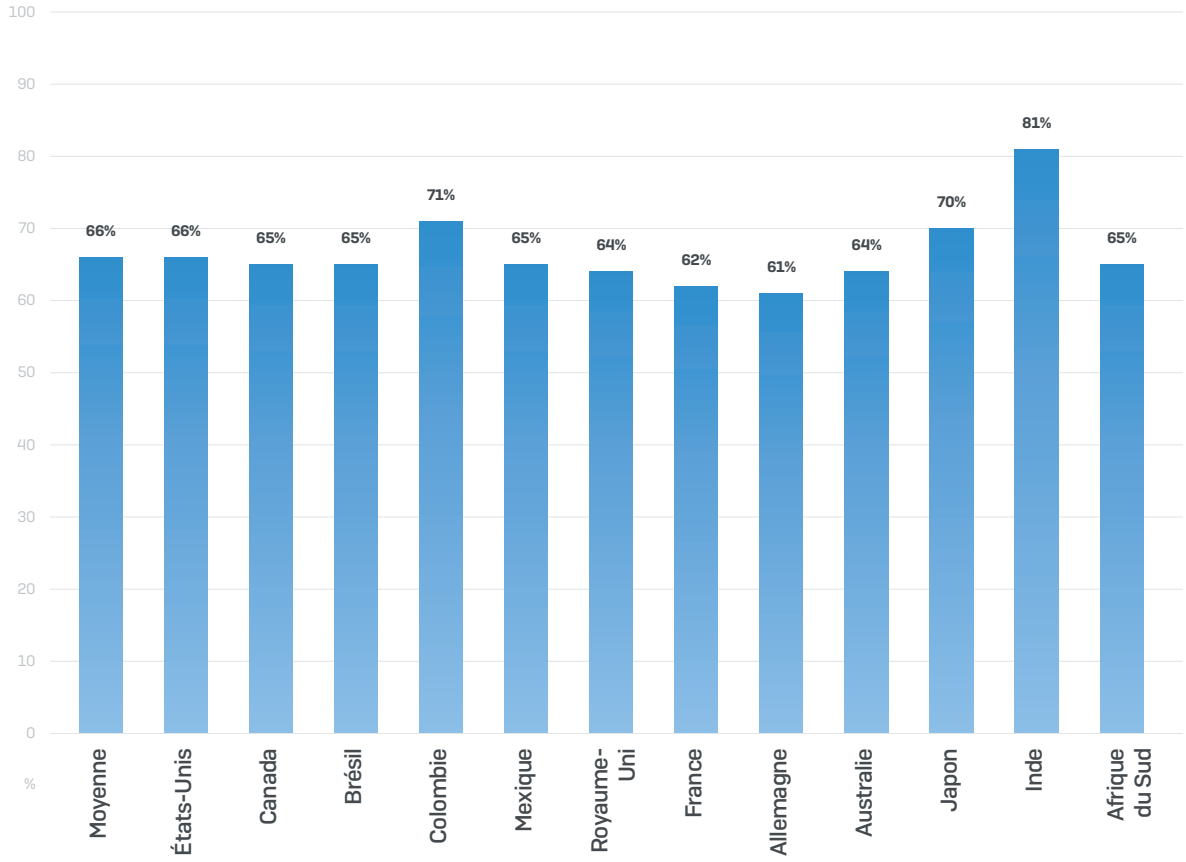
Toutefois, trouver les personnes dotées de l'expertise nécessaire est un défi majeur. 8 entreprises sur 10 déclarent avoir des difficultés à recruter les bonnes personnes. En matière de recrutement, l'Inde est le pays qui rencontre le plus de difficultés (89 %) et l'Allemagne celui qui en rencontre le moins. Et pourtant, 2 responsables informatiques allemands sur 3 disent avoir du mal à recruter des personnes qualifiées.

26 % du temps de travail des équipes informatiques est consacré à la cybersécurité



Pourcentage des répondants en accord avec l'énoncé : Recruter des personnes avec les compétences en cybersécurité dont nous avons besoin est un réel défi. ***Base :*** *tous les répondants (3 100)*

En même temps, les budgets consacrés à la cybersécurité ne sont pas suffisants pour 2/3 des répondants (66 %), qui estiment le budget dédié aux ressources humaines et aux technologies trop bas. Ce chiffre monte à 77 % lorsque l'entreprise a préalablement été touchée par une cyberattaque en 2018.



Pourcentage des répondants qui estiment que leur budget consacré à la cybersécurité (y compris les ressources humaines et la technologie) est inférieur à ce qu'il devrait être. ***Base :*** *tous les répondants (3 100)*

Il existe un lien très fort entre insuffisance budgétaire et recrutement en cybersécurité. L'Allemagne, pays qui rencontre le moins de difficultés à recruter, est aussi celui qui connaît le moins de contraintes budgétaires. À l'inverse, l'Inde fait face au plus grand défi budgétaire et au plus grand défi de recrutement.

Cela reflète l'offre limitée et la forte demande de compétences en matière de cybersécurité. Seul point positif de cette situation, les professionnels de la cybersécurité sont en mesure d'obtenir des salaires et des avantages sociaux plus élevés.

Le défi impossible de la cybersécurité

Les éditeurs de technologie développent depuis des décennies des produits de cybersécurité, et dans le même temps les entreprises continuent de dépenser du temps, de l'énergie et de l'argent pour leur cybersécurité. Pourtant, malgré des années d'innovations et d'investissements, notre enquête a révélé que la cybersécurité reste un défi difficile à relever et que les entreprises ne sont toujours pas dotées des ressources dont elles ont besoin.

Peut-être est-il temps d'adopter une approche différente ?

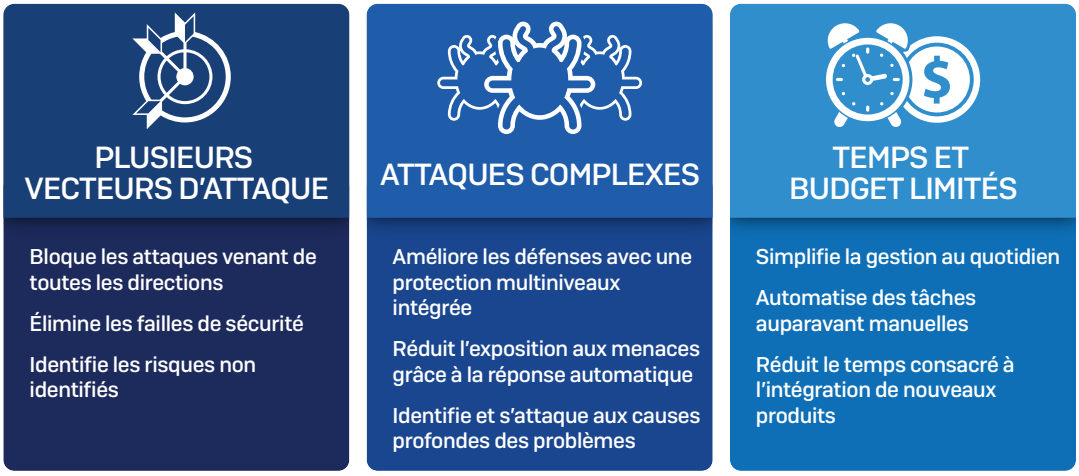
Une approche différente : la cybersécurité en tant que système

Comme nous l'avons vu, les cyber menaces fonctionnent comme un système, utilisant toute une gamme de techniques et de technologies interconnectées pour réaliser leurs attaques. Dans le même temps, toute infrastructure informatique est aussi un système, un réseau complexe et interconnecté composé de PC, Mac, serveurs, imprimantes, appareils mobiles, applications, ressources Cloud, commutateurs, pare-feu, réseaux sans fil, etc., et de tous les logiciels qui fonctionnent dessus. Avec une infrastructure informatique et des cyber menaces fonctionnant comme un système, il semble logique que la cybersécurité fonctionne elle aussi comme un système plutôt que comme l'addition de produits isolés.

La Sécurité synchronisée est le système de cybersécurité primé de Sophos. Les solutions de protection Endpoint, Réseaux, Mobile, Wi-Fi, Messagerie et Chiffrement se partagent en temps réel les informations sur les menaces et répondent automatiquement aux incidents. Et comme tout est contrôlé depuis une seule console Web, la gestion de la sécurité est un vrai jeu d'enfant.

Sécurité synchronisée : résoudre le puzzle impossible

La sécurité synchronisée permet aux entreprises de répondre aux défis complexes mis en lumière par notre enquête.



Plusieurs vecteurs d'attaque :

- Le portefeuille complet de solutions vous permet de bloquer les menaces venant de tout type de vecteur : email, Web, faille logicielle, clés USB.
- Les produits sont conçus pour fonctionner ensemble, éliminant les failles de sécurité tout en évitant les problèmes de compatibilité.
- Vous obtenez un aperçu sans précédent sur les risques précédemment non identifiés, tels que les applications malveillantes dans le trafic réseau.

Attaques complexes, coordonnées et multi-étapes :

- Une protection multiniveaux et intégrée maximise vos défenses contre les menaces avancées en les bloquant à différents stades et en utilisant de nombreuses technologies.
- La réponse automatisée aux incidents réduit considérablement votre exposition aux menaces en stoppant et en isolant les attaques en quelques secondes seulement.
- Une vue d'ensemble sur tout le parc informatique vous permet d'identifier et de traiter la cause profonde de tout incident.

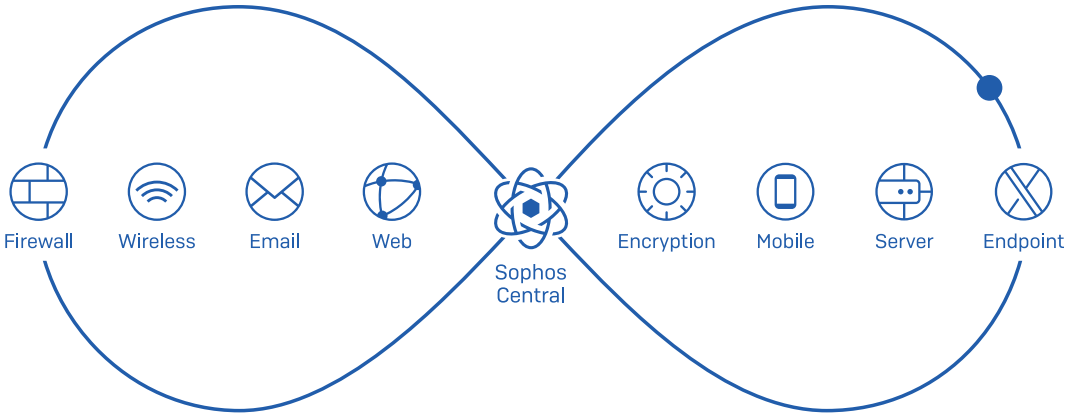
Pénurie de temps, de personnel qualifié et de technologie :

- Tout gérer depuis une seule console Web réduit de manière significative les frais généraux quotidiens tout en libérant le travail des membres de l'équipe.
- La réponse automatisée aux incidents allège également la charge administrative des équipes informatiques en supprimant le besoin d'identifier et de nettoyer manuellement les machines infectées.
- L'interface commune à tous les produits facilite et accélère l'intégration de nouveaux produits.

Conclusion

Malgré des investissements lourds et continus dans les technologies de cybersécurité, le travail des équipes informatiques dans le monde entier ne s'annonce pas plus simple qu'avant. Plutôt que de maintenir la même approche envers la cybersécurité, il est temps de passer à la cybersécurité en tant que système. En permettant aux produits de sécurité de partager en temps réel des informations et de travailler en synergie, vous gardez une longueur d'avance sur les menaces tout en libérant de précieuses ressources informatiques.

La Sécurité synchronisée de Sophos est le système de cybersécurité primé en qui des milliers d'entreprises dans le monde font confiance. Pour en savoir plus et pour la découvrir en action, RDV sur www.sophos.fr/synchronized.



Pour en savoir plus et commencer un essai:
www.sophos.fr/synchronized

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

19-06-21 WP-FR (RP)

SOPHOS