



Bitdefender 10 sur 10

2020

Les décideurs en matière de sécurité se doivent d'avoir toujours une longueur d'avance sur les acteurs malveillants. Cela a conduit à une culture d'aversion au risque, et à l'établissement compulsif de check-lists en matière de sécurité. Dans le même temps, les entreprises et les technologies qu'elles utilisent sont en constante évolution - en 2020 plus que jamais auparavant. C'est dans ce contexte de juxtaposition entre rapidité du changement et rigueur procédurale que réside le défi de la sécurité.

L'étude 10 sur 10 de Bitdefender met en lumière la dichotomie qui existe entre la façon dont les décideurs en matière de sécurité perçoivent le paysage actuel de la sécurité et les changements qu'ils savent qu'ils vont être amenés à mettre en œuvre.

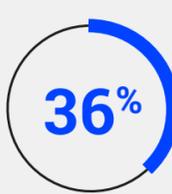
Il est reconnu nécessaire de changer le secteur de l'intérieur



71% estiment qu'une palette de compétences plus diversifiée est nécessaire chez les personnes en charge des tâches de cybersécurité



19% des professionnels français de la sécurité de l'information estiment qu'une neurodiversité accrue dans le secteur contribuera à la lutte contre la cyberguerre



36% estiment que la neurodiversité renforcera les défenses de cybersécurité



29% ont révélé qu'une force de travail davantage neurodiversifiée rétablirait l'équilibre avec les cybercriminels



24% des professionnels français de la sécurité de l'information estiment que si le déficit de compétences se poursuit encore pendant cinq années, celui-ci anéantira des entreprises

Enfin, l'étude révèle qu'il existe une forte conviction relative à la nécessité de diversifier le secteur.

La communication est essentielle

Concernant ce que les professionnels de la sécurité de l'information estiment devoir évoluer le plus en termes de communication opérée par le secteur de la sécurité à l'avenir, les réponses révèlent que :



55% des professionnels français de la sécurité de l'information reconnaissent qu'afin d'accroître les investissements dans le domaine de la cybersécurité, leur façon de communiquer autour de la sécurité doit radicalement changer



40% estiment que pour éliminer plus rapidement les risques, c'est le partage des connaissances qui doit faire l'objet d'un renforcement prioritaire, comment le secteur de la sécurité communique à l'avenir



40% estiment que le recours à un langage moins technique aiderait le secteur à communiquer plus efficacement, de sorte que tous les membres d'une organisation puissent comprendre les risques et comment se protéger.

Une évolution de la communication est indispensable si les professionnels de la sécurité de l'information veulent réagir au rythme nécessaire à la protection de leurs organisations et obtenir des investissements de la part de ces dernières.

La cyberguerre est une préoccupation majeure

Les risques de cyberguerre sont en hausse, et bien que préoccupés, certains professionnels de la sécurité de l'information sont encore mal préparés.

52% des professionnels français de la sécurité de l'information s'attendent à ce que l'intensification de la cyberguerre soit préjudiciable à l'économie dans les 12 prochains mois



59% des professionnels français de la sécurité de l'information estiment que le contexte de cyberguerre représente une menace pour leur organisation. Pourtant, seuls 63% des professionnels de la sécurité de l'information sont d'accord

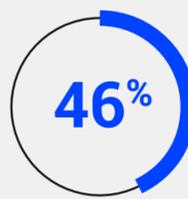
En dépit des inquiétudes, au moins 26% des professionnels français de la sécurité de l'information n'ont pas de stratégie en place pour se protéger de la cyberguerre



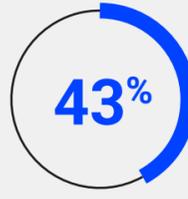
Une meilleure compréhension du paysage des menaces (33%) et davantage d'investissements dans des défenses de cybersécurité (34%) représentent les meilleurs moyens pour les entreprises d'affronter la cyberguerre.

Essor et déclin (et nouvel essor) des ransomwares

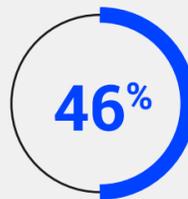
Les attaques de ransomwares sont de nouveau en hausse ; pourtant, les mesures de sécurité mises en place contre ces incidents ne se sont pas améliorées au même rythme.



46% des professionnels français de la sécurité de l'information reconnaissent qu'ils assistent à une résurgence des attaques de ransomwares, mais que les mesures de protection mises en œuvre contre ces attaques n'ont que peu progressé au cours des 5 dernières années.



43% sont préoccupés par le fait qu'une attaque de ransomware puisse anéantir l'entreprise dans les 12 à 18 prochains mois si les investissements en matière de sécurité ne sont pas renforcés



Presque la moitié estime que si leur entreprise subissait une attaque de ransomware, la rançon serait versée (46%)

La réalité, c'est que les ransomwares ne sont pas appelés à disparaître, et il convient de trouver, de concevoir et d'investir dans de meilleures défenses.

Tout le monde est connecté, mais tout le monde n'est pas protégé



42% des professionnels français de la sécurité de l'information estiment qu'il est aisé pour les cybercriminels de prendre le contrôle des appareils de l'IoT utilisés par les employés à leur domicile à des fins professionnelles



64% déclarent estimer qu'en raison de l'intensification de l'utilisation des appareils de l'IoT, les connaissances sécuritaires relatives à la façon de protéger ces appareils ont été renforcées au sein de leur entreprise



Pourtant, 18% des professionnels français de la sécurité de l'information affirment que les appareils de l'IoT continueront à se propager à un rythme plus rapide que celui de leur sécurisation au cours des 12 à 18 prochains mois

Le rythme auquel les appareils de l'IoT sont utilisés est plus soutenu que celui de la sécurité mise en place pour protéger les utilisateurs.

Méthodologie

6 724 professionnels de la sécurité de l'information ont été interrogés

Les personnes interrogées étaient originaires de France, des États-Unis, du Royaume-Uni, d'Australie, de Nouvelle-Zélande, d'Allemagne, d'Italie, d'Espagne, du Danemark et de Suède, personnes ayant un emploi ou une influence en termes de prise de décision dans le domaine de la cybersécurité dans des entreprises comptant 100 employés et plus dans différents secteurs d'activité, dont la Finance, le Gouvernement et l'Énergie.

Le paysage mondial des menaces est en constante évolution.

Découvrez comment garder une longueur d'avance