Rapport 2022

Economie de la sécurité informatique 2022

Executive summary

kaspersky BRING ON THE FUTURE

kaspersky.com

Economie de la sécurité informatique 2022

Après deux années marquées par des bouleversements et des dynamiques de dépassement des modèles économiques traditionnels, tendances au cœur du rapport sur l'Économie de la sécurité informatique 2021 de Kaspersky, les entreprises ont, en 2022, continué à faire face à des défis supplémentaires concernant les décisions à prendre au sein de leur organisation, dans un climat toujours plus marqué par l'incertitude.

Les grandes tendances en matière de cybersécurité poussent les organisations à adopter une attitude proactive, car elles doivent désormais être en mesure de se défendre malgré le contexte de numérisation galopante et de pénurie de main-d'œuvre compétente dans le domaine, le tout dans un environnement toujours marqué par l'incertitude géopolitique et économique.

Pour les responsables informatiques, parvenir à trouver un moyen pour protéger leur organisation en 2023 (et après) est un véritable casse-tête: la sécurisation des processus métier contre les intrusions qu'ils tentent de mettre en place nécessite une nette augmentation des budgets de sécurité au cours des trois prochaines années, estimée à 10 % en Europe (14 % au global et jusqu'à 17 % dans certaines régions).

Nos recherches révèlent également que les équipes de sécurité informatique luttent désormais contre les fuites de données causées par des employés en interne, presque aussi fréquemment que les failles causées par des cyberattaques, suite à l'introduction de nouveaux postes de travail portables ou de tablettes pour le personnel, et à l'utilisation massive de réseaux privés virtuels (VPN) pour permettre le travail à distance constatée l'année dernière.

Cette année, nous avons observé que de nombreuses entreprises ont changé leur fusil d'épaule et confié certaines fonctions à des services externalisés tels que les fournisseurs de services managés (MSP) et les fournisseurs de services de sécurité managés (MSSP) afin de trouver des moyens plus efficaces de mettre en œuvre des solutions de cybersécurité. A titre comparatif, l'année dernière, les responsables informatiques envisageaient plutôt une transition potentielle vers des serveurs cloud et des logiciels collaboratifs.

Méthodologie

L'enquête globale sur les risques de cybersécurité pour les entreprises de Kaspersky est une étude annuelle sur l'état de la sécurité informatique dans les entreprises conduite à l'internationale.

Cette étude repose sur des entretiens conduits auprès d'un total de 3230 répondants travaillant dans des entreprises de tailles diverses, allant des petites et moyennes entreprises de plus de 50 employés aux grandes sociétés. Elle a été menée dans 26 pays sur les principaux marchés B2B Kaspersky Lab est présent. Tout au long du rapport, les entreprises interrogées sont désignées par le terme PME pour les petites et moyennes entreprises de 50 to 999 employés, soit par le terme "grande entreprises" pour les entreprises de plus de 1000 employés.

Principales conclusions

Les incidents cyber ayant eu le plus d'impact en termes de coûts et d'efforts pour **les PME ont été les attaques sur l'infrastructure informatique hébergée par un tiers, tandis que les grandes entreprises ont surtout souffert des attaques ciblées.**

En Europe, les budgets de cybersécurité en 2022 s'élèvent en moyenne à **2 millions de dollars US pour les grandes entreprises**, et à **150 000 dollars US pour les PME**. Les deux segments prévoient d'augmenter les budgets de manière égale jusqu'à **10 %** l'année prochaine.

Les communications, le développement de produits et le service client sont les trois processus les plus touchés lors d'intrusions cyber.

Les fuites de données ont été le problème de sécurité le plus rencontré cette année. Ce type d'incidents a été le plus souvent **causé par des employés (22 %) et des attaquants externes (23 %).**

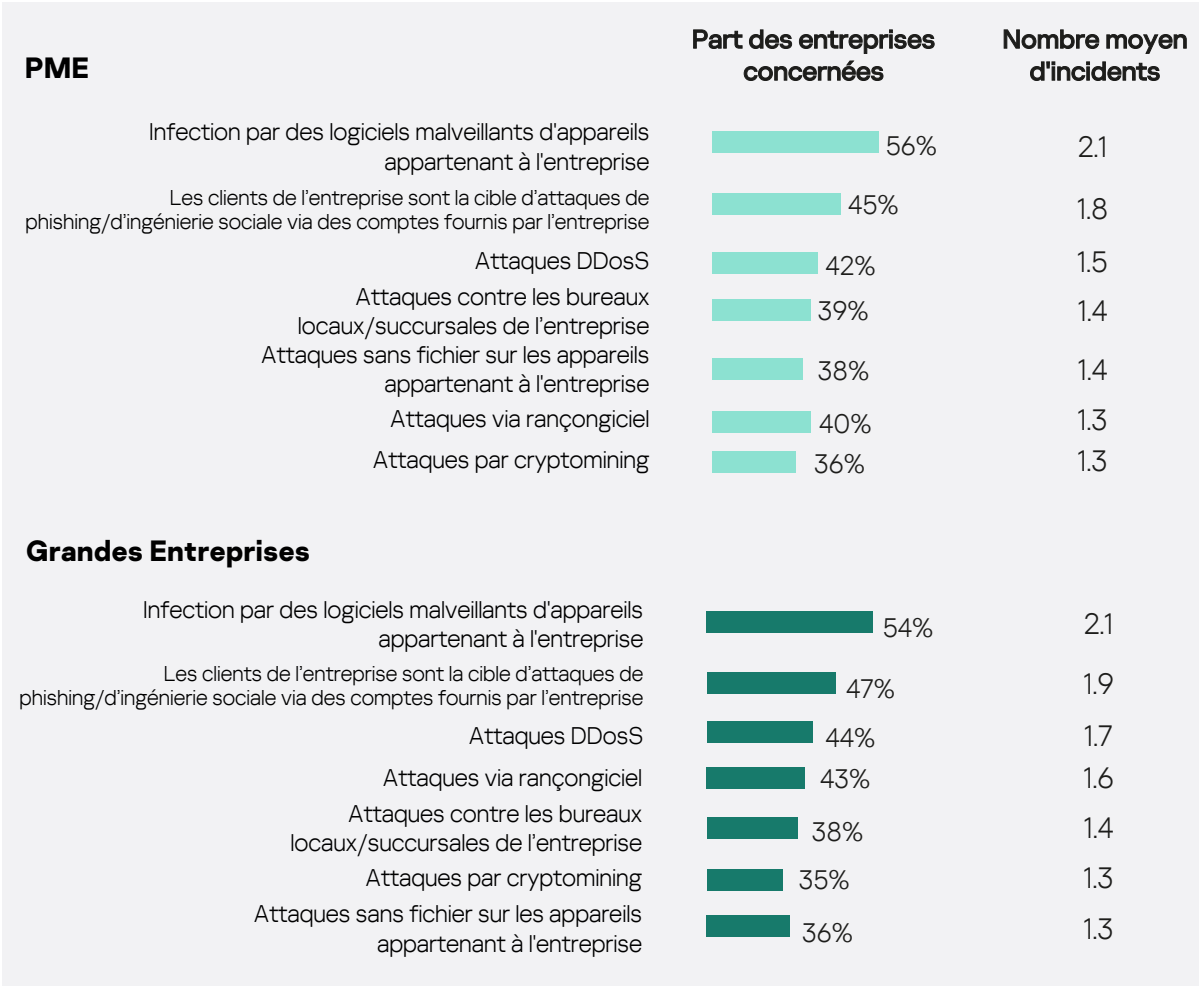
La mise en œuvre de solutions de cybersécurité efficaces et les gains d'efficacité obtenus en faisant appel à des spécialistes extérieurs en raison d'un manque de personnel spécialisé en sécurité informatique sont les deux **principaux facteurs** qui incitent les entreprises à externaliser leur sécurité informatique.

Mêmes défis, nouveaux obstacles

Les entreprises sont confrontées à de nouveaux obstacles qui les poussent à plus de résilience. Cette année, les risques cyber sont restés une préoccupation majeure pour les PME comme pour les grandes entreprises.

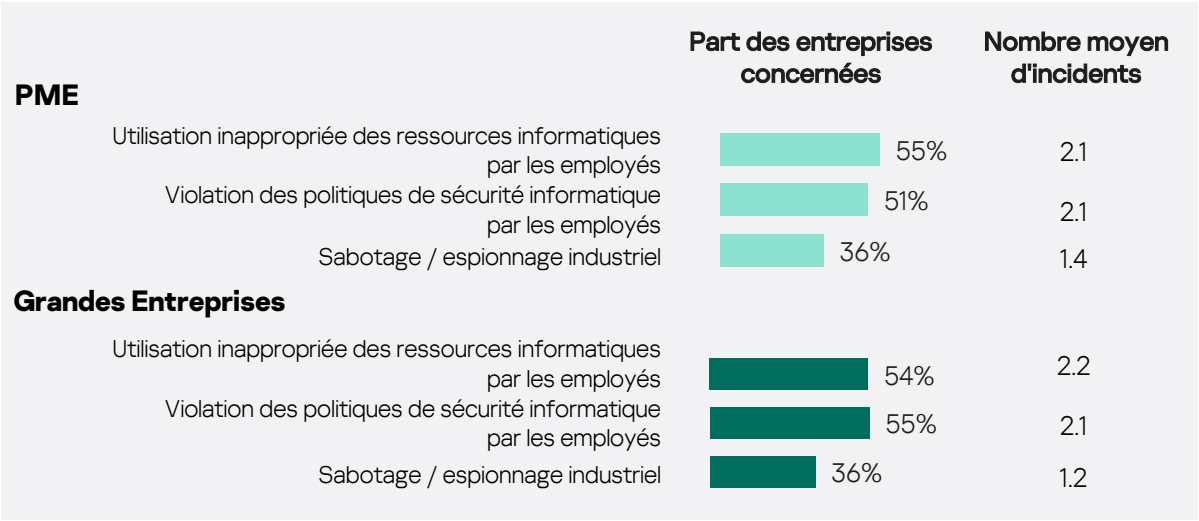
L'infection par logiciels malveillants et les attaques de phishing sur les comptes des clients apparaissent comme étant les principales menaces auxquelles les entreprises ont été confrontées en 2022. En moyenne, les PME comme les grandes entreprises doivent faire face à deux attaques par an.

Menaces et préoccupations : Continuité opérationnelle



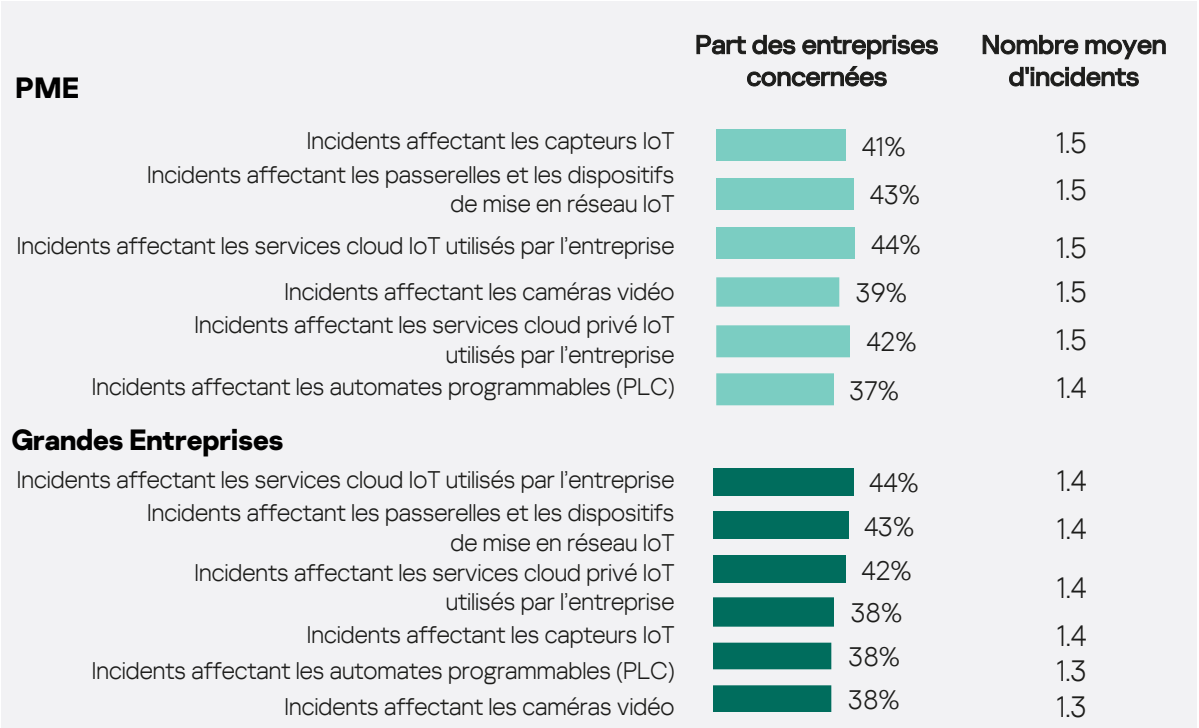
En 2022, les responsables de la sécurité informatique ont été confrontés à des cybermenaces causées non seulement par des cybercriminels étrangers à leur entreprise tentant de pénétrer dans les systèmes informatiques, mais aussi par des employés en interne, qui violent les politiques de sécurité informatique. 55 % des entreprises ont dû faire face à des violations des politiques de sécurité informatique de la part de leurs propres employés.

Menaces et préoccupations : S'assurer du respect des règles IT en interne



Les appareils intelligents utilisés à la maison et sur le lieu de travail, tels que les assistants virtuels et les ampoules connectées, sont devenus monnaie courante, mais ils peuvent aussi servir de porte d'entrée pour les cyberattaquants, tant pour les entreprises que pour leurs clients. Les entreprises ont été confrontées à deux incidents en moyenne en 2022, affectant les capteurs IoT, les services cloud IoT et les réseaux IoT.

Menaces et préoccupations : Problèmes de sécurité des infrastructures IoT



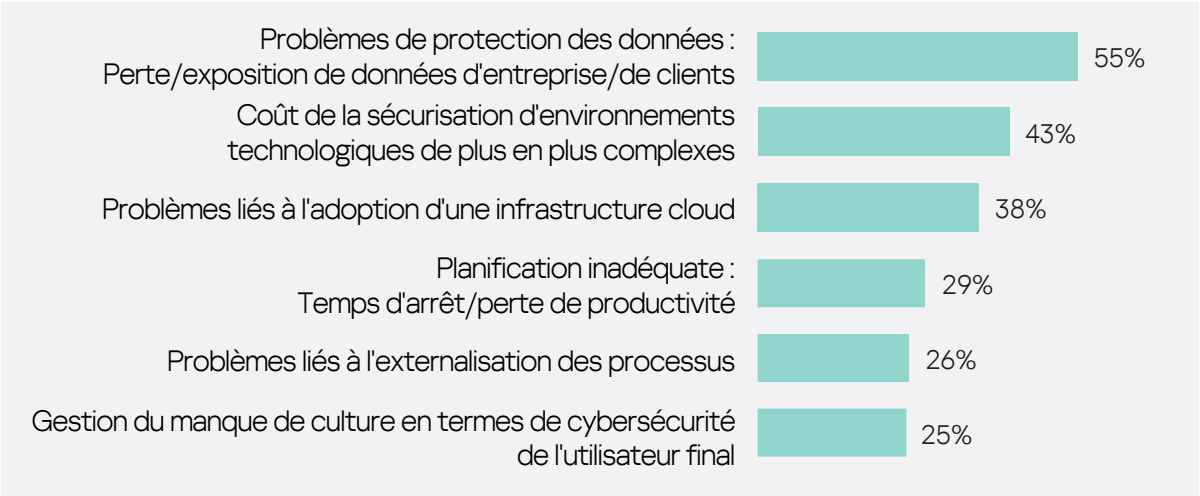
Protection des données et failles de cybersécurité

« La protection des données reste la principale préoccupation des entreprises en matière de sécurité, autant pour les petites enseignes familiales que pour les grands groupes. Les personnes interrogées ont fait état de fuites de données via les systèmes informatiques internes, causées par des cyberattaques mais aussi directement par des employés. » Yuliya Novikova, responsable de l'analyse des services de sécurité chez Kaspersky, explique en quoi les fuites de données représentent un risque croissant pour les entreprises :

1. Lorsque des données compromises d'une entreprise deviennent publiquement disponibles et consultables, elles peuvent intéresser les cybercriminels, qui peuvent alors les utiliser pour perfectionner leurs attaques de phishing et leurs techniques d'ingénierie sociale.
2. Les cybercriminels ont désormais une véritable présence en ligne et sur les réseaux sociaux, ce qui leur permet de communiquer sur les attaques réussies via leurs comptes Twitter, des sites Web personnels et des services de messageries publics. Cela constitue un risque sérieux pour la réputation des entreprises et des individus cités, car même une fausse déclaration peut avoir un échos plus large sur les réseaux sociaux et manipuler l'opinion publique.
3. Les risques de fuite des données augmentent s'ils impliquent une fuite de IPI (informations personnelles identifiables), car cela pourrait entraîner de graves conséquences pour la réputation de l'entreprise, mais aussi entraîner de lourdes pertes financières, associées à d'éventuelles amendes RGPD pour avoir enfreint les règles de protection des données. Les entreprises peuvent également être amenées à régler des frais juridiques si elles font face à un litige.

Cette année, un peu plus de la moitié (55 %) des entreprises considèrent que les problèmes de protection des données sont les plus épineux à résoudre.

La seconde source de préoccupation ayant le plus été relevée dans l'étude, par 43 % des répondants, est la question du coût de la sécurisation des environnements technologiques, dont la complexité est de plus en plus marquée. A la troisième place du podium, on retrouve les problèmes liés à l'adoption d'une infrastructure cloud, cités par 38% des personnes interrogées.



La transparence devient incontournable

L'attention accrue portée aux politiques de transparence est directement liée aux préoccupations concernant la protection des données devenue un enjeu majeur de sécurité pour les entreprises : les fournisseurs et les sous-traitants accordent une plus grande importance à la gestion des données et aux politiques de transparence.

Au total, 91 % des personnes interrogées considèrent que la présence (ou l'absence) de politiques de transparence est une donnée essentielle à prendre en compte lorsqu'elles envisagent de travailler avec un fournisseur ou un sous-traitant, les PME et les grandes entreprises y accordant une importance égale.

La région APAC est celle qui porte la plus grande attention à cette question, 98% des entreprises de la région déclarant que la transparence est un élément qu'il est important de prendre en considération lorsqu'elles envisagent une collaboration avec un fournisseur ou un entrepreneur.

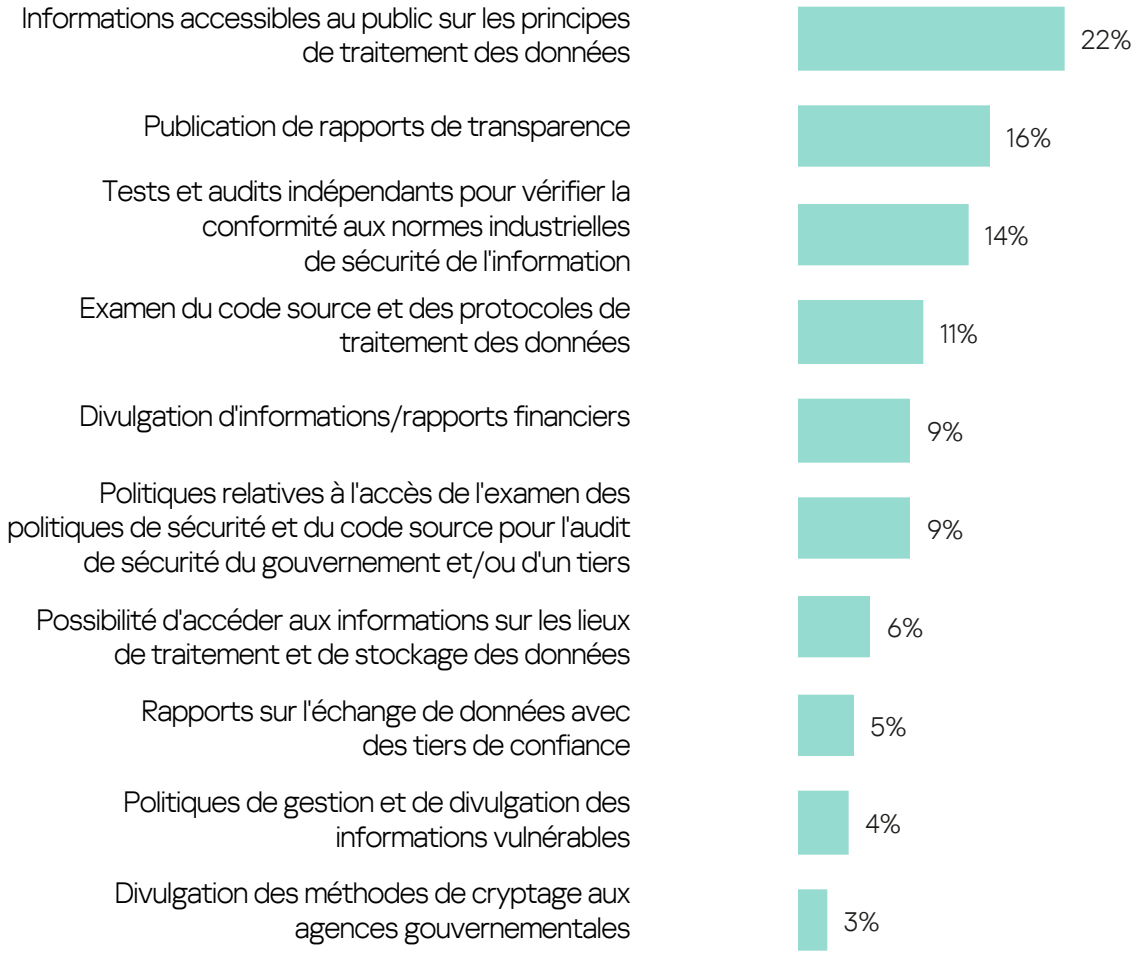
Kaspersky a été l'un des premiers à instaurer la confiance numérique dans le secteur de la cybersécurité, en lançant la Global Transparency Initiative (GTI) pour offrir à ses parties prenantes une plus grande visibilité sur le fonctionnement de l'entreprise et de ses solutions. La GTI permet la vérification et la validation de la fiabilité des produits, des processus internes et des opérations commerciales de l'entreprise. Depuis son lancement en 2017, l'initiative intègre de nouveaux paramètres, à l'image des révisions du code source, devenant ainsi une référence du secteur en matière de transparence.

Pour en savoir plus, rendez-vous ici.

L'étude révèle que près de 80 % (78 %) des personnes interrogées dans le monde ont déjà mis en place des politiques de transparence au sein de leur organisation. Les entreprises de la région APAC affichent le taux d'adoption le plus élevé (88 %), suivies par l'Amérique du Nord (84 %) et l'Amérique latine (82 %). En Europe, ce sont déjà 73% des entreprises qui sont concernées. Globalement, les politiques de transparence sont plus répandues dans les grandes entreprises (82 %), tandis que 76 % des PME commencent à s'y intéresser.

A noter que 81 % des organisations interrogées se déclarent prêtes à allouer des ressources supplémentaires pour le déploiement de politiques de transparence. Les entreprises les plus intéressées par ces investissements sont celles du secteur de l'informatique et des télécommunications (85 %) et celles des services financiers (82 %)

À la question de savoir ce que les politiques de transparence devraient inclure, aucune réponse claire n'a pu être obtenue auprès des organisations. Les trois premiers points énumérés par la majorité des répondants comprennent des informations sur les principes de traitement des données (mentionnées par 22%), la publication de rapports de transparence (16%) et des tests et audits indépendants de conformité aux normes industrielles de sécurité de l'information (14%).



Approches et pratiques couvertes par les politiques de transparence

Proven. Transparent. Independent.

Preuve de son engagement auprès de toute la communauté de la cybersécurité et des parties prenantes, Kaspersky a lancé en 2017 la "Global Transparency Initiative" (GTI), qui propose des mesures concrètes de validation et de vérification de la fiabilité des produits, des processus internes et des opérations commerciales de l'entreprise. Pour en savoir plus, rendez-vous ici.

Les fuites de données affectent les entreprises

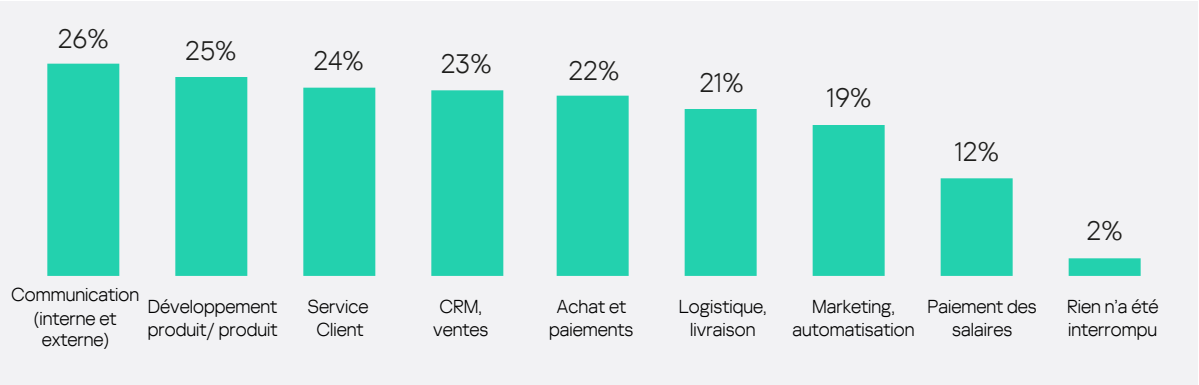
Qu'elles soient le résultat d'une cyberattaque (23%), ou imputables à des employés (22%), les fuites de données sont le problème de sécurité auquel les entreprises sont le plus fréquemment confrontées. Arrive ensuite la capacité d'identification et de correction des vulnérabilités des systèmes informatiques, qui est un problème pour 20% des personnes interrogées.

« Un répondant sur cinq a signalé des problèmes de gestion des vulnérabilités et nous constatons que nos clients sont confrontés aux mêmes problèmes. La difficulté commence dès l'inventaire réseau relatif aux ressources externes, dès qu'une entreprise commence à se constituer une identité numérique.

Les ressources réseaux des grandes entreprises et des PME sont éparpillées géographiquement, avec des dizaines de systèmes et d'applications web hébergés par différents fournisseurs et sur des services dans le cloud, ce qui nécessite une gestion minutieuse des vulnérabilités.

Le problème est aggravé par toute nouvelle vulnérabilité ou code d'exploitation, car les entreprises n'ont pas plus de quelques heures pour appliquer des mesures correctives avant d'être confrontées à de multiples tentatives d'exploitation de ces vulnérabilités de la part des cybercriminels », explique Yulia Novikova.

Les failles de cybersécurité et intrusions ont principalement affecté les communications (26 %), le développement et la production de produits (25 %), suivis par le service client (24 %).

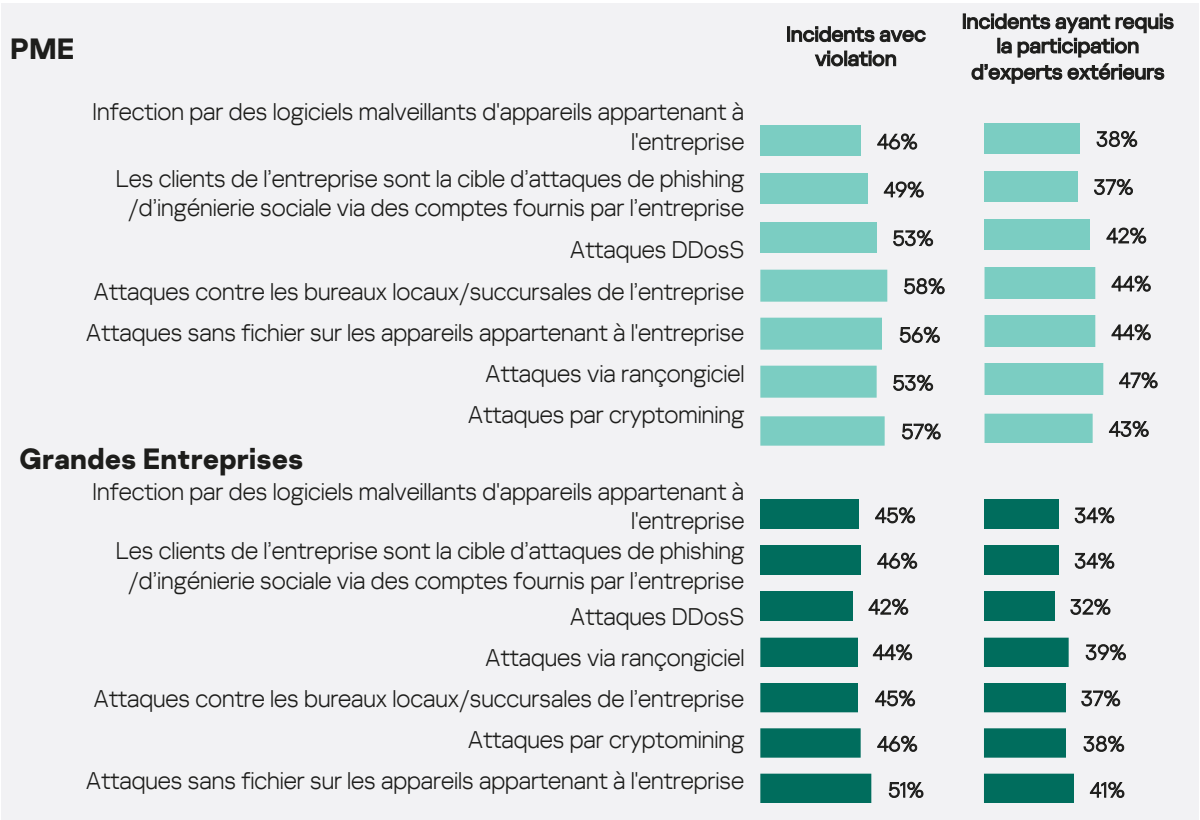


En 2022, des entreprises de toutes tailles ont eu recours à des spécialistes externes à leur organisation, un investissement supplémentaire pour pouvoir faire face aux fuites de données les plus critiques.

Les attaques sans fichier sur des appareils appartenant à l'entreprise constituent l'un des plus grands défis pour les équipes de sécurité informatique: cette année, plus de la moitié des PME (56 %) et des entreprises clientes (51 %) ayant signalé des intrusions de ce type.

Les répondants des petites et moyennes entreprises ont également mentionné des attaques contre leurs filiales (58 %) et du cryptominage malveillant (57 %), tandis que 46 % des grandes entreprises ont signalé des cas de phishing et d'ingénierie sociale.

Incidents avec violations & Participation d'experts externes : Continuité des activités



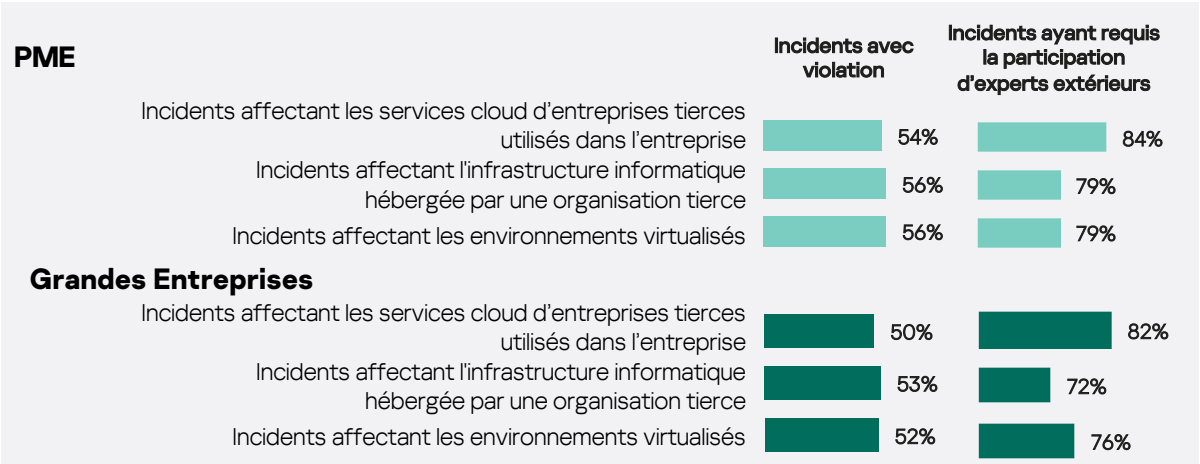
Les trois principaux incidents jugés suffisamment complexes pour nécessiter l'intervention d'experts externes en sécurité informatique ont touché les environnements virtualisés des entreprises (76 % pour les grandes entreprises, 79 % pour les PME), les services cloud IoT (72 % des ENT et 84 % des PME) et l'infrastructure informatique (82 % des grandes entreprises et 79 % des PME).

Les incidents liés à la violation des politiques de sécurité informatique (30 % des grandes entreprises et 37 % des PME) et à l'utilisation inappropriée des ressources informatiques par les employés (31% des grandes entreprises et 36% des PME) ont nécessité moins d'assistance externe.

En ce qui concerne les problèmes de sécurité affectant l'infrastructure cloud, en 2022, plus de la moitié des répondants ont déclaré des incidents affectant les environnements virtualisés qui impliquaient une intrusion.

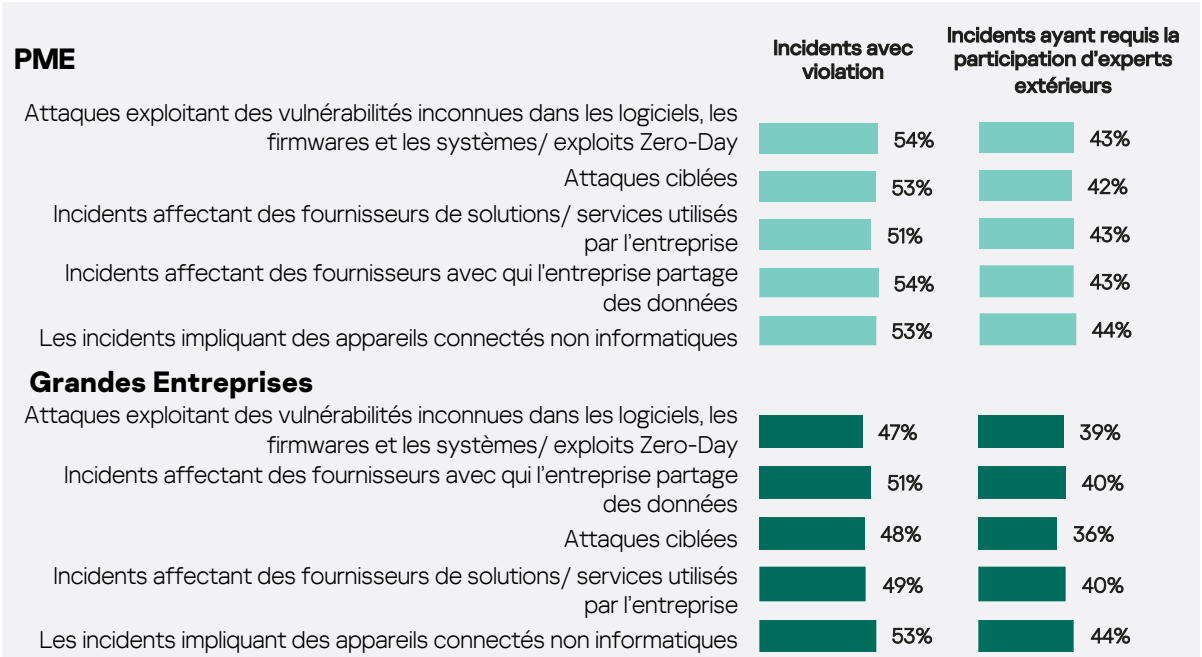
Les PME ont fait appel à des spécialistes externes pour traiter les incidents liés à des services cloud tiers (84 %), tandis que 82 % des entreprises ont signalé des incidents avec des infrastructures informatiques tierces.

Incidents avec violations & Participation d'experts externes : Problèmes de sécurité des infrastructures Cloud



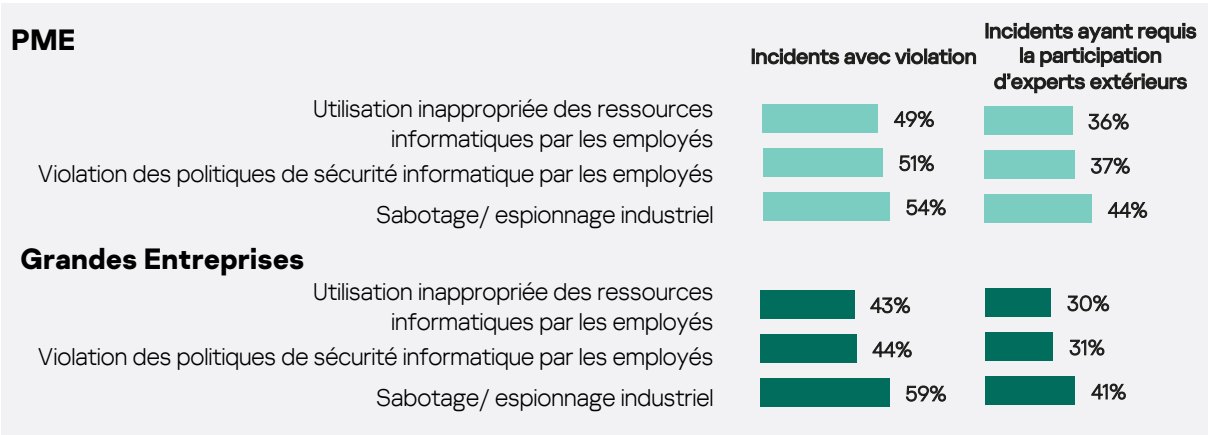
La gestion des incidents relatifs aux appareils non informatiques connectés tels que des systèmes de contrôle industriels est de plus en plus externalisée. Le rapport révèle également que de tels incidents sont devenus un événement régulier pour 44 % des entreprises interrogées.

Incidents avec violations & Participation d'experts externes : Sécurisation des environnements complexes



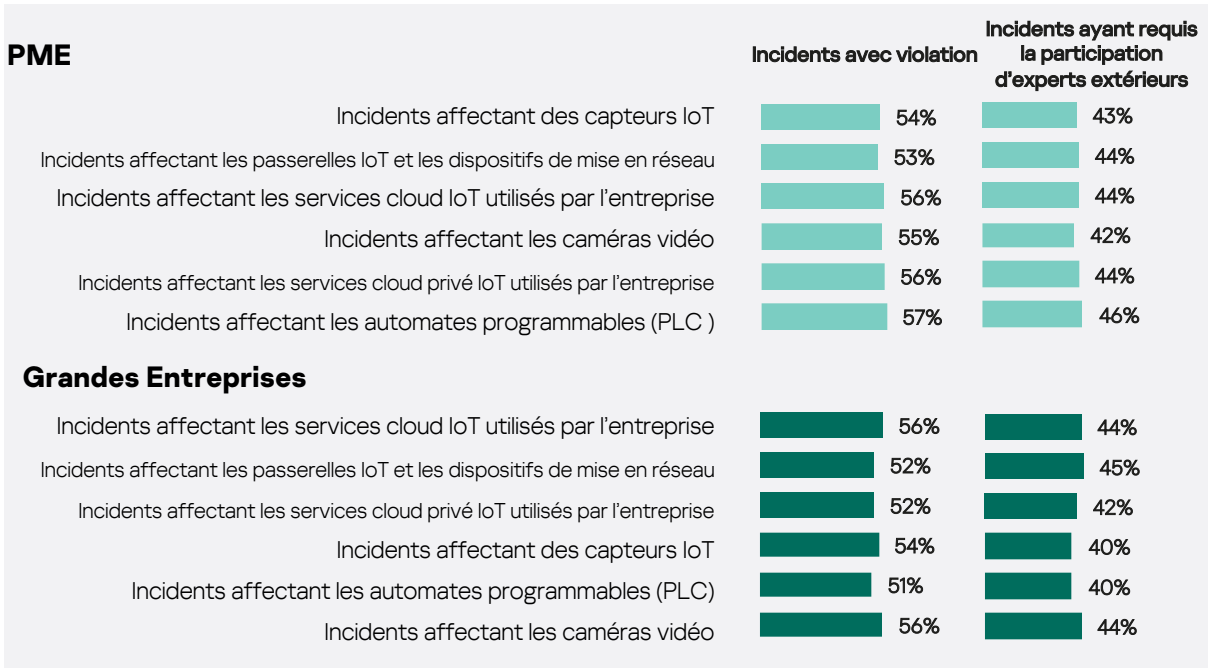
Sans surprise, les grandes organisations ont été confrontées à une forme de sabotage ou d'espionnage industriel (59 % pour les entreprises, 54 % pour les PME), nécessitant l'aide d'experts externes.

Incidents avec violations & Participation d'experts externes : S'assurer du respect des règles IT en interne



Les chaînes de montage équipées de robots et les ordinateurs industriels dotés d'automates programmables IoT connectés à Internet pour gérer les processus de fabrication sont courants mais les problèmes de sécurité les plus épineux pour les PME concernent désormais les automates programmables (PLC) (57 %) et les services cloud IoT (56 %). De leur côté, les répondants travaillant pour les grandes entreprises soulignent que la plupart des incidents touchent également les caméras, les capteurs IoT et les services cloud IoT (54-56 %).

Incidents avec violations & Participation d'experts externes : Problèmes de sécurité de l'infrastructure IoT



Le coût réel des cyberattaques pour les entreprises

Pour se remettre d'une cyberattaque, le coût moyen engagé par les entreprises est extrêmement élevé, mais il doit être mis en perspective avec les autres besoins financiers d'une organisation.

Les entreprises doivent donner la priorité aux investissements portant sur les besoins essentiels, tels que le recrutement ou les ventes, alors que le coût élevé d'une cyberattaque va encore alourdir les charges budgétaires.

Grandes Entreprises

$109K
Le plus coûteux

$53K
Le moins coûteux

- Les attaques ciblées et les incidents affectant les services de cloud privé IoT ont été les plus coûteuses pour les grandes entreprises en 2022, avec des montants respectifs de **104 488 $ et 109 405 $.**
- Les incidents les moins coûteux ont été ceux causés par une utilisation inappropriée des ressources informatiques par les employés (**52 887 $**).

PME

$7.7K
Le plus coûteux

$5K
Le moins coûteux

- Pour les PME, les attaques ciblant des bureaux locaux ou des succursales se sont avérées les plus onéreuses, coûtant **7 694 $** en moyenne, tandis que les récupérations après des attaques DDoS ont engendré des factures de **7 298 $**.
- Les incidents les moins coûteux, ceux qui touchent les fournisseurs, ont entraîné des factures de **4 956 $**, tandis que les incidents causés par des violations des politiques de sécurité informatique par les employés ont nécessité des réparations de système de **4 951 $.**

Les cyber-héros en renfort

Le recrutement est une autre priorité sur la liste des responsables de la sécurité informatique en 2023, qui cherchent à mieux protéger leurs organisations contre les cybermenaces tout en réduisant les temps de réponse aux incidents. Il faut ajouter qu'après avoir été exposées à un risque cyber, les équipes se perfectionnent en se dotant de personnel spécialisé dédié, disposant d'une réelle expertise sur le sujet.

Globalement, près de la moitié des répondants (48 %) ont investi dans du personnel additionnel en 2022, afin de mieux répondre aux incidents survenus. Le recrutement d'analystes ou de spécialistes de la sécurité informatique complémentaires en réponse aux incidents de cybersécurité est apparu comme la meilleure solution pour 52 % des PME et 56 % des entreprises.

La moitié des PME et 46 % des entreprises ont créé de nouvelles équipes/employés dédiés à la sécurité informatique des suites d'une cyberattaque. En outre, 86 % des entreprises ont engagé ou employé des professionnels de l'informatique pour résoudre les problèmes causés par les incidents qu'elles ont connus au cours des 12 derniers mois.

Pour faire face à ces situations, 57 % des PME et 62 % des grandes entreprises ont fait appel à différents consultants en sécurité informatique, notamment pour l'évaluation des risques de cybersécurité (32 % pour les PME et 38 % pour les grandes entreprises), et pour des services de cybersécurité en réponse à des incidents (28 % pour les PME et 33 % pour les grandes entreprises).

« D'après notre expérience, les entreprises ne commencent généralement à penser à engager des professionnels de la sécurité de l'information qu'après un incident, car la sécurité de l'information est assurée par un administrateur réseau, un programmeur ou un informaticien. Il est également important de comprendre qu'un spécialiste de la réponse aux incidents travaillant sans les bonnes politiques de sécurité de l'information, les logiciels et le matériel appropriés n'a pas vraiment la capacité de traiter ou d'être au courant de tous les problèmes.

La meilleure façon, et la plus rentable, de réduire le coût des incidents est d'être proactif et bien préparé à à faire face à toute cyberattaque éventuelle.

Pour protéger une entreprise de façon pérenne contre une infection par un logiciel malveillant ou une fuite de données, seule l'application d'un ensemble de mesures proactives, incluant la création d'un plan de réponse aux incidents, des tests de pénétration réguliers et des audits de sécurité de l'information, peut justifier le coût d'un personnel spécialisé.

Dans de nombreux cas, le moyen le plus économique de protéger efficacement votre entreprise, particulièrement pour les petites entreprises, est de faire appel à des professionnels externes », commente Konstantin Sapronov, Head of Global Emergency Response Team chez Kaspersky.

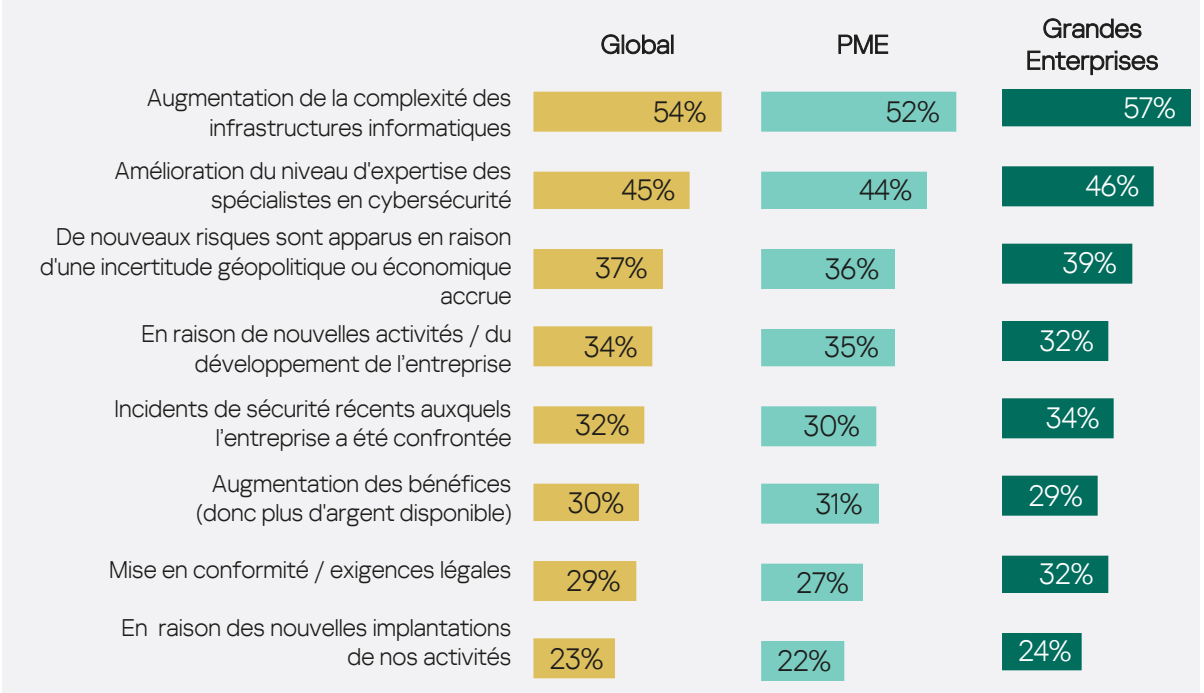
Les budgets dans la cybersécurité vont encore augmenter en 2023

Les budgets dans la cybersécurité devraient à nouveau augmenter au cours des trois prochaines années, tant pour les PME que pour les grandes entreprises, afin de couvrir une série de différents domaines. En Europe, en 2022, les budgets médians consacrés à la cybersécurité dans les grandes entreprises se sont élevé à 2 millions de dollars, contre 150 000 dollars pour les PME. Les entreprises, toute taille confondue, prévoient une augmentation de leur budget de sécurité informatique de 10 % au cours des trois prochaines année.

Europe	PME Moyenne	Grandes Enterprises Moyenne
Budget IT	$375,000	6,77M$
Budget Sécurité Informatique	150K$	2M$
Evolution du budget moyen prévu pour la sécurité informatique sur 3 ans	+10%	+10%

Les risques liés à l'incertitude géopolitique ou économique constituent le principal facteur d'augmentation des budgets de sécurité informatique pour 36 % des PME et 39 % des entreprises.

Budgets des services de sécurité informatique : Principaux facteurs influençant les dépenses



« La continuité des activités dépend plus que jamais de la sécurité de l'information. Pourtant, nous voyons encore de grandes entreprises opérer soit avec des systèmes non protégés, soit avec des équipements anciens car elles considèrent que les cyberattaques ne constituent pas une menace pour leur activité.

Cependant, l'infrastructure informatique étant de plus en plus complexe et les cyberattaques de plus en plus sophistiquées, ces entreprises sont de plus en plus conscientes de la nécessité de protéger tous leurs actifs, y compris les ordinateurs, les données et les utilisateurs, et d'étendre la cybervigilance à tous les vecteurs d'attaque possibles.

Certains États exigent désormais que les organisations soient plus sûres sur le plan de la cyber-sécurité et des données, et qu'il s'agisse d'un régulateur exigeant une personne désignée pour ce rôle, ou de nouvelles règles pour l'ensemble d'un secteur vertical ou industriel, ce sont des facteurs qui influencent les budgets croissants » commente Bertrand Trastour, DG France de Kaspersky.

Les solutions MSP permettent de répondre aux besoins en constante évolution des entreprises

Face à l'évolution rapide des besoins et des priorités des entreprises en 2022, de nombreuses sociétés ont externalisé certaines fonctions informatiques auprès de fournisseurs de services gérés (MSP) et de fournisseurs de services de sécurité gérés (MSSP) lorsqu'elles cherchaient à réaliser des économies budgétaires ou à renforcer les compétences de leurs équipes.

La principale raison d'externaliser certaines responsabilités en matière de sécurité informatique à des MSP/MSSP en 2022 était de réaliser des économies dans la fourniture de solutions de cybersécurité, tant pour les PME (62 %) que pour les grandes entreprises (69 %). Parmi les autres raisons les plus fréquemment citées pour l'externalisation figurent la pénurie de personnel informatique ou le manque d'effectifs dans les services informatiques (53 % pour les PME) et le besoin d'une expertise particulière (50 % pour les PME et 52 % pour les grandes entreprises). En outre, 47 % des entreprises ont fait appel à des experts externes pour gérer des processus commerciaux complexes pour leur organisation.

Conclusion

Encore une année éprouvante pour les équipes informatiques devant travailler avec moins de personnel, qui confirme que le paysage des cybermenaces demeure complexe, avec des attaques persistantes contre les entreprises. Mais avec l'augmentation des dépenses informatiques à l'horizon, la gestion future des incidents et des violations de sécurité semble présager du positif, car les entreprises adoptent une position plus proactive et informée en matière de cybersécurité.

Si les infections par des logiciels malveillants et les attaques par hameçonnage restent les principales menaces, les nouvelles fuites de données provenant de l'intérieur de l'entreprise, et notamment causées par des employés, sont un casse-tête supplémentaire pour les équipes de sécurité informatique, qui de ce fait, font le choix de transférer certaines fonctions vers des services externalisés.

Après deux années de mesures d'économie, les entreprises, grandes et petites, entrent maintenant dans un monde post-pandémie et s'adaptent à la vie avec le cloud computing en raison de la complexité accrue de l'infrastructure informatique.

La protection des organisations à travers l'infrastructure informatique distante et avec le cloud pendant la pandémie n'est peut-être pas la panacée, mais dans l'environnement économique et géopolitique actuel, elle offre une certaine tranquillité d'esprit lorsqu'il s'agit de répondre aux exigences de sécurité des entreprises en constante évolution.

Pour faire face aux menaces permanentes que représentent les logiciels malveillants et le phishing, et pour protéger vos entreprises contre les fuites de données et d'informations indésirables, Kaspersky propose quelques recommandations simples :

Anticipez et budgétez les risques cyber et les risques liés aux données propres à votre pays et à votre secteur d'activité en utilisant des ressources spécialisées telles que le calculateur de sécurité informatique. Cet outil vous aidera à optimiser l'efficacité de vos mesures de protection.

Utilisez une solution de sécurité adaptative multiplateforme comme Kaspersky Endpoint Detection and Response (EDR) pour bénéficier d'une visibilité complète sur tous les terminaux d'un réseau d'entreprise, ce qui permet d'automatiser les tâches EDR de routine et de permettre aux équipes informatiques de chasser, de hiérarchiser, d'enquêter et de neutraliser rapidement les menaces complexes.

Une expertise supplémentaire sans recrutement complémentaire peut être obtenue en adoptant un service de sécurité géré tel que notre service MDR (Managed Detection and Response. Il permet de bénéficier des meilleurs services de sécurité automatisés avancés possibles et d'analyser les données de l'entreprise recueillies chaque jour, en temps réel, 24 heures sur 24 et 7 jours sur 7, afin de se protéger contre les cyberattaques sophistiquées, même si l'entreprise ne dispose pas de personnel spécialisé en sécurité informatique.

Investissez dans la formation afin que vos spécialistes de la sécurité informatique maintiennent leurs compétences à jour et soient les mieux préparés au paysage des cybermenaces. Grâce à la formation Kaspersky Expert, les professionnels de l'InfoSec peuvent améliorer leurs compétences ou aider les responsables d'équipe à aider les équipes de réponse aux incidents à lutter contre la cyber-réalité en constante évolution.

Réfléchissez à l'avance aux structures auxquelles vous pouvez demander de l'aide en cas d'incident de cybersécurité. S'il n'est pas toujours possible de stopper une attaque avant qu'elle ne pénètre votre périmètre de sécurité, une aide professionnelle de la part d'experts en sécurité peut contribuer à limiter les dommages qui en résultent et à empêcher l'attaque de se propager.