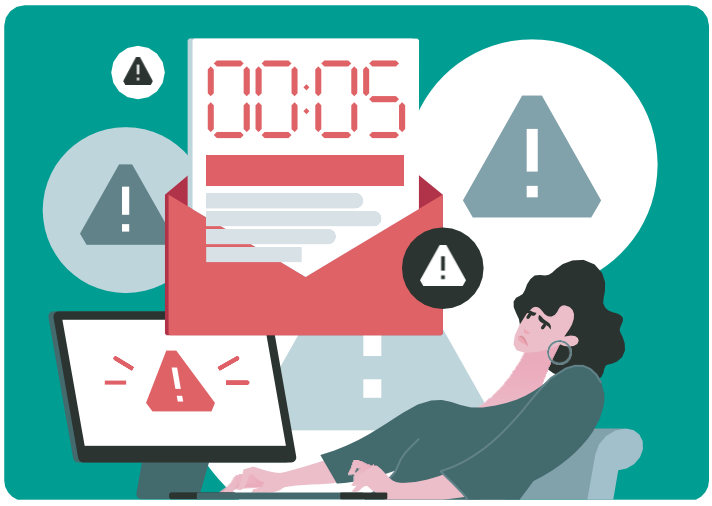


La maturité des PME ivoiriennes en matière de cybersécurité à la loupe.

Comment les petites et moyennes entreprises de Côte d'Ivoire envisagent la cybersécurité ? Quels outils utilisent-elles et quels conseils peut-on leur apporter pour une meilleure résilience en matière de cybersécurité ?

kaspersky BRING ON THE FUTURE

En savoir plus : kaspersky.com

Mot d’accueil

Pascal Naudin, Head of B2B Sales, Afrique du Nord, de l’Ouest et Afrique Centrale.

La question de la cybersécurité est indissociable de la question de la transformation numérique et les entreprises devraient en saisir à la fois le sens, mais aussi les tenants et aboutissants. Depuis des années que Kaspersky exerce sur le territoire, nous échangeons avec des entreprises et des administrations sur notre thème de prédilection qu’est la cybersécurité, et même la cyber-immunité, afin qu’elles développent une stratégie cyber. L’environnement virtuel dans lequel nous gravitons rend complexe cette question de cyber et les entreprises mais n’en maitrisent pas toujours le sens n’identifient pas la réalité de leurs besoins ou de leur exposition.

Nous les éditeurs, sommes en partie responsables de cette confusion. Pendant longtemps nous avons été en avance technologiquement vis-à-vis de la maturité numérique de nombreuses entreprises et nous n’avons pas toujours su adresser les bons enjeux, ou communiquer de manière appropriée. La multiplication du jargon et des acronymes n’aide pas non plus à une bonne compréhension des différentes technologies et services accessibles pour les entreprises. Etre en avance technologiquement est un atout puisque cela nous permet d’être toujours plus performants que les cybercriminels, mais en même temps il faut que nos clients s’approprient ces technologies, ce que nous nous efforçons de faire dans le cadre notamment de nos événements KNext.

Alors que les petites et moyennes entreprises représentent la grande majorité du tissu économique local, et international, les médias et beaucoup d’experts se focalisent avant tout sur les risques auxquels sont exposées les grandes administrations, les industries, les multinationales. Comment se positionnent les PME là-dedans ? Ne devraient-elles pas se préoccuper un peu davantage de la réalité du paysage des menaces pour réfléchir à implémenter des stratégies de cybersécurité adaptées à leurs besoins, et à leur exposition ? Mais d’ailleurs est-ce qu’il existe des technologies et des services à disposition des entreprises de petite et moyenne taille ? Est-il possible d’investir dans une stratégie de cybersécurité sans dépenser des centaines de millions de francs ?

Chez Kaspersky, nous avons à cœur de protéger les entreprises de toutes les tailles contre les menaces cyber. Pour cela, il est d’abord important de faire comprendre à chacune d’entre-elles son champ d’exposition aux menaces, de faire prendre conscience des risques qui se cachent derrière des cyberattaques et de démystifier un certain nombre d’idées reçues. Non, la cybersécurité n’est pas réservée aux grandes entreprises, non, ce n’est pas trop compliqué, non ce n’est pas non plus une contrainte au développement économique. Elle devrait même être intégrée directement à la politique de digitalisation et de développement économique.

C’est pourquoi, nous avons décidé de faire appel à un cabinet d’étude, OpinionWay pour essayer de mettre des chiffres sur un constat : la conscience de la cybersécurité existe mais la maturité cyber quant à elle est encore fragile. Prendre des décisions éclairées adaptées à la réalité du besoin des entreprises n’est pas chose aisée. Avec notre écosystème de partenaires nous avons à cœur d’accompagner les entreprises et les faire monter en compétences progressivement pour qu’enfin, elles puissent reprendre le pouvoir sur leur cybersécurité et avoir une longueur d’avance sur la cybercriminalité.

Introduction

En Afrique, le développement de la connectivité et des infrastructures de réseau a été fulgurant. Entre 2021 et 2022, le nombre d'Africains ayant accès à internet a augmenté de 7% pour atteindre le chiffre des 40% d'internautes[1]. Cependant, cette croissance rapide ne s'est pas accompagnée d'un élargissement des compétences en matière de cybersécurité. Le gap de croissance entre le développement des infrastructures, les usages numériques et la compréhension des enjeux cyber fait peser une menace importante sur la souveraineté stratégique et économique des États du continent. Ainsi, au cours des six derniers mois de 2021, en Afrique francophone subsaharienne, des incidents de cybersécurité ont été détectés dans 56 % des entreprises de plus de 500 personnes, 33 % des entreprises employant entre 100 à 500 personnes, et 25 % des entreprises de moins de 100 personnes[2]. Le coût de ces cybercrimes et infractions commises est estimé à 1,37 milliards d'euros[3].

Pourtant, le rapport de 2020 « *Global Cybersecurity Index* » de l'Union internationale des télécommunications (UIT) indiquait que seuls 23 pays africains s'étaient dotés d'une stratégie nationale de cybersécurité. En 2021, après avoir été la cible d'une douzaine d'attaques de grande ampleur sur ses réseaux depuis 2018, entraînant de lourdes pertes économiques chiffrées en millions d'euros, la Côte d'Ivoire s'est dotée d'une Stratégie Nationale de Cybersécurité 2021-2025 qui comprend notamment la création d'une Agence Nationale de la Cybersécurité. Véritable enjeu de souveraineté stratégique et économique pour le pays, la lutte contre les menaces cybercriminelles s'est imposée à l'agenda politique du pays. Mais cette prise de conscience doit être collective. Le gouvernement seul ne peut mener à termes un tel chantier et l'ensemble des parties prenantes, y compris la population, doivent se mobiliser en faveur d'un écosystème numérique sûr.

Ainsi l'objet de la présente étude proposée par *Kaspersky* intitulée "***La maturité des PME ivoiriennes en matière de cybersécurité à la loupe",*** est de faire un état des lieux de la compréhension des enjeux cyber par les entreprises afin de les sensibiliser et de les outiller pour faire face à ces défis qui sont encore trop invisibilisés au sein du pays. En effet, d'après la Plateforme de Lutte Contre la Cybersécurité de Côte d'Ivoire, il apparaît que seulement 50% des risques cyber sont résolus. Il est ainsi urgent de faire de ce défi, un pilier du développement de la nouvelle économie numérique ivoirienne.

Méthodologie

Dans le cadre de cette étude menée avec *Opinion Way*, 300 entreprises représentatives du tissu économique formel de la Côte d'Ivoire ont été auditionnées sur leur connaissance, appréhension et gestion des menaces et attaques cybercriminelles. Il s'agit d'entreprises publiques, à 6%, et privées ayant entre 0 et plus de 15 ans d'ancienneté. Toutes sont basées à Abidjan, Bouaké ou San Pedro et emploient entre 10 et 200 employés. A l'issue de cette enquête, Kaspersky a analysé les résultats du rapport et propose des recommandations adaptées à destination des entreprises.

[1] « Connectivité : 40 % de la population africaine est connecté à Internet (UIT) », *CIO Mag*, septembre 2022.

[2] « Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne », *PWC*, mars 2021.

[3] « Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne », *PWC*, mars 2021.

Chiffres clés :

Les PME ont la volonté d'investir dans le numérique et dans la cybersécurité.

57% des entreprises estiment que le numérique est une priorité

90% des entreprises estiment que les questions de cybersécurité sont au moins centrales, si ce n'est indispensables

80% des PME ivoiriennes prévoient d'investir dans la cybersécurité dans les années à venir, majoritairement pour améliorer la protection des données.

La notion de cybersécurité ne donne pourtant pas lieu à des actions concrètes :

81% des entreprises n'ont jamais donné ou reçu de formation en cybersécurité

66% des répondants indiquent que la cybersécurité n'est jamais abordée lors des comités de direction

24% gèrent la question de cybersécurité « seuls » sans faire appel à des professionnels externes

Un manque de lucidité vis-à-vis des outils et de l'exposition aux menaces.

Un tiers des PME ivoirienne est certaine d'être bien protégée contre les menaces.

Parmi elles :

Seules 7% ont une solution EDR

96% utilisent des antivirus grand public individuels

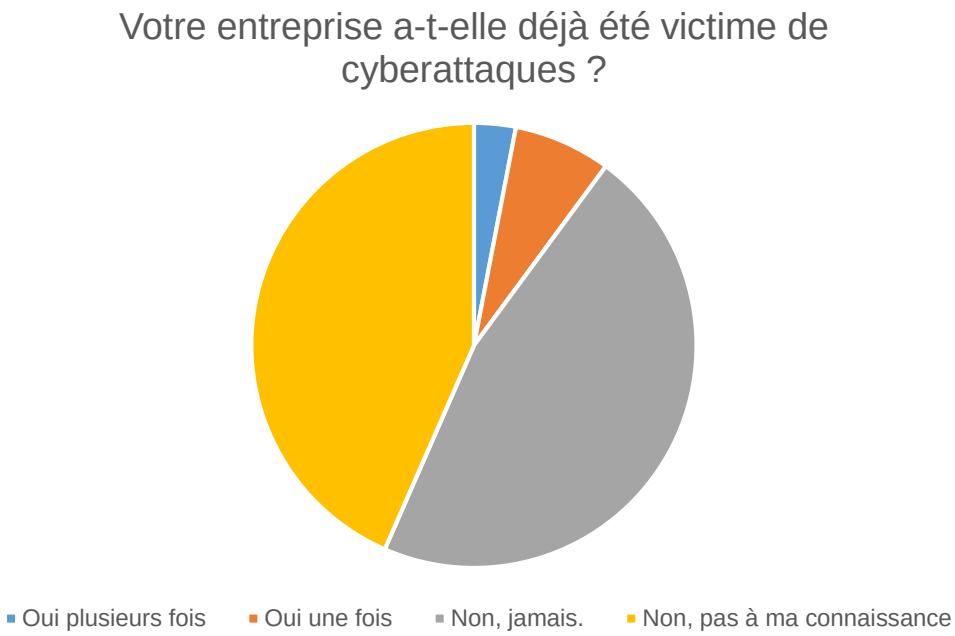
13% forment régulièrement leur personnel aux bonnes pratiques de cybersécurité

89% des entreprises estiment ne jamais avoir été ciblées par des cyberattaques. Les chiffres Kaspersky indiquent pourtant plus de 2 millions d'attaques sur les PME en Côte d'ivoire en 2022

67% des entreprises ne s'estiment pas exposées / pas concernées par le risque cyber.

1 – La perception de la menace cyber pour les PME

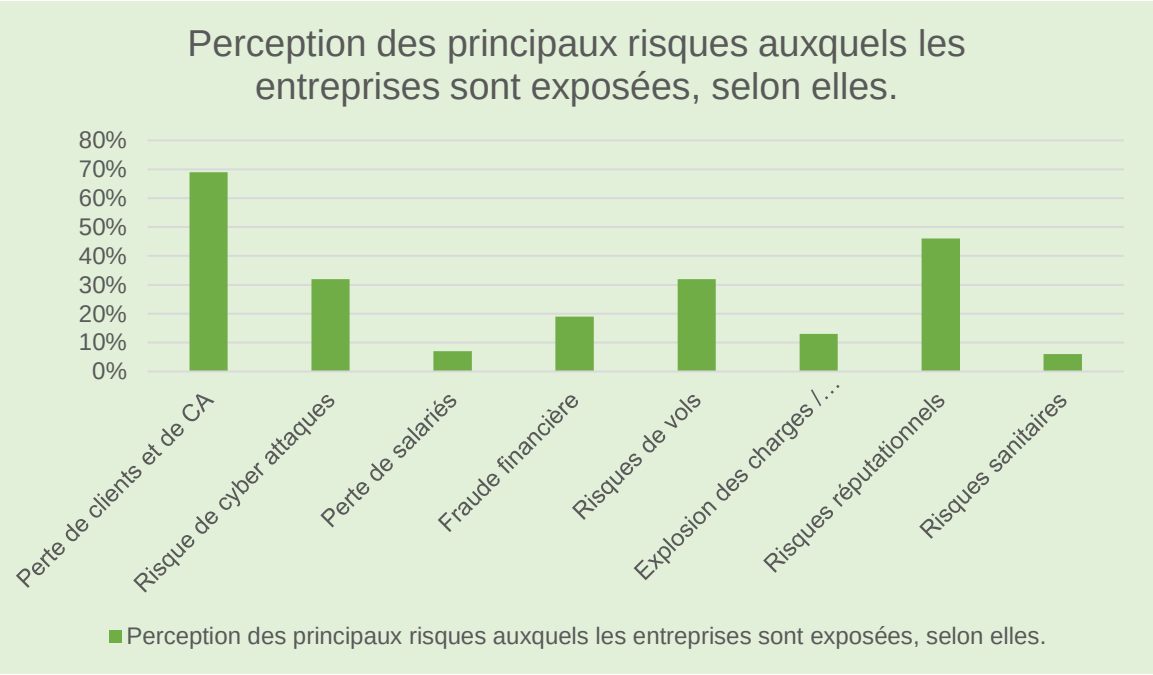
Si les petites et moyennes entreprises en Côte d'Ivoire ont connaissance de l'existence de cybermenaces et jugent la question du numérique comme des priorités au sein de leurs entreprises, elles sont peu conscientes du risque et de l'exposition de leurs structures à la menace cyber. Un chiffre assez parlant ressort : 67% des PME estiment ne pas être du tout, ou assez peu exposées aux risques de cybermenaces. Un chiffre qui témoigne d'un manque de compréhension de l'attractivité que constituent les entreprises pour les cybercriminels.



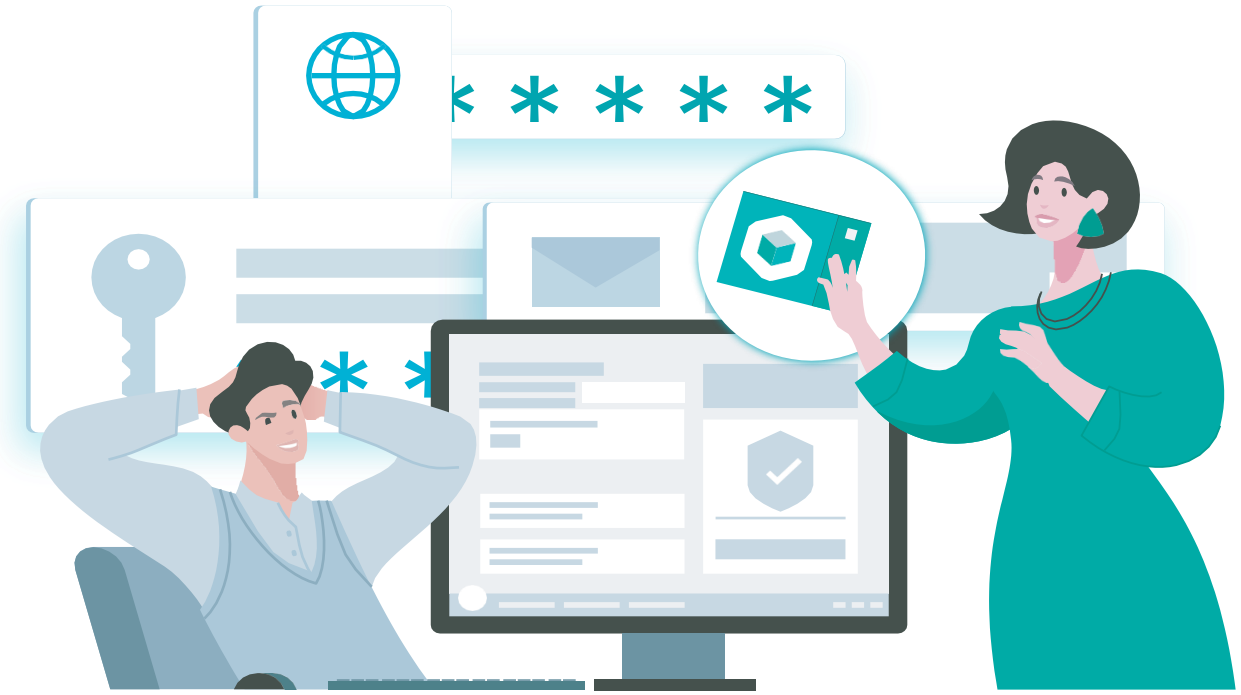
Quand on compare cette analyse aux chiffres détectés par nos chercheurs en cybersécurité, on constate que malheureusement, les PME ivoiriennes sont bien victimes de cyberattaques. En 2022, plus de 2,8 millions d'attaques sur les PME ont été détectées en Côte d'Ivoire, ciblant plus de 27 500 entreprises distinctes. Des chiffres évocateurs de deux réalités : non seulement les entreprises ivoiriennes sont de plus en plus ciblées par les menaces - les chiffres de 2021 faisant l'état de 1,7 millions d'attaques environ – mais en plus, les entreprises victimes de problèmes de sécurité le sont plusieurs fois, le nombre d'entreprises ciblées étant largement inférieur au nombre total d'attaques. Si l'on s'intéresse aux différents types de menaces détectées, on compte, sur l'année 2022, des menaces en provenance d'emails (plus de 479 000), des menaces en provenance de sites web malveillants (plus de 560 000) ou encore des menaces en provenance du poste local et donc via une infection de type disque amovible, clé USB etc. (plus d'1,7 million). Selon nos données, la Côte d'Ivoire semble être le pays d'Afrique de l'Ouest le plus ciblé par les attaques au niveau des petites et moyennes entreprises. Une prise de conscience de leur exposition au risque semble donc indispensable pour les entreprises ivoiriennes.

Pascal Naudin, Head of B2B Sales en Afrique de l'Ouest n'est pas étonné par ces résultats, il commente "*A chaque fois que nous venons chez un client et qu'on réalise un POC (proof of concept) pour l'installation d'une solution de sécurité, qu'il s'agisse d'EDR Optimum ou EDR Expert, on constate que l'entreprise qui pensait anticiper la menace était en fait déjà attaquée. Dès la mise en test de nos solutions sur une partie infime du parc, nous recevons systématiquement des alertes. Certaines se corrigent facilement, d'autres nécessitent de faire appel à notre service de réponse à incident à travers lequel nous dépêchons des analystes qui vont travailler sur l'infrastructure complète du client afin de détecter toutes les traces liées à une, ou plusieurs attaques* ».

Lorsque l'on pose la question aux dirigeants et responsables des entreprises ivoiriennes interrogées sur leur gestion des risques et sur leur analyse du risque, le risque cyber n'apparaît qu'en troisième position de l'ordre des priorités. Dans l'ordre des risques les plus importants identifiés pour leur entreprise arrive la perte de clients et de chiffres d'affaires (69%), le risque de réputation (49%) et le risque cyber (32%) qui arrive au même niveau que le risque de vols et de fraudes (32%). Cette analyse de risque est une preuve supplémentaire du manque de perspectives et de compréhension des enjeux de la cybersécurité. En effet, les cyberattaques peuvent également causer des pertes financières, des pertes de clients, être dommageables pour la réputation d'une entreprise, provoquer l'arrêt total de la productivité, représenter une perte d'avantage compétitif - par exemple, en cas d'espionnage - ou encore causer la fuite d'employés.



En ce qui concerne les risques auxquelles les entreprises ont déjà été confrontées, la plupart des entreprises répondantes estiment être plutôt à l'abri des risques majeurs dont ils ont la connaissance, avec 57% des entreprises indiquant ne pas avoir dû faire face à un risque en particulier. Pour les entreprises ayant déjà été dans la tourmente, les risques principaux auxquels elles ont été exposées sont la perte de clients et de CA (18%), les risques liés à la réputation (12%), et les risques de vols/fraudes (12%). Les risques liés à la cybersécurité arrivent en 4e position des risques les plus fréquemment rencontrés par les PME avec 10% des entreprises admettant avoir déjà dû y faire face.



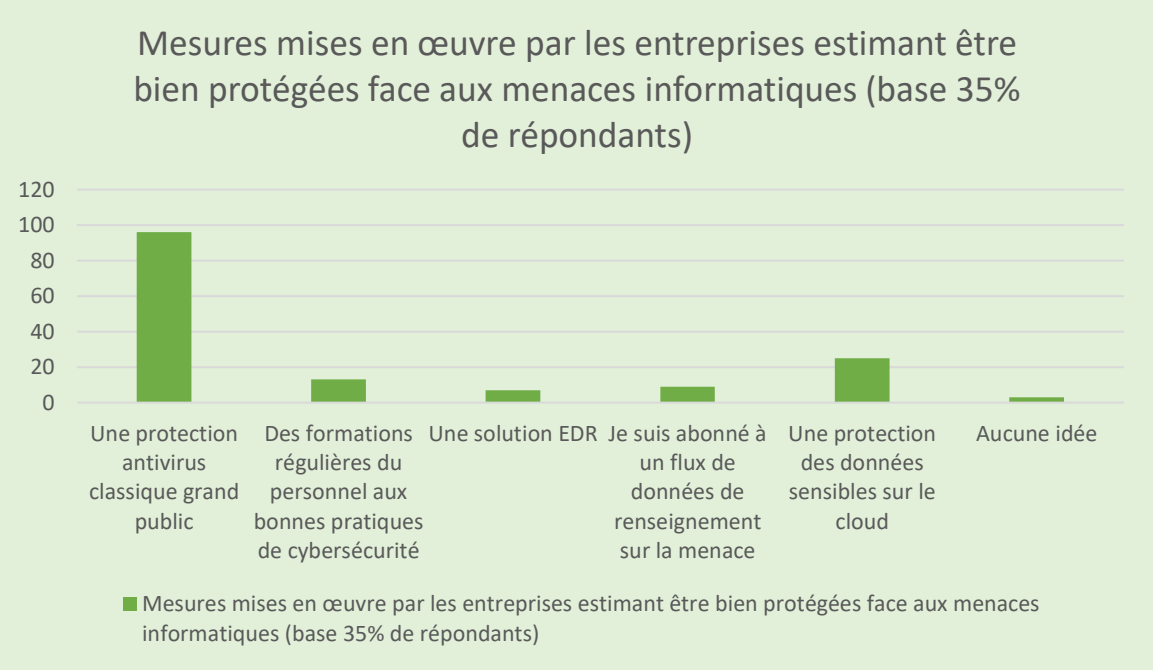
2- Confusions dans la technique et les notions clés en matière de sécurité. Quels outils pour quels besoins ?

Les entreprises ivoiriennes ont conscience que leur protection n'est pas forcément optimale face aux cybermenaces. En effet, 35% des entreprises s'estiment correctement protégées face aux cybermenaces, 36% savent qu'elles ne le sont pas suffisamment et 29% ne sont pas certaines de l'être et donc, n'ont soit pas conscience des technologies et stratégies de cybersécurité déployées dans leur entreprise, soit elles ne sont pas convaincues qu'elles soient les plus adaptées à leur situation.

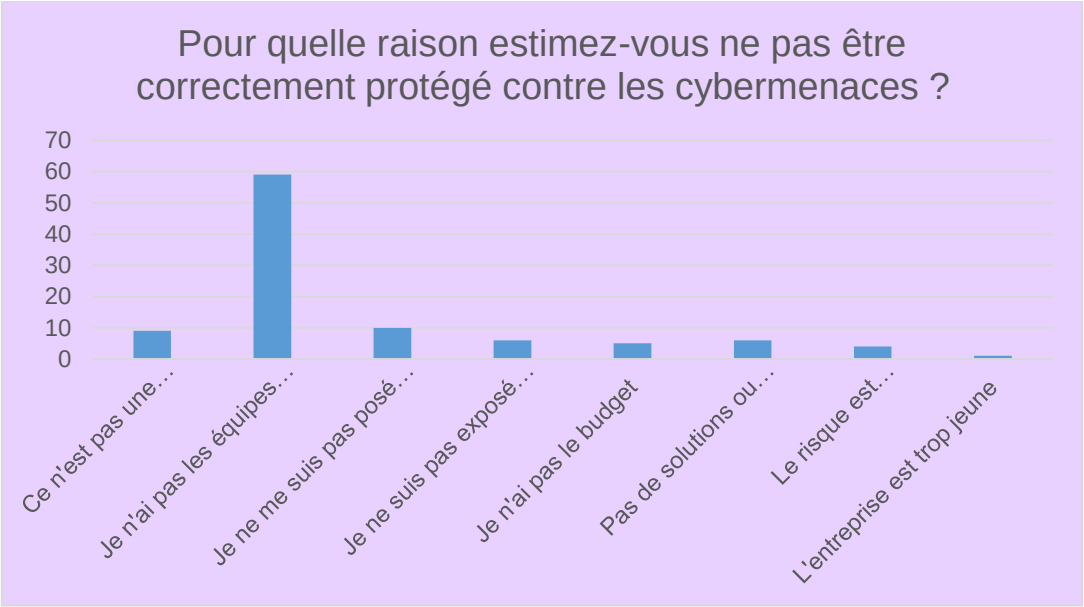
Ce constat s'accompagne malheureusement de preuves qu'en 2023, encore de nombreuses entreprises ne sont pas correctement équipées, et donc sensibilisées aux enjeux de la cybersécurité pour les entreprises. En effet 96% des PME qui estiment être correctement protégées face aux cybermenaces indiquent avoir des solutions antivirus grand public déployées sur les postes de leurs salariés. Si ces solutions ne sont pas mauvaises en soi, cette approche n'est pas recommandée pour les entreprises puisqu'elles ne permettent pas au responsable informatique d'avoir la maitrise de ces solutions et de les piloter depuis un poste unique.

Concrètement, cela signifie que la responsabilité des mises à jour, des patchs, de la gestion des vulnérabilités ou même des bonnes pratiques d'hygiène numérique sont laissées à la seule responsabilité de l'utilisateur individuel qui est administrateur de son poste. Seuls 7% des répondants ont déclaré avoir une solution EDR de déployée dans leur entreprise et 25% déclarent avoir une solution de protection des données sensibles sur le cloud.

Pascal Naudin explique « *Il nous est arrivé (et ça arrive encore) qu'un client nous questionne sur nos produits et nous nous rendons compte qu'il utilise la version pour particulier. Même si les signatures virales sont identiques, la méthode de déploiement et de mise à jour n'est pas du tout adaptée et recommandée. En prenant la version B2C, le client ne maitrise rien car l'utilisateur peut désinstaller le logiciel puisqu'il est l'administrateur de son poste. De plus aucune stratégie de sécurité ne peut être mise en place de façon globale ce qui est extrêmement dangereux. Nous avons eu des clients avec environ 1000 postes qui avaient ce mode de fonctionnement il y a encore moins d'un an*. »



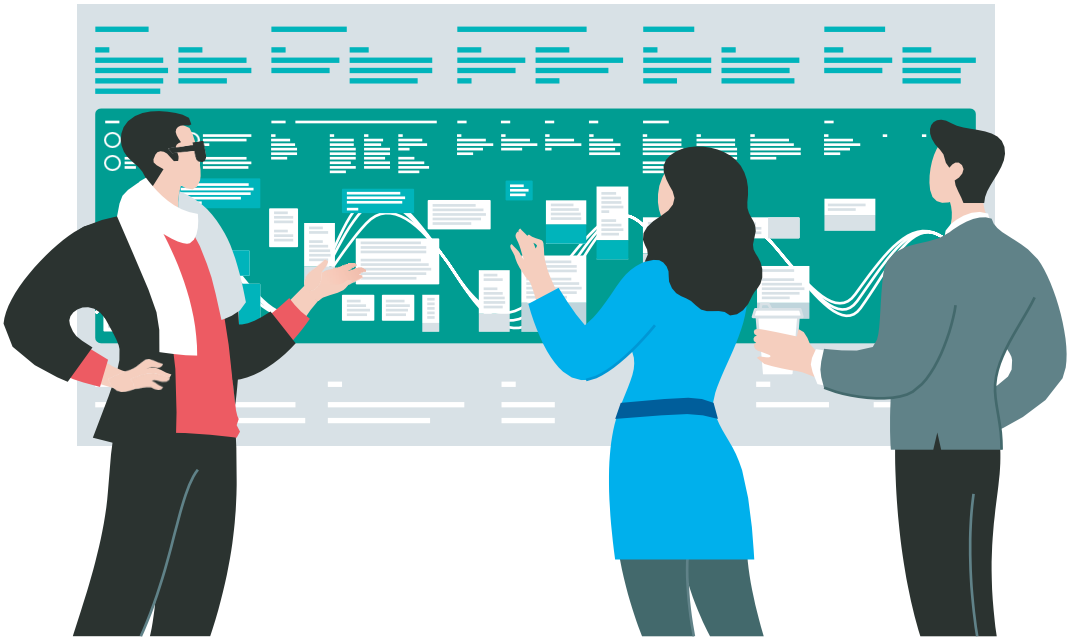
En ce qui concerne les entreprises estimant ne pas être bien protégées vis-à-vis des cybermenaces, 9% admettent qu'il ne s'agit pas d'une priorité business, 6% estiment ne pas être exposées au risque et 59% estiment ne pas avoir les équipes adaptées.



Des pratiques et outils pas toujours adaptés à la réalité des usages.

Afin de comprendre les usages en matière de digitalisation des entreprises, nous avons posé la question du télétravail et des outils utilisés par les employés dans ce cadre-là. On constate malheureusement que les pratiques ne suivent pas toujours les recommandations de base en matière de cybersécurité.

Même si le télétravail n'est pas majoritaire dans les PME en Côte d'Ivoire avec 76% des répondants indiquant que les salariés ne font pas du tout de télétravail, pour le quart restant, beaucoup de risques sont pris en matière d'exposition aux menaces cyber. Seules 25% des entreprises dont les salariés font du télétravail proposent des outils tels que des VPN/token ou agents sécurisés pour se connecter au réseau de l'entreprise, exposant alors les données confidentielles aux intrus. 38% des entreprises faisant du télétravail utilisent des outils de visioconférence ou de collaboration open source ou gratuits et seules 31% ont mis en place des formations de cybersécurité pour les salariés travaillant à distance. C'est plus que la moyenne des entreprises qui ne proposent pas de télétravail, mais cela reste insuffisant au regard des nombreuses menaces énoncées en début de rapport. Moins de la moitié des entreprises proposant du travail ont fourni du matériel dédié à leurs équipes (38%) et seul un peu plus d'un quart d'entre elles ont automatisé les mises à jours logiciels à distance, le reste laissant la main aux salariés pour gérer leurs politiques de mises à jour de sécurité.



Pour protéger les entreprises et réduire la probabilité d'un incident de cybersécurité, Kaspersky recommande les mesures suivantes :

· Éliminez la probabilité d'une attaque par force brute lorsqu'un adversaire tente d'accéder à votre point d'entrée numérique en soumettant de nombreux mots de passe ou de nombreuses phrases de passe dans l'espoir de finir par les deviner correctement. Mettez en place une politique de mot de passe solide pour l'ensemble de vos ressources numériques et celles de vos employés. Un mot de passe sûr doit être composé d'au moins huit lettres, d'un chiffre, de lettres majuscules et minuscules et d'un caractère spécial. Si vous soupçonnez que le mot de passe a été compromis, modifiez-le immédiatement. Une solution de sécurité, comme **Kaspersky Small Office Security**, avec un gestionnaire de mots de passe intégré, vous aidera à mettre cette approche en pratique sans effort.

· Ne laissez pas les adversaires profiter des vulnérabilités de vos logiciels. Ce sont des proies faciles à pour les attaquants qui exploitent les vulnérabilités dans le but d'obtenir un accès initial aux données d'une entreprise. N'ignorez pas les mises à jour des fournisseurs de logiciels et d'appareils. En général, elles apportent non seulement de nouvelles fonctionnalités et des améliorations de l'interface, mais elles permettent également de combler des failles de sécurité.

· Protégez-vous contre les attaques par ransomware, lorsqu'un intrus chiffre les données de l'entreprise et demande une rançon pour les déchiffrer. Outre la mise à jour de tous les appareils, une autre étape importante consiste à mettre en place des sauvegardes hors ligne de vos données afin de pouvoir y accéder rapidement si l'un des fichiers de votre organisation est chiffré. Cette menace étant en augmentation, la solution de sécurité pour votre entreprise doit être capable d'assurer une **protection à 100 %** contre les ransomwares. Ses fonctionnalités doivent inclure l'identification et le blocage des logiciels malveillants inconnus avant leur exécution, et le lancement de la création automatique de copies de sauvegarde en cas d'attaque ;

· Maintenir un niveau élevé de sensibilisation à la sécurité parmi les employés. Encouragez vos équipes à s'informer **sur les menaces** actuelles ainsi que les moyens de protéger leur vie personnelle et professionnelle, et suivez des formations **gratuites pertinentes**. Un autre moyen consiste à mettre en place des programmes de formation tiers efficaces pour les employés, tels que le programme **automatisé de sensibilisation à la sécurité de Kaspersky**, qui permet d'acquérir des compétences et des pratiques concrètes en matière d'hygiène cyber.

Pascal Naudin commente « *On voit quand même une évolution positive au niveau des demandes des clients. Même si on a encore des demandes pour les solutions les plus basiques type EPP à cause notamment d'un manque de ressources techniques pour exploiter des solutions, de plus en plus d'entreprises, même très petites font évoluer leur demande pour s'équiper de solutions de protection via une console cloud. La demande évolue, en même temps que la réalité de la menace et on constate quand même un accroissement des questionnements autour de nos solutions disponibles sur un modèle MSP. C'est positif, on va dans la bonne direction et beaucoup de clients souhaitent ce qui se fait de mieux sur le marché. Après, la question est toujours la même : savoir s'ils disposent des ressources humaines, financières et techniques pour être capables de les opérer. On avance, mais il reste encore un peu de chemin à parcourir.* »

Comment Kaspersky Endpoint Security Cloud protège votre entreprise.

Une seule attaque ciblant une entreprise qui ne s'est pas préparée à affronter de tels risques peut entraîner :
• la perte de données sensibles, y compris de propriété intellectuelle ;
• la fuite d'informations confidentielles relatives aux clients et aux collaborateurs ;
• un impact négatif sur la productivité des collaborateurs qui se répercute directement sur la rentabilité.
Contrairement aux grandes sociétés, les TPE/PME ne disposent généralement pas d'équipes informatiques internes importantes. Elles ont besoin d'une solution de sécurité facile à installer et à mettre en œuvre, voire d'externaliser sa gestion à distance.

La solution Kaspersky Endpoint Security Cloud couvre les besoins spécifiques de ces entreprises en les aidant à protéger l'ensemble de leurs terminaux Windows et Mac, de leurs serveurs de fichiers Windows et de leurs appareils mobiles Android et iOS. La protection leader du marché qu'elle offre est rapide à déployer, à mettre en œuvre et à exécuter sans qu'il soit nécessaire d'acheter du matériel supplémentaire. En outre, tous les paramètres de sécurité peuvent être gérés à distance, depuis tout appareil doté d'une connexion Internet.

Atouts principaux de cette solution pour les PME :

- Toutes les fonctionnalités de sécurité sur l'ensemble des ordinateurs de bureau et ordinateurs portables Windows ou Mac, des serveurs de fichiers Windows, sans oublier des appareils mobiles Android et iOS, peuvent être configurées et gérées via une console d'administration centralisée. Vous n'avez pas besoin de compétences particulières en matière de sécurité informatique pour utiliser la console et gérer votre sécurité. Par ailleurs, les politiques de sécurité que vous appliquez sur tous vos terminaux sont faciles à définir.
- La console basée dans le Cloud et prête à l'emploi permet aux administrateurs d'utiliser quasiment n'importe quel appareil doté d'une connexion à Internet pour configurer et régler l'ensemble des fonctionnalités de protection, pour tous les terminaux. Si vous choisissez d'externaliser la gestion de votre sécurité informatique, la console permettra également à vos consultants externes de la gérer à distance, en toute simplicité. Étant basée dans le Cloud, vous n'aurez pas besoin d'investir dans du matériel supplémentaire ou d'en assurer la maintenance et bénéficierez d'une configuration initiale extrêmement rapide.

Kaspersky EDR Optimum : garder une longueur d'avance sur les menaces grâce à une solution complète qui ne drainera pas vos ressources.

Kaspersky EDR Optimum a été développé afin de répondre au besoin d'une solution de sécurité de qualité, capable de faire face aux menaces actuelles complexes malgré les ressources limitées. Il est conçu pour détecter les menaces de manière robuste, y répondre de façon proactive, et simplifier les opérations quotidiennes. Ce type de solution permet aux entreprises qui ne disposent pas d'équipes dédiées à la gestion d'un EDR de disposer des meilleures technologies même si elles n'ont pas les moyens d'avoir un SOC. Kaspersky Optimum Security offre une solution efficace de détection et de réponse aux menaces, soutenue par une surveillance de la sécurité 24h/24, 7j/7, des réponses automatisées et une recherche des menaces, ainsi que par le soutien et les conseils des experts de Kaspersky.

Les méthodes de prévention automatique constituent le fondement de toute protection des terminaux, mais elles doivent être complétées par des outils avancés si vous vous retrouvez à devoir gérer les menaces évasives les plus dangereuses. Kaspersky Optimum Security fournit offre des capacités avancées de détection basée sur le Machine Learning et de réponse rapide, le tout fourni depuis le cloud. Votre équipe peut désormais traiter avec rapidité et précision les menaces qui auparavant l'empêchaient de dormir la nuit. Kaspersky Optimum Security vous permet de réduire les risques liés à la perte d'argent, de clients et de réputation, et renforce vos défenses contre les nouvelles menaces inconnues et évasives

3– La cybersécurité, une question de technologies mais surtout d'humain.

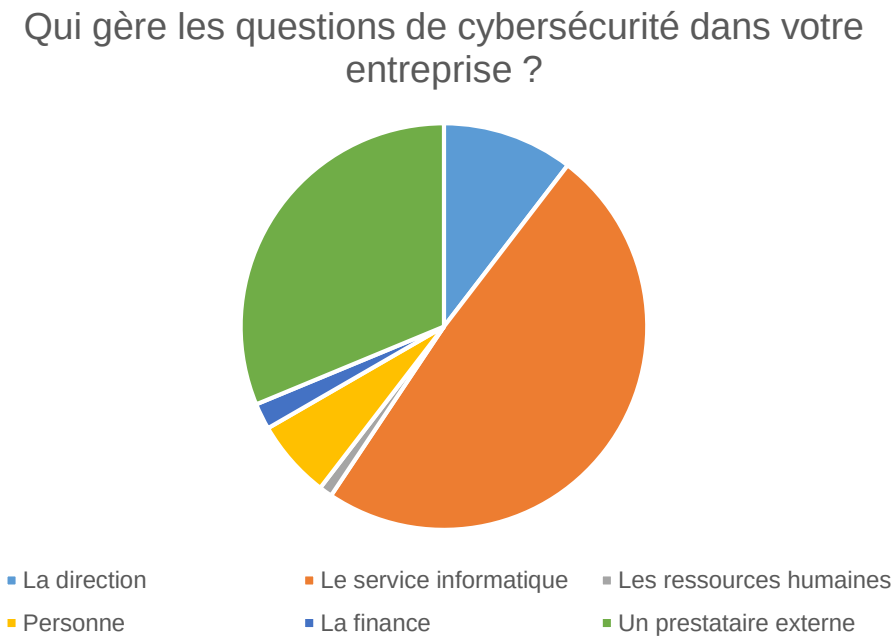
La cybersécurité est une question de technologies, certes, mais aussi d'humains. D'une part, parce qu'il faut des humains qui soient capables de comprendre et d'opérer les différentes technologies déployées sur le parc informatique - il ne sert à rien d'empiler les couches de sécurité si personne n'est capable de mettre à jour les bases, ni même de prendre des actions en fonction des alertes remontées. D'autre part, parce que de nombreuses vulnérabilités et failles de sécurité en entreprise sont également dues à des erreurs humaines à cause d'employés pas toujours sensibilisés aux risques cyber ou formés aux bonnes pratiques d'hygiène numérique.

Chez Kaspersky nous sommes convaincus qu'une bonne stratégie de cybersécurité commence par une politique interne de bonnes pratiques et d'outils. Dans un monde qui se digitalise de plus en plus avec des salariés amenés à travailler en dehors du bureau, et dont le périmètre de sécurité peut plus difficilement être maitrisé, une formation de base aux bonnes règles du numérique semble indispensable. Cela commence par le fait d'imposer des mots de passe fort, la double authentification, la capacité de reconnaitre des mails de phishing de mails « officiels », par le fait de ne pas utiliser les appareils professionnels pour des usages personnels, de systématiquement scanner les appareils amovibles avant de les insérer dans le lecteur USB de l'ordinateur, de ne pas cliquer sur des liens suspicieux et d'uniquement utiliser des sites de e-commerce officiels etc. Cela requiert des notions sur les portes d'entrées des différents malwares, des notions sur les différents types de menaces qui existent ainsi que des codes liés à la cybersécurité. Concrètement : 66 % des personnes interrogées dans le cadre de cette étude n'ont absolument aucune notion de ce qu'est un ransomware, qui représente pourtant la menace principale à laquelle les entreprises sont exposées en 2022.

Parmi les chiffres qui nous interpellent : 13% des entreprises ayant le sentiment d'être bien protégées face aux menaces indiquent proposer des formations régulières aux bonnes pratiques de cybersécurité à leur personnel. Pour qu'une société soit bien protégée, il faudrait que ce chiffre atteigne les 100%. En parallèle, 59% des entreprises qui estiment ne pas être protégées face aux cybermenaces jugent que c'est parce qu'elles n'ont pas le personnel adapté pour déployer de bonnes approches en matière de cybersécurité.

Pour pallier à ces problématiques de manque de ressources humaines, qui constituent un défi international, Kaspersky a déployé des outils qui permettent d'automatiser une partie de la détection et de la réponse aux incidents. Ainsi les équipes informatiques peuvent se concentrer sur les tâches plus importantes. En cas de manque cruel de personnel, des solutions telles que le Managed Detection and Response sous-traitent toute cette partie détection et réponse aux incidents de cybersécurité.

Lorsque l'on pose la question aux entreprises de qui gère les questions de cybersécurité, seules 30% indiquent faire appel à un prestataire dédié, 6% admettent qu'il n'y a personne et 47% ont un service informatique dédié.



Un autre chiffre qui indique qu'il est nécessaire de continuer à sensibiliser les entreprises à l'importance de la formation des salariés à la cybersécurité, mais également des membres de la direction, et des responsables informatiques, c'est que sur toutes les entreprises interrogées, 81% des répondants ont admis ne jamais avoir reçu, ni donné de formation en cybersécurité. 12% en ont reçu ou donné une fois dans leur carrière, et 7% seulement participent régulièrement, ou donnent régulièrement des formations en cybersécurité. Quand on sait qu'une large majorité des incidents peut être évitée avec une bonne politique de mots de passe et des bonnes pratiques d'hygiène numérique, à travers lesquelles les salariés savent reconnaitre un mail de phishing d'un mail légitime ou savent sur quels types de lien ne pas cliquer par exemple.

Les formations Kaspersky en matière de cybersécurité

Afin d'ajouter les compétences humaines à la stratégie de cybersécurité d'une entreprise, Kaspersky a également déployé des programmes de formations, allant de la sensibilisation de tous les salariés d'une entreprise aux bonnes bases d'hygiène numérique, aux formations plus techniques dédiées aux professionnels de l'informatique et proposées par nos chercheurs du GREAT.

Tour d'horizon de quelques-unes des principales formations proposées par Kaspersky, pour les entreprises. Certains de ces modules sont intégrés directement dans les offres de sécurité 360°.

KASAP : Il s'agit d'une plateforme en ligne, destinée à tous les employés d'une entreprise pour les aider à développer progressivement des connaissances efficaces et pratiques en matière d'hygiène numérique. Le programme est composé de leçons interactives, de renforcements constants, de tests et de simulations d'attaques de phishing pour s'assurer que les compétences puissent être appliquées. Les principaux thèmes abordés pendant la formation sont les mots de passe et comptes, les mails, la navigation web, les messageries et réseaux sociaux, la sécurité du PC, les appareils mobiles, les données confidentielles et le RGPD.

CITO : Cybersecurity for IT online. Il s'agit d'une formation en sécurité interactive qui fournit des compétences approfondies en cybersécurité et un premier niveau de compétences en réponse à incidents. Cette formation est dédiée aux spécialistes informatiques généralistes et est composée de 6 modules : logiciels malveillants, programmes et fichiers potentiellement indésirables, basiques de l'investigation, réponse aux incidents de phishing, sécurité des serveurs et sécurité de l'active directory.

Le programme équipe les professionnels de l'IT de compétences pratiques pour reconnaître un scénario d'attaque possible dans un incident apparemment bénin, et pour collecter les données relatives à l'incident afin de les transmettre à la sécurité informatique. Il suscite également une passion pour la chasse aux signes d'activité malveillante, cimentant le rôle de tous les membres de l'équipe informatique en tant que première ligne de défense de la sécurité.

X-TRAINING : Le paysage des menaces étant en constante évolution, il est essentiel que les spécialistes de la sécurité informatique maintiennent leurs compétences à jour. Grâce à notre formation en ligne, vous pouvez apprendre des stratégies efficaces de détection et d'atténuation des menaces depuis le confort de votre maison, grâce à des cours pratiques très concrets. Nos auteurs experts savent comment gérer au mieux les menaces posées par les plus de 400 000 échantillons de logiciels malveillants que nous rencontrons chaque jour, et comment partager ces connaissances avec ceux qui luttent contre les dangers en constante évolution de la cyber-réalité d'aujourd'hui.

La prochaine génération d'experts mondiaux qui suivra ces cours acquerra les connaissances actualisées nécessaires pour se défendre contre les attaques les plus sophistiquées. Que vous soyez un professionnel de l'InfoSec souhaitant améliorer vos compétences ou un chef d'équipe cherchant à investir dans votre équipe de SOC et de réponse aux incidents, nous pouvons vous aider.

Le modèle MSP, pour les entreprises ne disposant pas de toutes les ressources humaines en interne.

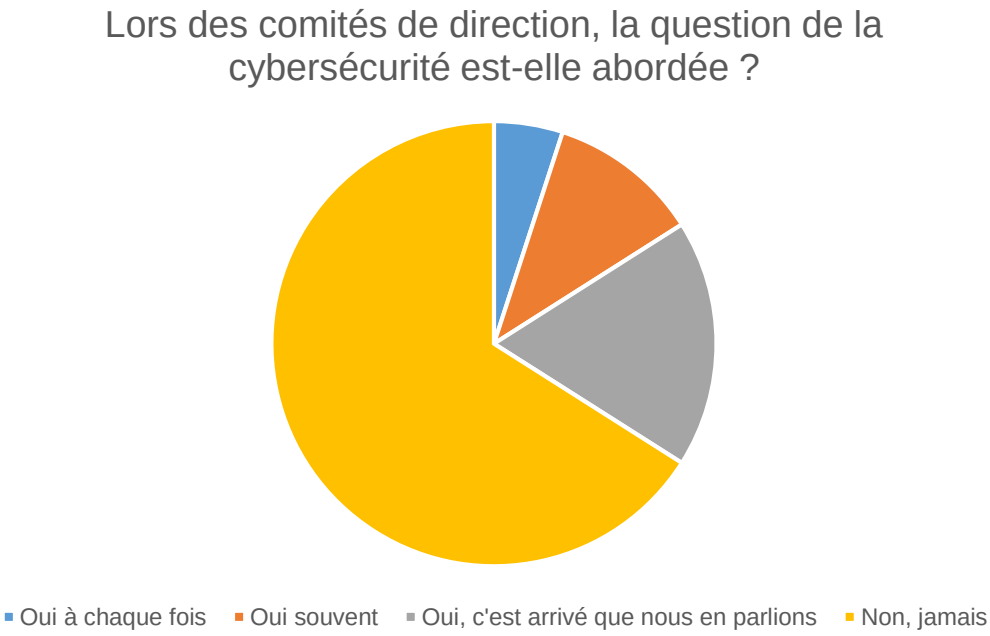
Afin de pallier le manque de maturité des entreprises, quelles que soient leur taille, nous pouvons également recommander de passer par un partenaire de services de sécurité managés (MSP). Un MSP (Managed Service Provider), ou fournisseur de services managés en français, est une entreprise de services informatiques qui gère les systèmes informatiques de ses clients à distance. Fini le temps où le professionnel de l'informatique attend d'être contacté par le client en cas de panne (modèle Break/fix). Maintenant, avec le modèle MSP, le professionnel est proactif dans le management des parcs informatiques pour assurer un fonctionnement optimal de ces derniers. L'autre plus-value de ce modèle est la méthode de facturation. Cette dernière se fait de façon forfaitaire avec le plus souvent un abonnement mensuel. La plupart des solutions de Kaspersky sont proposées sur un modèle MSP, et même les offres et flux de threat intelligence depuis peu. Cela permet à la fois aux partenaires de l'entreprise de développer une forte valeur ajoutée sur le marché de la cybersécurité et aux entreprises de pouvoir travailler avec des prestataires de confiance, capables de gérer de bout en bout l'opérationnel en matière de cybersécurité.

CONSEILS POUR UNE UTILISATION APPROPRIEE DES DONNEES D'ENTREPRISE PAR LES SALARIES.

- Si possible, réduisez le nombre de personnes ayant accès aux données cruciales de l'entreprise, en réduisant la quantité de données accessibles à tous les employés. Les violations sont plus susceptibles de se produire dans les organisations où un trop grand nombre d'employés traite des informations confidentielles de valeur qui sont susceptibles d'être vendues ou utilisées d'une manière ou d'une autre.
- Mettez en place une politique d'accès aux ressources de l'entreprise, notamment aux boîtes aux lettres électroniques, aux dossiers partagés et aux documents en ligne. Maintenez-la à jour et supprimez tout accès si un employé quitte l'entreprise. Utilisez une passerelle sécurisée d'accès au cloud qui permet de gérer et de surveiller l'activité des employés dans les services cloud ainsi que d'appliquer les politiques de sécurité.
- Effectuez des sauvegardes régulières des données essentielles pour garantir la sécurité des informations de l'entreprise en cas d'urgence.
- Fournissez des directives claires sur l'utilisation des services et ressources externes. Les employés doivent connaître les outils qu'ils peuvent et ne peuvent pas utiliser, et pourquoi. Lors du passage à un nouveau logiciel pour le travail, une procédure d'approbation claire doit être mise en place avec le service informatique et les autres personnes responsables.
- Encouragez les employés à utiliser des mots de passe forts pour l'ensemble des services numériques dont ils se servent et à modifier régulièrement ces mots de passe.
- Rappelez régulièrement au personnel l'importance de respecter les règles de base de la cybersécurité en matière de gestion sécurisée des comptes et des mots de passe, de sécurité des messageries et de navigation sur Internet.
- Usez de services de cybersécurité dédiés qui offrent une visibilité sur les services cloud utilisés par les employés, comme Kaspersky Endpoint Security Cloud

4 – Le manque de maturité se fait aussi ressentir par une approche trop segmentée.

Dans le déroulé de ce rapport, nous avons pointé du doigt le fait que les outils de cybersécurité, les formations et les approches pratiques en termes de cybersécurité n'étaient pas toujours adaptés à la réalité du marché et des besoins. L'une des explications, c'est que la cybersécurité est encore trop perçue comme une contrainte, une discipline à part au sein des entreprises : 66% des répondants indiquent que les enjeux cyber ne sont absolument jamais abordés lors des réunions des comités de direction.



Pourtant, la grande majorité des entreprises indiquent que la question du numérique est importante, soit parce qu'elles sont déjà 100% digitalisées (57%), soit parce que la digitalisation est en cours, ce qui rend la question du numérique centrale dans leurs prises de décision stratégiques (26%), soit à minima un projet d'avenir avec des velléités de digitalisation dans les années à venir. Preuve en est que malheureusement, il reste encore un fort travail de sensibilisation pour positionner la question de la cybersécurité au cœur des questions liées au numérique dans les entreprises. Alors que la plupart des entreprises se posent la question de la sécurité informatique une fois qu'elles ont déjà été victimes d'attaques, nous recommandons plutôt une approche de sécurité « by design » dès la conception du projet de numérisation. Pourquoi ? Parce que comme nous l'avons mentionné plus haut dans ce rapport, les enjeux liés aux failles de sécurité en entreprise peuvent être dévastateurs. Un rapport récent réalisé dans le monde entier indique qu'en moyenne, un incident de sécurité pour les PME coûte une centaine de milliers d'euros et que ce genre d'incident est vite revenu sans une politique de cybersécurité proactive. Les volontés d'investissement confirment ce ressenti, car parmi les 20% d'entreprises qui ne prévoient pas d'investir dans la cybersécurité dans les prochaines années, beaucoup répondent qu'elles préfèrent se concentrer sur leur digitalisation. L'un n'allant pourtant pas sans l'autre.

Un travail de sensibilisation reste à mener au niveau du réseau de partenaires, pour plus de confiance au sein de l'écosystème.

Nous avons déjà identifié le problème lié au manque de ressources, de personnel et de compétences en matière de cybersécurité. Ainsi, alors même que les entreprises estiment ne pas avoir la possibilité d'instaurer une stratégie de cybersécurité efficace à cause d'un manque de personnel qualifié (54%), nous conseillons alors de faire appel à des prestataires de services managés, ou à des partenaires de confiance pour opérer la cybersécurité. Une démarche qui n'est pas toujours évidente alors que 47% des répondants indiquent ne pas savoir à qui faire appel en cas de cyberattaque. Choisir son partenaire et son prestataire de services, ou de solutions, de confiance semble aujourd'hui être une priorité. A la fois pour s'équiper d'outils en phase avec la stratégie de l'entreprise mais également pour être accompagnés par une notion de services qui permet d'être à même d'identifier les options à notre disposition en cas de problème de sécurité. Kaspersky a toujours positionné la confiance et la transparence comme deux valeurs centrales

dans son approche. Transparence dans la manière de traiter les données, dans ses mises à jour de sécurité, dans ses procédures. Confiance dans la création et l'entretien de son écosystème de partenaires, dans la sécurité et l'intégrité de ses solutions et dans sa réactivité. La notion de confiance est primordiale à l'heure où encore une minorité des entreprises estime que la notion de cybersécurité est « une arnaque » alors que 70% estiment qu'assurer la protection des données est une priorité pour les années à venir.

Redda Ben Gelloune, directeur général d'Aitek : *La confiance entre deux entreprises est définie comme la croyance mutuelle qu'elles sont dépendantes l'une de l'autre pour atteindre leurs objectifs communs. Le but d'une alliance est en effet d'obtenir des résultats qui sont supérieurs à ce qu'une relation purement transactionnelle donnerait, la confiance partagée permettant toujours de s'adapter au contexte si nécessaire. Il ne s'agit pas uniquement de savoir tenir ses promesses car certains évènements ne peuvent pas être planifiés en avance. Évidemment, la confiance n'implique pas une harmonie parfaite et mêmes les meilleurs partenaires ne peuvent pas être alignés en toutes circonstances. Toutefois, dans une relation de confiance, les différents acteurs posent des questions afin de mieux comprendre les évènements tout en cherchant des solutions constructives. La confiance crée de la bonne volonté, qui maintient la solidité des relations. Avoir cette confiance dans un partenariat renforce la volonté commune de construire sur le long terme et permet d'atteindre des résultats qu'une relation purement transactionnelle ne pourra jamais atteindre.*

Dans le secteur de l'économie numérique, et plus précisément dans celui de la cybersécurité, la notion de confiance est d'autant plus stratégique que non seulement il s'agit de bâtir dans la durée, mais aussi et surtout de protéger des actifs critiques. Il est ainsi extrêmement important pour les entreprises africaines de choisir des éditeurs qui font confiance aux partenaires locaux, capables de transférer les compétences et de les accompagner dans la montée en puissance de leurs équipes respectives. C'est exactement ce que font AITEK et Kaspersky depuis maintenant près de quinze ans, en travaillant avec les revendeurs du continent pour fournir les solutions les plus pointues afin de protéger les particuliers comme les entreprises des risques croissants d'attaque. A travers l'Authorized Training Center, ce sont également des milliers d'ingénieurs qui ont été formé ces dix dernières années afin de répondre aux besoins récurrents des petites comme des grandes entreprises.

Sur les deux dernières décennies, AITEK et Kaspersky n'ont cessé d'être aux côtés des partenaires du continent pour lutter contre la cybercriminalité et consolider cette confiance indispensable et réciproque. Kaspersky et son équipe ont toujours eu cette ferme volonté d'investir prioritairement avec AITEK en Afrique, par l'Afrique et pour l'Afrique. Cela s'est toujours démontré par des actes clairs visant à offrir des outils sur mesure prenant en compte les spécificités du marché Africain. En choisissant AITEK comme distributeur à valeur ajoutée sur la région à une époque où la majorité des éditeurs de l'industrie considérait le continent comme non prioritaire, Kaspersky a démontré avant tout le monde que son entreprise croyait fermement au développement de l'Afrique et de son expertise locale. Et depuis lors, avec la croissance au rendez-vous, AITEK et Kaspersky contribuent jours après jours au renforcement de la sécurité numérique des différents pays du continent »

Top 5 des menaces que les petites et moyennes entreprises doivent surveiller en 2023.

Les cybercriminels sont bien souvent opportunistes, à la recherche de données, d'argent et de facilité d'accès. Si les grandes entreprises ont souvent été la cible de cyberattaques ces dernières années, les petites et moyennes entreprises ne sont pas épargnées pour autant, car comme le démontrent les statistiques, plus de 60 % des PME ont subi des cyberattaques au cours de l'année 2022.

Les PME contribuent considérablement à l'économie mondiale : selon l'Organisation mondiale du commerce, elles représentent plus de 90 % de toutes les entreprises dans le monde. Les cyberattaques peuvent causer de nombreux dommages aux entreprises : fuite de données confidentielles, perte de capitaux et de parts de marché précieuses, etc. ; les cybercriminels ne manquent pas de moyens pour atteindre leurs objectifs. Les recenser est le moins que l'on puisse faire. Définir les risques auxquels les PME peuvent être exposées, et les moyens de s'en protéger, semble aujourd'hui une priorité.

Risque #1 : Les fuites de données causées par les employés

Les données d'une entreprise peuvent être divulguées de différentes manières, et dans certains cas, de manière involontaire.

Pendant la pandémie, de nombreux travailleurs à distance ont utilisé leurs ordinateurs professionnels dans le cadre de leurs loisirs, que ce soit pour jouer à des jeux en ligne, regarder des films ou utiliser des plateformes de cours. Cette nouvelle habitude est un facteur de risques pour les entreprises, d'autant plus que cette tendance est appelée à perdurer: en 2020, 46 % des employés n'avaient jamais travaillé à distance, tandis qu'aujourd'hui deux tiers d'entre eux déclarent ne pas souhaiter retourner au bureau, et le tiers restant se dit en faveur du travail hybride.

Le niveau de cybersécurité depuis l'adoption massive du télétravail s'est amélioré. Néanmoins, les ordinateurs professionnels utilisés à des fins de divertissement demeurent l'un des principaux moyens d'obtenir un accès initial au réseau d'une entreprise. En cherchant des sites pour télécharger le dernier épisode d'une série ou un film récemment sorti, les internautes peuvent rencontrer divers types de logiciels malveillants, notamment des chevaux de Troie, des logiciels espions, des portes dérobées, et des logiciels publicitaires. Selon les statistiques de Kaspersky, **35 % des utilisateurs qui ont été confrontés à des menaces par le biais de plateformes de streaming ont été affectés par des chevaux de Troie**. Si ces logiciels malveillants se retrouvent sur un ordinateur professionnel, les attaquants peuvent pénétrer dans le réseau de l'entreprise, rechercher et voler des informations sensibles.

D'autre part, il n'est pas rare de voir attribuer d'éventuelles fuites de données à d'anciens employés. Pourtant, selon une étude récente, seuls 40% des dirigeants de PME interrogés ont répondu être convaincus que leurs anciens employés n'ont pas accès aux données de l'entreprise stockées dans les services cloud, ou ne peuvent pas utiliser les comptes de l'entreprise. Il arrive que ces ex-collaborateurs ne se souviennent même pas avoir eu accès à telle ou telle ressource. Mais un contrôle de routine effectué par les responsables pourrait permettre de révéler que des personnes non autorisées ont effectivement accès à des informations confidentielles, une raison suffisante pour justifier une amende.

Et même si vous êtes absolument certain de vous être séparé en bons termes avec tout le monde, cela ne signifie pas que vous êtes sorti d'affaire. Qui peut garantir que vos anciens collaborateurs n'ont pas utilisé des mots de passe faibles, ou toujours identiques, pour accéder aux systèmes de l'entreprise, que des cyberattaquants pourraient trouver par force brute, ou découvrir dans une fuite sans rapport ? Tout accès à un système, qu'il s'agisse d'un environnement collaboratif, d'une messagerie professionnelle ou d'une machine virtuelle, augmente la surface d'attaque. Même une simple discussion entre collègues sur des sujets non professionnels peut être exploitée pour des attaques par ingénierie sociale.

Risque #2 : Les attaques DDoS

Les attaques par déni de service distribué tirent parti des limites de capacité spécifiques qui s'appliquent à toutes les ressources du réseau, comme l'infrastructure qui permet la mise en place du site web d'une entreprise. L'attaque DDoS envoie de multiples requêtes à la ressource web attaquée, dans le but de dépasser la capacité du site web à traiter toutes les requêtes et ainsi empêcher le site de fonctionner correctement.

Les cyberpirates recourent à différentes sources pour agir sur des organisations telles que les banques, les médias ou les détaillants, fréquemment victimes d'attaques DDoS. Récemment, des cybercriminels ont pris pour cible le site Takeaway.com (Lieferando.de), et exigé deux bitcoins (environ 11 000 dollars) pour mettre fin à l'afflux de trafic. A noter

que les attaques DDoS contre les sites de vente en ligne ont tendance à augmenter pendant les vacances, périodes où les clients sont plus actifs.

On observe également une tendance à la hausse du côté des entreprises de jeux vidéo. Les centres de données nord-américains de Final Fantasy 14 ont été attaqués début août. Les joueurs ont rencontré des problèmes de connexion, d'ouverture de session et de partage de données. Les jeux multi-joueurs de l'éditeur Blizzard (Call of Duty, World of Warcraft, Overwatch, Hearthstone et Diablo : Immortal) ont également fait l'objet de nouvelles attaques DDoS.

Il convient de souligner que de nombreuses attaques DDoS ne sont pas signalées, car les montants versés sont généralement peu élevés.

Risque #3 : La chaîne d'approvisionnement

Être attaqué par le biais d'une chaîne d'approvisionnement signifie généralement qu'un service ou un programme utilisé par une entreprise depuis longtemps est devenu malveillant. Il s'agit d'attaques menées par l'intermédiaire des vendeurs ou des fournisseurs de l'entreprise : il peut s'agir d'institutions financières, de partenaires logistiques, ou encore d'un service de livraison à domicile. Ces attaques peuvent varier en complexité et en puissance.

Par exemple, certains attaquants ont utilisé ExPetr (alias NotPetya) pour compromettre le système de mise à jour automatique d'un logiciel de comptabilité appelé M.E.Doc, le forçant à diffuser un ransomware à tous ses utilisateurs. En conséquence, ExPetr a causé des millions de pertes, en infectant aussi bien des grandes entreprises que des petites.

Prenons CCleaner, l'un des programmes de nettoyage de registre les plus populaires, utilisé aussi bien par des particuliers que par des administrateurs systèmes. Il est arrivé que des attaquants compromettent l'environnement de compilation du développeur du programme, le dotant alors de plusieurs versions d'une porte dérobée. Pendant un mois, ces versions compromises ont été distribuées à partir des sites Web officiels de la société, téléchargées 2,27 millions de fois, et au moins 1,65 million de copies du malware ont tenté de se connecter aux serveurs des criminels.

Parmi les événements récents ayant interpellés les experts, on peut citer l'incident DiceyF, qui a eu lieu en Asie du Sud-Est, prenant pour cibles un développeur et un opérateur de casino en ligne, et une plateforme de service client, attaqués sur un mode à la Ocean 11. On peut aussi penser à l'incident SmudgeX : une APT inconnue a compromis un serveur de distribution et remplacé un installateur légitime par un trojan, propageant ainsi le PlugX malveillant dans toute une nation d'Asie du Sud, en le distribuant à tous les employés fédéraux qui devaient télécharger et installer le nouvel outil requis. De toute évidence, le support informatique gérant le serveur de distribution et les développeurs ont été affectés.

Risque #4 : Les malwares

Les fichiers malveillants peuvent se cacher partout : si vous téléchargez des fichiers illégitimes, assurez-vous qu'ils ne puissent pas vous nuire. Alors que plus d'un quart des petites et moyennes entreprises optent pour des versions piratées ou sans licence des logiciels professionnels afin de réduire leurs coûts, il convient de mentionner que ces logiciels peuvent contenir des fichiers malveillants ou indésirables susceptibles de compromettre les systèmes de l'entreprise.

En outre, les dirigeants de PME doivent se méfier des brokers d'accès, car il est probable que ces groupes causent beaucoup de torts aux entreprises en 2023. Leurs clients, demandeurs d'accès illégaux, comprennent aussi bien des personnes adeptes de cryptojacking que des voleurs d'identifiant bancaires, des ransomwares, des voleurs de cookies et d'autres logiciels malveillants problématiques. On peut citer Emotet, un logiciel malveillant qui vole les informations d'identification bancaires de ses victimes et cible les organisations du monde entier ; mais aussi DeathStalker, surtout connu pour ses attaques contre des entités juridiques, financières et touristiques. Les principaux objectifs du groupe reposent sur le pillage d'informations confidentielles relatives à des litiges impliquant des personnalités et des actifs financiers importants, des renseignements commerciaux concurrentiels ainsi que des informations sur les fusions et acquisitions.

Risque #5 : L'ingénierie sociale

La suite Office 365 de Microsoft est de plus en plus utilisée et, sans surprise, ses utilisateurs sont de plus en plus ciblés par tentatives de phishing. Les fraudeurs ont recours à toutes sortes d'astuces pour inciter les utilisateurs professionnels à saisir leur mot de passe sur un site Web illégitime ressemblant à la page de connexion de Microsoft.

Les experts de Kaspersky ont mis au jour de nombreuses nouvelles façons dont les cybercriminels spécialisés en phishing tentent de tromper les dirigeants d'entreprises. Ces stratagèmes s'avèrent parfois très élaborés : certains imitent des services de prêt ou de livraison, en partageant un faux site Web ou envoient des e-mails contenant de faux documents comptables.

Certains attaquants se font passer pour des plates-formes en ligne légitimes afin de tirer profit de leurs victimes. Il peut même s'agir de services de transfert d'argent très populaires, tels que Wise Transfer.

Les chercheurs de Kaspersky ont aussi signalé un lien vers une page traduite à l'aide de Google Translate, utilisée pour contourner les mécanismes de cybersécurité. Les expéditeurs de l'e-mail prétendent que la pièce jointe est une sorte

de document de paiement disponible exclusivement pour le destinataire, qui doit être étudié pour une "réunion de présentation de contrat et de paiements ultérieurs." Le lien du bouton Ouvrir pointe vers un site traduit par Google Translate. Cependant, le lien mène à un faux site créé par les attaquants dans le but de voler de l'argent à leurs victimes.

Conclusion

Le paysage des cybermenaces est en constante évolution et de manière exponentielle, à l'image du développement des usages du numérique. Alors que la transformation digitale des entreprises et des administrations semble être une priorité d'aujourd'hui comme de demain pour s'inscrire dans une société en mouvement et interconnectée, il est nécessaire qu'elle soit envisagée avec une approche la plus résiliente possible. Qu'est-ce que cela signifie ? Que pour faire en sorte que le numérique apporte plus d'opportunités que de dangers, il est nécessaire de réfléchir à la valeur des données traitées par l'entreprise, à la valeur de son activité et aux dommages que pourraient provoquer une cyberattaque, ou une faille de sécurité. On l'a vu au fil du rapport, les principaux facteurs de risques identifiés par l'entreprise tournent autour de la perte de clients, de la fraude financière et de la perte de réputation. Lorsqu'on sait qu'un problème lié à l'informatique peut à la fois paralyser la capacité de production, faire fuiter des données sensibles de clientèle dans la nature, bloquer la capacité opérationnelle pendant un temps donné ou encore faire perdre un avantage stratégique vis-à-vis d'un concurrent, pour ne citer que ces risques, il semble primordial d'anticiper le risque et d'intégrer la question de la cybersécurité à la transformation numérique.

Mais finalement, qu'est-ce qu'une bonne stratégie cyber ? C'est comprendre son parc informatique et son périmètre et s'équiper avec des outils adaptés. Parfois, inutile de se suréquiper avec des technologies certes robustes, mais pas adaptées aux équipes et au quotidien de l'entreprise. C'est également savoir s'entourer de professionnels de qualité à travers un réseau de partenaires de confiance, auprès d'un éditeur réactif et capable d'offrir des services en adéquation avec son besoin. C'est comprendre ses « faiblesses » : manque de ressources, manque de moyens ? Est-ce que finalement un modèle de services sur abonnement ne serait pas plus pertinent pour la trésorerie de l'entreprise ainsi que pour pallier le un manque de compétences ? Une bonne stratégie cyber, c'est également intégrer de la gouvernance numérique au sein de l'entreprise. Quelles règles établir auprès des salariés ? Quelles formations d'hygiène numérique de base imposer à tous ? Quels outils utiliser, quelle approche en matière de travail à distance ?

Enfin, une bonne stratégie de cybersécurité, c'est aborder toutes les décisions stratégiques de l'entreprises en y intégrant le prisme de la sécurité. Faire rentrer la cybersécurité dans les prises de décision et dans les comités de direction. Cela permettra d'éviter d'agir, puis de remédier aux problèmes mais plutôt d'agir en toute conscience, de manière cyber-sécure. Chez Kaspersky, nous avons à cœur d'accompagner la montée en maturité des entreprises en Côte d'Ivoire sur les enjeux de cybersécurité en travaillant avec un écosystème local qualifié et de confiance, en proposant des solutions adaptées aux besoins des entreprises quelles que soient leurs tailles et en développant des offres de services telles que des formations allant des cours de base de bonne hygiène numérique aux sessions très qualifiées pour développer des compétences pointues quand on est déjà un professionnel de l'informatique. Les petites et moyennes entreprises produisent énormément de valeur et sont en contact avec des organisations et entreprises de plus grande taille, parfois hautement stratégiques. Pour ces raisons, elles sont également la cible de cybercriminels qui n'ont pas d'état d'âme, ils suivent l'argent et les opportunités. Pour ces raisons, il est temps de briser les idées reçues et de prendre conscience de sa valeur et donc, de la protéger. Chez Kaspersky, nous avons pour objectif d'aider tous nos clients à se protéger contre toutes les menaces, d'où qu'elles viennent et quel que soit leur objectif et cela passe aussi par de la sensibilisation.

A propos de Kaspersky

Kaspersky est une société internationale de cybersécurité et de protection de la vie privée numérique fondée en 1997. L'expertise de Kaspersky en matière de « Threat Intelligence » et sécurité informatique vient constamment enrichir la création de solutions et de services de sécurité pour protéger les entreprises, les infrastructures critiques, les autorités publiques et les particuliers à travers le monde. Le large portefeuille de solutions de sécurité de Kaspersky comprend la protection avancée des terminaux ainsi que des solutions et services de sécurité dédiés afin de lutter contre les menaces digitales sophistiquées et en constante évolution. Les technologies de Kaspersky aident plus de 400 millions d'utilisateurs et 240 000 entreprises à protéger ce qui compte le plus pour eux.

Contacts presse

Noémie Minster / Corporate Communications Manager
Noemie.minster@kaspersky.com

Agence 35° Ouest
Elodie Filopon / Inès Bousquet / Inès Ré
ef@35ouest.com / ib@35nord.com / ir@35ouest.com