HarfangLab

LA CYBER-RÉSILIENCE DES PME EUROPÉENNES DANS UN MONDE À RISQUES MULTIPLES.

Un rapport et une étude de HarfangLab, analysant les cyber-risques, les stratégies et la résilience des PME pour affronter les menaces actuelles et futures ainsi que leurs conséquences.

2024

LES PME FACE AUX CYBERMENACES : ANALYSE DE LEUR RÉSILIENCE, LEURS STRATÉGIES, ET DES RISQUES AUXQUELS ELLES SONT EXPOSÉES.

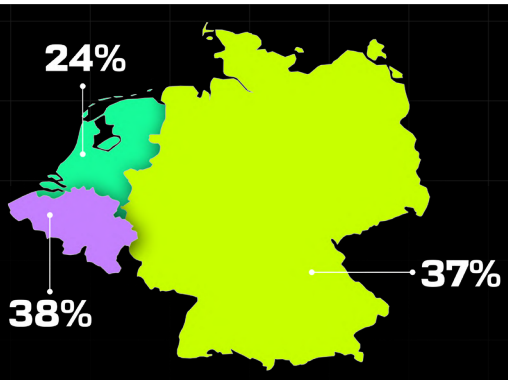
L'année 2024 marque un tournant crucial : avec l'intensification des tensions géopolitiques, les organisations européennes se retrouvent plus vulnérables que jamais face aux cybermenaces. Un contexte pesant qui fait émerger une interrogation : à quel point les PME européennes sont-elles prêtes à affronter ces nouveaux défis ?

Les PME représentent la majorité du tissu économique européen, et améliorer leur résilience face aux cybermenaces devient capital. En effet, bien qu'elles soient confrontées aux mêmes menaces que les grandes entreprises, elles disposent de ressources bien plus limitées pour se défendre.

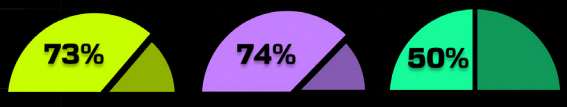
Nous avons cherché à comprendre la résilience des PME européennes face aux cybermenaces. Comment perçoivent-elles le niveau de risque ? Quelles actions mettent-elles en place pour se protéger ? Et quel est l'impact des nouvelles réglementations européennes sur leur conformité ? Pour répondre à ces questions, nous avons mené une enquête auprès de 750 responsables informatiques en France, en Allemagne, en Belgique et aux Pays-Bas.

QUELQUES-UNS DE NOS PRINCIPAUX RÉSULTATS :

38 % des répondants en Belgique perçoivent le niveau de menace comme extrême ou très sévère, comparé à 37 % en Allemagne et 24 % au Pays-Bas.

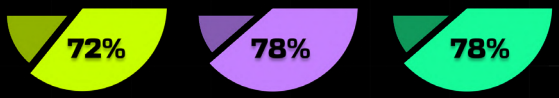


72 % des répondants en Europe estiment que les fournisseurs européens de cybersécurité sont mieux placés pour développer des produits adaptés aux besoins européens.



Les responsables de la sécurité informatique en Allemagne (73 %) et en Belgique (74 %) sont plus convaincus de l'avantage concurrentiel qu'offrent les réglementations de l'UE.

Les répondants de l'ensemble des régions interrogées ont appuyé l'idée de choisir des partenaires européens pour la cybersécurité.



Les décideurs informatiques sont convaincus que les partenaires européens en cybersécurité peuvent mieux répondre à leurs besoins.

INTRODUCTION:

Les organisations à l'échelle mondiale font face à un risque croissant de cybermenaces. La situation internationale actuelle – marquée par les conflits géopolitiques, l'instabilité économique et politique, ainsi que des taux d'inflation élevés – stimule la recrudescence de la criminalité, et incite les acteurs malveillants à lancer des attaques par ransomware à la fois lucratives et destructrices. Par ailleurs, nous n'avons jamais été aussi connectés. L'ère post-COVID a intensifié la connectivité au sein des organisations, augmentant ainsi les surfaces d'attaque et compliquant la surveillance des infrastructures informatiques. L'adoption de nouvelles technologies, telles que l'intelligence artificielle de nouvelle génération, nécessite également de nouveaux modèles de sécurisation. Bien que les entreprises déploient des technologies EDR pour protéger leurs endpoints, souvent considérés comme les portes d'entrée de leur infrastructure IT, les cybercriminels développent constamment de nouvelles tactiques pour exploiter les vulnérabilités. Il s'agit d'une course sans fin contre l'ingéniosité des attaquants.

Les organisations européennes sont particulièrement exposées aux cyberattaques. Le vieux continent, avec ses entreprises perçues comme prospères, constitue une cible de choix. Cette année, la tenue de nombreux événements sportifs, tels que les Jeux Olympiques de Paris et l'Euro 2024 en Allemagne, ont attiré une attention mondiale, créant ainsi des opportunités d'attaque pour des criminels organisés, des activistes et des États malveillants.

Ces événements ont mis à rude épreuve les défenses en cybersécurité européennes. Les organisateurs des Jeux Olympiques de Paris anticipaient un niveau de menace sans précédent, craignant des incidents de cybersécurité encore plus nombreux qu'aux Jeux de Tokyo en 2021.

La plupart des entreprises européennes sont déjà conscientes de la menace, mais elles doivent trouver un équilibre entre la nécessité d'une cybersécurité renforcée et la réalité des budgets de plus en plus serrés, de priorités concurrentes et des difficultés à attirer, recruter et retenir des talents en cybersécurité. Les décideurs informatiques et les responsables de la sécurité doivent également relever le défi de sensibiliser l'ensemble de l'organisation : comment faire comprendre à tous les employés qu'ils ont également un rôle à jouer dans la réduction des risques cyber ?

Dans ce contexte, il est nécessaire d'avoir une réglementation qui puisse fournir des directives, une orientation et des attentes en matière de cybersécurité. L'Union Européenne est à la pointe dans ce domaine, avec des législations telles que le Règlement général sur la protection des données (RGPD), le Digital Operational Resilience Act (DORA) et la Directive sur la sécurité des réseaux et de l'information 2 (NIS 2), qui imposent un niveau élevé et cohérent de cybersécurité à tous les États membres. Le cadre et les exigences de ces réglementations envoient un message fort aux entreprises sur la nécessité de prioriser la défense cyber et la protection des données. Mais que pensent les entreprises européennes de ce cadre réglementaire ?

Il est essentiel que ce cadre réglementaire ne devienne pas une contrainte supplémentaire pour les entreprises, ni qu'il aggrave le fossé déjà important entre les Responsables de la Sécurité des Systèmes d'Information (RSSI) et les autres dirigeants, ainsi que le reste de l'organisation. Les RSSI sont parfois – à tort – perçus comme des freins aux affaires ; il est important que cette perception change. Comment les RSSI peuvent-ils faire en sorte que la recherche de conformité réglementaire de leur entreprise ne se transforme pas en une simple formalité qui compromettrait la sécurité ?

Dans un monde numérique en perpétuelle évolution, la cybersécurité relève avant tout de la culture collective, où chacun a un rôle à jouer. Mais, alors que les budgets sont restreints et que les priorités doivent encore être fixées, quel est véritablement le niveau de résilience cyber à travers l'Europe ?

Dans ce contexte, et pour répondre à ces questions tout en apportant des conseils aux PME européennes, HarfangLab a confié à Sapio Research le soin d'interroger 750 responsables informatiques à travers une partie de l'Europe. L'objectif est de comprendre comment ces professionnels évaluent leur capacité à faire face à un environnement de menaces en constante évolution. Cette analyse nous aidera à identifier les enjeux spécifiques et à guider les acteurs de la sécurité informatique dans l'accompagnement des entreprises là où elles en ont le plus besoin.

Dans un monde où les cybermenaces évoluent sans cesse et où les investissements ralentissent, il est essentiel de comprendre précisément d'où viennent les risques et de les gérer de manière stratégique. C'est crucial pour préserver son autonomie, maintenir son positionnement économique et, à la fin, garantir la survie de l'organisation.

Dans ce rapport, nous dévoilons les priorités et attentes des PME, explorons les obstacles à une cybersécurité renforcée et cherchons à répondre à une question critique : quelle est réellement la cyber-résilience des PME européennes ?

NOTES MÉTHODOLOGIQUES :

Ce rapport se base sur une enquête réalisée en ligne par Sapio Research en avril 2024. 750 décideurs en matière de sécurité informatique en Belgique, France, Allemagne et aux Pays-Bas ont été interrogés sur leur perception et leur sensibilisation aux cybermenaces, ainsi que sur la préparation de leur organisation à gérer les cyber-risques.

Parmi les 750 répondants, 300 proviennent de France, 300 proviennent d'Allemagne, 100 de Belgique et 50 des Pays-Bas. La taille des entreprises varie entre 300 et 4 000 employés.

À PROPOS D'HARFANGLAB

HarfangLab est une entreprise de cybersécurité française spécialisée dans la protection du endpoint. Elle édite des technologies qui permettent d'anticiper et neutraliser les cyberattaques sur les ordinateurs et les serveurs, mais également de mieux connaître son infrastructure informatique pour mieux la sécuriser.

Premier EDR certifié par l'ANSSI, HarfangLab compte aujourd'hui de nombreux clients parmi lesquels des administrations, des entreprises et des organisations d'envergure internationale, évoluant dans des secteurs très sensibles.

Les solutions d'HarfangLab se distinguent par : l'ouverture, avec des solutions qui s'intègrent nativement à toutes les autres briques de sécurité ; par leur transparence, car les données collectées par les outils restent accessibles et par l'indépendance numérique qu'elles offrent, car ses clients sont libres de choisir leur mode d'hébergement : cloud public, SecNumCloud, ou leur propre infrastructure (on-premise ou cloud privé).

LA LÉGISLATION EUROPÉENNE SUR LA CYBERSÉCURITÉ OFFRE UN AVANTAGE CONCURRENTIEL AUX PME

Le cadre législatif européen en matière de données et de cybersécurité se complexifie. En plus du RGPD, la nouvelle loi européenne sur les données est entrée en vigueur cette année. Plus tard dans l'année, la directive NIS 2 prendra effet, imposant aux États membres de l'UE d'adopter et de faire respecter des règles strictes en cybersécurité. À partir de janvier 2025, les acteurs du secteur financier devront également se conformer à la norme DORA et mettre en place des mesures de cybersécurité adaptées.

On pourrait s'attendre à ce que les PME européennes voient ces nouvelles exigences de conformité en cybersécurité d'un mauvais œil. Pourtant, les résultats de notre étude montrent une toute autre réalité.

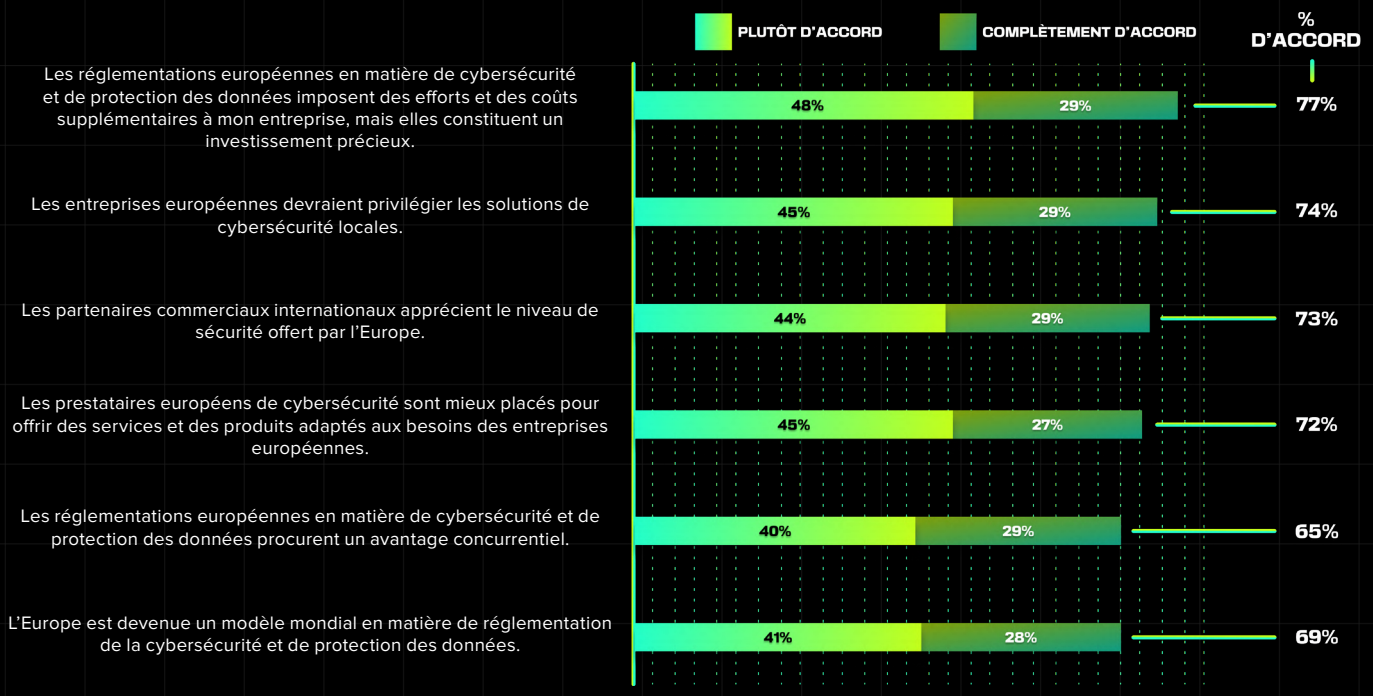
Se conformer aux différentes législations européennes en matière de cybersécurité et de protection des données impose un travail et des coûts supplémentaires pour les PME. Cependant, plus de trois quarts (77 %) des répondants à notre enquête estiment que cet investissement est finalement justifié.

Pourquoi ? Selon nos résultats, 73 % des décideurs en sécurité informatique reconnaissent que les partenaires commerciaux internationaux apprécient les niveaux de protection qu'offre ce cadre législatif européen. En conséquence, 70 % des répondants estiment que les réglementations européennes en cybersécurité et en protection des données offrent aux PME un avantage concurrentiel sur le marché mondial.

«C'est une excellente nouvelle que la majorité des PME voit les nouvelles réglementations comme une opportunité, car c'est vraiment le cas. Même si toutes les régulations ne sont pas encore en vigueur partout, les entreprises peuvent déjà se préparer à leur objectif principal : la sécurité. La cybersécurité ne se réduit pas à une simple formalité, mais nécessite une combinaison de personnes, de technologies et de gouvernance. Mon principal conseil pour les entreprises dans le cadre de la directive NIS2 est d'impliquer les dirigeants et les décideurs, en leur montrant l'importance de la cybersécurité et le rôle que chacun doit jouer. NIS 2 représente une véritable chance pour les RSSI de sensibiliser l'ensemble de l'organisation.»

Anouck Teiller, Chief Strategy Officer chez Harfanglab

77 % des responsables sondés reconnaissent que la réglementation européenne sur la cybersécurité et la protection des données entraîne plus de travail et de coûts pour leur organisation, mais jugent que cet investissement est nécessaire.



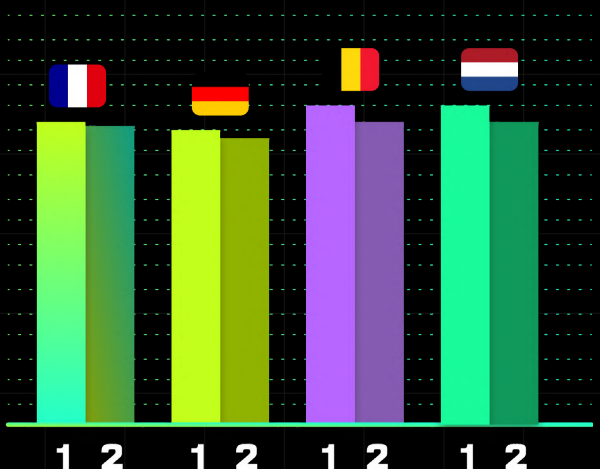
Il y a eu peu de divergences entre les régions sur ce point. Toutefois, les décideurs informatiques en Allemagne et en Belgique sont encore plus convaincus que les législations européennes en cybersécurité et en protection des données représentent un avantage concurrentiel (73 % et 74 %) que leurs homologues français (68 %). Les répondants néerlandais étaient un peu plus sceptiques, avec seulement 50 % partageant ce point de vue. Toutefois, les proportions de répondants dans chaque pays qui estiment que les efforts de conformité en valent le coût sont assez similaires (FR 77 %, ALL 76 %, BE 77 %, NL 82 %).

UNE PRÉFÉRENCE POUR LA CYBER-AUTONOMIE EUROPÉENNE

Notre étude montre également que les PME européennes préfèrent collaborer avec des fournisseurs et des solutions de cybersécurité européens.

En effet, 72 % des répondants estiment que les prestataires européens sont mieux à même de fournir des conseils et de développer des produits adaptés aux besoins spécifiques de l'Europe. Par ailleurs, près de trois quarts (74 %) soutiennent que les organisations européennes devraient privilégier l'utilisation de solutions locales de cybersécurité.

Une fois de plus, il y a eu peu de divergences entre les différents pays sondés pour ce rapport. Toutes les régions soutiennent l'idée de choisir des partenaires européens en cybersécurité (FR 74 %, ALL 72 %, BE 78 %, NL 78 %) et sont convaincues qu'ils peuvent mieux répondre à leurs besoins.



Pour quelle raison ? Tout d'abord, les fournisseurs européens, soumis aux mêmes exigences réglementaires que les PME, peuvent intégrer la conformité directement dans leurs produits et offrir des conseils adaptés aux nouvelles et anciennes législations. En revanche, les fournisseurs non européens, qui évoluent dans des conditions de marché et des cadres législatifs très différents, ne sont pas nécessairement en mesure de fournir un soutien aussi personnalisé.

Une autre explication pourrait être d'ordre géopolitique : en effet, 28 % des répondants ont identifié l'escalade des conflits géopolitiques comme le principal facteur augmentant les niveaux de menaces auxquels leur organisation est confrontée.

Les organisations européennes sont plus vulnérables que jamais aux cybermenaces. Dans un contexte mondial tendu, des événements internationaux comme les Jeux Olympiques, le Championnat d'Europe de football et les élections européennes ont créé des opportunités pour de nombreux acteurs malveillants – qu'il s'agisse de menaces persistantes avancées, de hacktivistes, de cybercriminels ou d'États rivaux. Ces acteurs exploitent ces occasions pour lancer des attaques visant à déstabiliser, désinformer, espionner ou perturber les organisations. Ces attaques peuvent également chercher à financer des activités illégales, freiner l'activité économique ou paralyser des infrastructures cruciales. En guise d'exemple, un rapport de nos chercheurs s'est particulièrement intéressé aux opérations de désinformation de Doppelgänger menées, en France et en Europe, au début de l'été 2024.

Face à ces tensions croissantes, les PME européennes semblent de plus en plus séduites par l'idée d'une architecture de défense en cybersécurité souveraine européenne. Elles comprennent qu'il est crucial de s'entourer de partenaires capables de saisir les spécificités locales des menaces et de les aider à se préparer à toutes les éventualités.

«Le contexte actuel de menaces, amplifié par les enjeux géopolitiques et économiques, met en évidence l'urgence de renforcer la résilience de l'Europe en cybersécurité. Cela implique non seulement de rehausser les standards de sécurité, mais aussi d'adopter une approche proactive et de définir clairement ses propres exigences en matière de confidentialité et de sécurité. Il est essentiel de contrôler l'accès à vos données et de déterminer leur usage. Avec l'extension des lois et régulations extraterritoriales, cette capacité devient indispensable. C'est la clé de notre autonomie et de notre indépendance. La bonne nouvelle, c'est qu'il ne s'agit pas simplement d'une question d'idéologie : des solutions concrètes et techniques sont disponibles pour répondre à ces besoins.»

Anouck Teiller, Chief Strategy Officer chez Harfanglab

UN APPEL À L'ACTION POUR L'EUROPE

Étant donné les liens entre les tensions géopolitiques et l'augmentation des cyberattaques, que doivent faire les PME européennes ?

Tout d'abord, il est essentiel de bien évaluer la valeur de leurs données et de mettre en place une stratégie de cybersécurité adaptée. Les PME constituent la majorité de l'économie européenne, et renforcer leur résilience face aux cybermenaces est crucial pour la stabilité à long terme du continent. Elles sont confrontées aux mêmes menaces que les grandes entreprises, mais disposent de ressources beaucoup plus limitées pour se défendre.

Aucune entreprise ne devrait réduire ses exigences en matière de sécurité en raison de sa taille. Il existe des solutions efficaces pour offrir à la fois des technologies de qualité, une expertise humaine et une attention particulière à la souveraineté des données. En optant pour une approche de cybersécurité sur-mesure, et qui s'appuie sur plusieurs technologies qui communiquent les unes avec les autres, les PME peuvent bénéficier d'une plus grande autonomie et indépendance, comparé à une dépendance vis-à-vis d'entreprises uniques, potentiellement localisées à plusieurs fuseaux horaires d'écart et foncièrement moins réactives en cas de problème. Choisir des partenaires de confiance capables de répondre au besoin de "simplicité" dans la gestion et dans le nombre d'interlocuteurs, et de fournir une offre complète d'outils de qualité et de management de la cybersécurité via une approche « cybersecurity as a service » est une stratégie pertinente, qui peut aussi permettre de pallier les pénuries de compétences internes. Un tel partenaire sera expert non seulement dans l'utilisation des technologies choisies, mais aussi dans les exigences spécifiques de son marché.

Au final, quels sont les critères de confiance ? Proximité, performance et transparence. Lorsque nous demandons aux décideurs de PME ce qu'ils recherchent le plus chez un fournisseur de sécurité informatique, les critères les plus importants qui ressortent sont : le rapport qualité-prix (44 %), l'innovation (51 %) et la performance (44 %), suivis de près par « la compréhension de mes besoins spécifiques ».

Docaposte, la filiale numérique du groupe La Poste, a lancé une offre de cybersécurité « clé en main » entièrement adaptée aux besoins des TPE, PME, ETI, collectivités locales et établissements de santé. Cette solution regroupe toutes les options de prévention, de protection et de réponse disponibles sur le marché, accessibles à travers un point de contact unique. Pour garantir cette accessibilité, Docaposte s'appuie sur son expertise en conseil et sur la collaboration avec un réseau de 12 entreprises partenaires françaises et européennes, sélectionnées pour leur excellence. HarfangLab est intégré dans cette offre en tant que fournisseur d'EDR.

Cette initiative met en évidence la nécessité d'un interlocuteur unique qui comprend les spécificités de l'écosystème et du marché, sans pour autant s'appuyer sur un fournisseur unique en matière de technologies. Elle répond également au défi de choisir des solutions fiables, européennes et de haute qualité, afin d'offrir aux PME européennes une alternative solide et accessible.

Investir dans les technologies numériques et savoir les exploiter efficacement, ou choisir le bon partenaire pour le faire, est essentiel. Ces technologies peuvent offrir un avantage concurrentiel important, permettant à certaines entreprises et secteurs de se démarquer. Cependant, si elles sont détournées par des acteurs malveillants, elles peuvent également servir à soumettre économiquement des régions entières.

Pour éviter cette situation, l'Europe doit adopter une approche proactive. Les PME du vieux continent comprennent qu'il est essentiel d'adopter une stratégie technologique qui assure leur autonomie et leur indépendance, soutenue par une gouvernance solide.

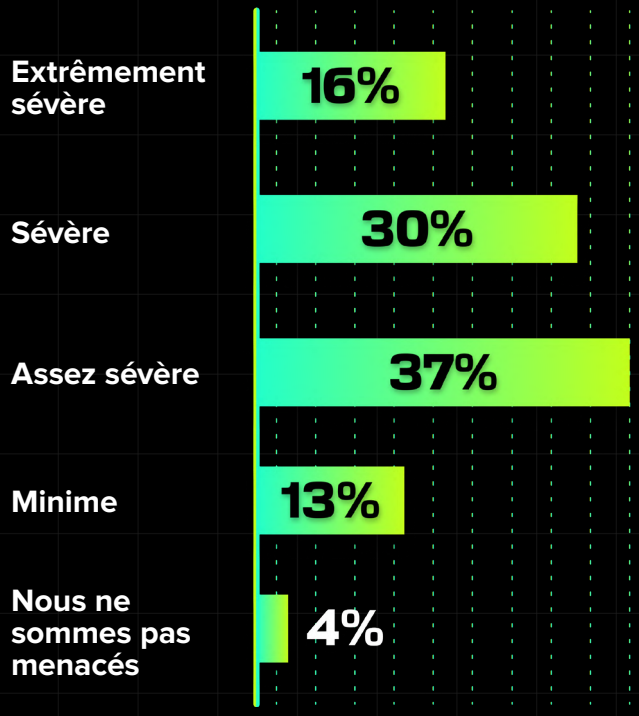
Dans la prochaine section de ce rapport, nous examinerons la préparation des PME face aux menaces actuelles et les risques qu'elles jugent les plus préoccupants.

CYBER-RISQUES : PERCEPTION, FACTEURS DE RISQUE ET PRÉPARATION

Avec l'évolution rapide des menaces, nous avons voulu comprendre comment les PME européennes perçoivent les dangers auxquels elles sont confrontées. Nous avons constaté que près de la moitié des répondants (47 %) jugent le niveau de menace actuel comme extrême ou très grave, tandis que seulement 3 % estiment ne faire face à aucun risque. Ces résultats démontrent que la plupart des décideurs en informatique ont une vision réaliste de la situation actuelle.

Il semble aussi que le degré de préoccupation des responsables de la sécurité influence leurs actions et investissements. Parmi ceux qui se considèrent entièrement préparés à un incident de cybersécurité, 28 % jugent le niveau de menace actuel comme « extrême », contre seulement 10 % parmi ceux qui estiment ne pas être bien préparés.

Près de la moitié d'entre eux (46 %) estiment que le niveau de menace auquel ils sont confrontés est extrêmement ou très élevé.



Comment les différentes régions perçoivent-elles les niveaux de menace ? Nous avons constaté que le niveau de menace est perçu comme extrême en France : 62 % des répondants estiment que la menace est extrême ou très grave, contre 38 % en Belgique, 37 % en Allemagne et moins d'un quart (24 %) aux Pays-Bas.

Par ailleurs, le secteur de la santé est le plus inquiet face aux cybermenaces, avec 70 % des répondants le considérant comme extrême ou très grave. Viennent ensuite les secteurs de la comptabilité et des finances (56 %), de la production industrielle et du commerce de gros/détail (43 % chacun), et enfin de l'éducation (37 %).

Nous avons également constaté que la perception du niveau de menace cyber augmente avec la taille de l'entreprise. Alors que seulement 40 % des répondants travaillant dans des organisations de 300 à 999 employés jugent la menace comme extrême ou très grave, plus de la moitié (52 %) des entreprises de plus de 2 000 employés partagent ce sentiment, soit une différence de 12 points de pourcentage.

À première vue, cela pourrait sembler logique : les grandes organisations sont plus visibles et perçues comme ayant davantage de données et de ressources financières, ce qui les rend plus attractives pour les cybercriminels. Pourtant, les cyberattaques touchent toutes les entreprises, quelle que soit leur taille. Les PME sont particulièrement vulnérables : en 2022, elles ont subi plus de 330 000 attaques, avec des conséquences pouvant aller jusqu'à la faillite. La leçon à en tirer : les petites entreprises doivent prendre la menace cyber au sérieux et déployer des stratégies d'anticipation.

L'ŒIL DE L'EXPERT : LES DIFFÉRENTS TYPES DE CYBER-RISQUES POUR UNE ORGANISATION

par Léna Jakubowicz, Ingénieur Avant-vente chez HarfangLab

Une crise cyber est un type de crise particulièrement complexe, car elle implique divers risques, chacun ayant ses propres conséquences. Comprendre ces risques permet d'élaborer un plan de gestion de crise efficace, en se concentrant sur les menaces les plus graves pour l'entreprise.

RISQUE FINANCIER : l'attaque de Colonial Pipeline en 2021. Colonial Pipeline a été ciblé par une attaque ransomware orchestrée par le groupe DarkSide, entraînant la fermeture temporaire de son réseau de pipelines et perturbant l'approvisionnement en carburant sur la côte Est des États-Unis pendant plusieurs jours. Cette attaque a coûté à l'entreprise plus de 4,4 millions de dollars de rançon, sans compter les pertes financières liées aux interruptions de la chaîne d'approvisionnement.

RISQUE RÉPUTATIONNEL : la fuite de données chez Facebook (2021).
En 2021, les données personnelles de plus de 530 millions d'utilisateurs de Facebook ont été compromises, comprenant des numéros de téléphone et des informations de profil. Cette violation a soulevé des interrogations sérieuses sur les mesures de protection des données de Facebook, ébranlant la confiance des utilisateurs et du public envers la plateforme.

RISQUE OPÉRATIONNEL : l'attaque par ransomware contre JBS (2021).
JBS, le plus grand fournisseur de viande au monde, a subi une attaque ransomware qui a forcé la fermeture de plusieurs de ses centres de production et interrompu ses opérations en Amérique du Nord et en Australie. Cette attaque a causé d'importantes perturbations dans la chaîne d'approvisionnement en viande, affectant la distribution.

RISQUE JURIDIQUE : la violation de données chez British Airways (2018).
En 2018, une violation de données chez British Airways a exposé les informations personnelles de 429 612 clients. En 2020, l'ICO britannique a infligé à la compagnie une amende de plusieurs millions de livres pour ses pratiques de sécurité insuffisantes. Les nouvelles régulations européennes augmentent également le risque de sanctions pour les entreprises ne respectant pas les normes de sécurité.

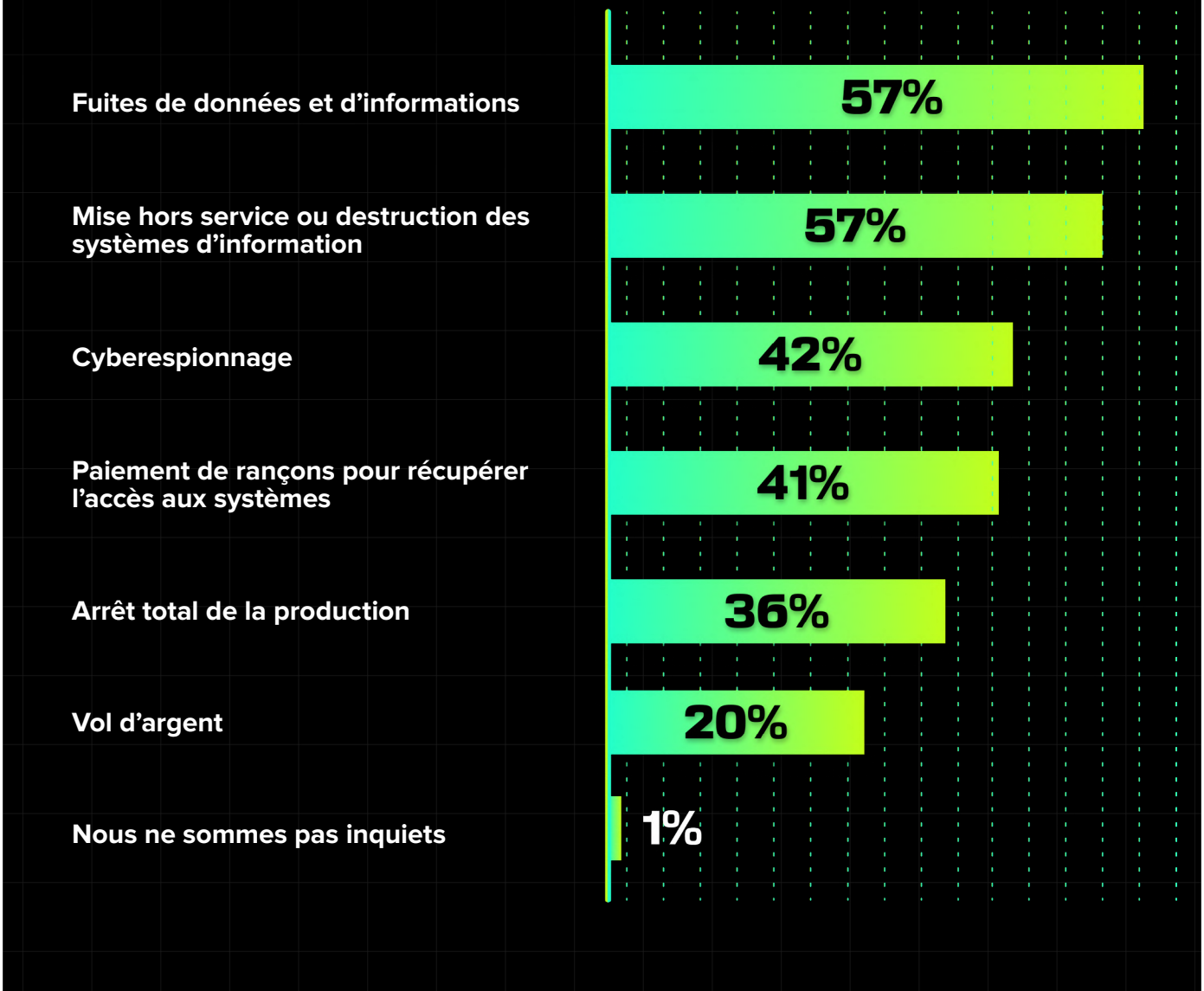
L'IMPACT D'UN CYBER-INCIDENT

Il n'est pas surprenant que presque tous les répondants à notre enquête (99 %) se préoccupent des conséquences d'un cyber-incident. Mais parmi les différents types de cyberattaques, lesquelles inquiètent le plus les décideurs informatiques ?

À première vue, le vol d'argent semble susciter le moins de préoccupations : seuls 20 % des répondants expriment cette crainte. Cette relative indifférence pourrait s'expliquer par les difficultés liées à ce type de vol, la présence possible d'une assurance couvrant les pertes, ou les contrôles financiers conçus pour prévenir ce genre de problème.

En revanche, 57 % des répondants sont particulièrement préoccupés par les fuites de données et d'informations. Une telle violation peut engendrer des dommages importants à la réputation de l'entreprise et entraîner de lourdes amendes, notamment en vertu du RGPD. De plus, plus de la moitié des répondants (51 %) craignent qu'un cyber-incident ne provoque l'effacement ou la destruction de leurs systèmes d'information.

99 % des responsables informatiques sont préoccupés par les impacts potentiels des cyberattaques. 57 % d'entre eux craignent particulièrement les fuites de données et d'informations, et 51 % s'inquiètent de la destruction des systèmes d'information.



L'ÉCONOMIE CONNECTÉE ET L'AGGRAVATION DES RISQUES CYBER

Nous avons désormais une bonne compréhension des préoccupations des PME face aux incidents de cybersécurité. Mais quels sont les principaux risques que les décideurs informatiques jugent susceptibles de mener à une cyberattaque réussie ?

Près de la moitié des répondants (56%) estiment que les vulnérabilités techniques représentent des risques majeurs. Cette inquiétude est encore plus marquée dans le secteur de l'éducation (61%) et dans les secteurs industriels et de l'énergie (64%).

Autre risque significatif : celui des employés cliquant sur des liens ou des fichiers malveillants (52%). Cela souligne l'importance de former et de sensibiliser régulièrement les employés aux cybermenaces au sein de l'organisation.

Près de la moitié des répondants (49%) craignent que les faiblesses dans leur supply chain ne représentent un risque majeur. Ce point est lié à une autre question de notre enquête concernant les développements qui augmentent les niveaux de menace.

En effet, 48% des répondants considèrent que l'économie connectée est la principale source de risques majeurs. Aujourd'hui, de nombreuses PME européennes reconnaissent la valeur du partage de données avec leurs partenaires et clients. La future loi européenne sur les données vise d'ailleurs à encourager cet échange entre entreprises, citoyens et secteur public. Cependant, cette économie de plus en plus interconnectée crée aussi plus de points vulnérables et de vecteurs d'attaque pour les cybercriminels.

Les responsables de la sécurité informatique devront donc élargir leur approche au-delà de leur propre infrastructure IT et intégrer leurs partenaires dans leurs stratégies de cybersécurité. Assurer la sécurité des chaînes de valeur devrait être une priorité essentielle pour chaque organisation.

D'autres facteurs de risque incluent la multiplication des endpoints et les pénuries de travailleurs qualifiés, chacun cité par 47% des répondants. La pénurie de talents est particulièrement préoccupante pour les répondants en Belgique (52%) et aux Pays-Bas (56%), et elle est la principale inquiétude dans le secteur du commerce de détail/gros (58%).

La montée de l'IA générative a également été mentionnée par 46% des répondants. C'est le facteur qui augmente le plus le niveau de menace pour le secteur de la santé (59%). Selon les dirigeants de PME européennes, l'IA pourrait entraîner des attaques plus sophistiquées (81% d'accord), mais elle pourrait également permettre une meilleure compréhension des menaces et contribuer à élaborer de meilleures stratégies de sécurité (85%), ainsi qu'à contrer les attaques renforcées par l'IA (82%).

«Le monde numérique connecte les gens et les économies de façon inédite, mais il offre aussi aux cyberattaquants de nouvelles opportunités pour cibler les entreprises. Le rythme rapide des avancées technologiques dépasse de loin l'évolution des compétences humaines et de la formation. Nous faisons face à une pénurie mondiale de talents. C'est pourquoi il est crucial que les outils et technologies de défense soutiennent les experts, en amplifiant leur efficacité plutôt qu'en creusant encore plus le fossé des compétences. Chaque technologie apporte son lot d'opportunités et de risques. Il est donc de notre responsabilité, dans le domaine de la cybersécurité, d'adopter les dernières innovations, de sensibiliser et de contribuer à l'amélioration des compétences et des niveaux de sécurité à l'échelle mondiale.»

Anouck Teiller, Chief Strategy Officer chez HarfangLab

QUELLE EST LA PRÉPARATION DES PME FACE AUX CYBER-RISQUES ?

Les décideurs informatiques ont une bonne compréhension du paysage des menaces, des conséquences des cyberattaques réussies et des facteurs qui aggravent les risques pour leur organisation. Mais quelle est réellement la préparation des PME européennes face à ces attaques ?

Actuellement, seulement 17 % des répondants se jugent « entièrement préparés » en matière de cybersécurité. Environ la moitié (50 %) se considèrent comme « bien préparés », 30 % comme « plutôt préparés », et 2 % admettent ne pas l'être.

Une proportion plus élevée de responsables informatiques se dit « entièrement préparée » dans les secteurs de l'informatique (32 %), de la santé (28 %) et de la finance (26 %). Cela paraît logique : les entreprises informatiques sont souvent plus avancées techniquement et mieux à même de comprendre les menaces, tandis que le secteur de la santé, ayant exprimé des préoccupations majeures sur les niveaux de cybermenaces, a probablement renforcé ses mesures de sécurité. De même, le secteur financier a dû se conformer à la réglementation DORA de l'UE, entrée en vigueur en janvier 2023 et applicable dès janvier 2025.

Les entreprises opérant à l'international se disent également plus souvent « entièrement préparées » que celles qui se limitent à un périmètre national (19 % contre 15 %).

Mais à quoi ressemblent ces préparations ? Et que peuvent faire les 83 % de répondants qui ne se sentent pas « entièrement préparés » pour renforcer leur résilience face aux cybermenaces ? Nous examinerons ces questions dans la dernière section de ce rapport.

— **ANTICIPER** : Pour maîtriser les risques, il est essentiel de bien connaître les systèmes d'information, les actifs critiques, les données, ainsi que les menaces et le contexte. En cas d'incident de cybersécurité, il faut aussi pouvoir mettre en place rapidement une cellule de crise pour gérer les problèmes techniques et de communication.

— **DÉTECTER** : Pour une détection efficace, il est important d'avoir les outils et les ressources appropriés. En pratique, cela signifie que le système d'information doit être protégé par des solutions adaptées et performantes, installées et gérées par des experts, qu'ils soient internes à l'entreprise ou partenaires externes.

— **ANALYSER** : Une fois qu'un outil a détecté un événement de sécurité, les experts doivent évaluer sa gravité et le documenter pour déterminer les actions à entreprendre. Cette étape vise également à comprendre la menace et les objectifs de l'attaquant afin de limiter la propagation immédiate et future de l'incident.

— **RÉPONDRE** : Après avoir évalué la situation, les experts peuvent, en fonction du contexte, prendre des mesures telles que bloquer la menace, arrêter les processus, isoler les endpoints ou mettre les fichiers en quarantaine, dans le but de récupérer le système ou les données. En plus de ces aspects techniques, la phase de réponse peut également inclure des actions de communication, tant en interne qu'en externe.

— **FAIRE LE BILAN** : L'analyse post-incident offre l'occasion de tirer des leçons précieuses de l'incident. Elle permet de renforcer la sécurité du système d'information et d'améliorer la sensibilisation des utilisateurs pour mieux anticiper et se préparer à de futures attaques.

AGIR POUR LA CYBER-RÉSILIENCE

La cyber-résilience est la capacité d'une organisation à maintenir sa mission et son intégrité face aux cyberattaques et autres événements perturbateurs. Elle dépasse les mesures de cybersécurité traditionnelles telles que la prévention et la défense pour inclure la préparation, la détection, la réponse et le rétablissement.

La cyber-résilience ne se contente pas de protéger l'organisation contre les menaces, mais elle implique également la capacité de détecter et d'atténuer rapidement ces menaces, de s'adapter aux circonstances changeantes et de continuer à fonctionner sans interruption. Pour atteindre cet objectif, il est essentiel de combiner des solutions techniques appropriées, des processus robustes, une formation continue des employés et une approche proactive.

Ces éléments permettent à une organisation de faire face efficacement aux incidents de cybersécurité et de se rétablir rapidement.

Dans ce contexte, quelle est la résilience des PME européennes face à une cyberattaque ? La majorité des PME (81 %) dispose d'un plan de gestion de crise en cybersécurité, et 80 % ont une confiance totale ou élevée en ce plan. Cependant, moins d'un tiers se considèrent comme « excellents » dans la prévention ou la détection (27 % chacun), la réponse (28 %) ou le rétablissement après (26 %) des incidents de cybersécurité.

La confiance dans ces compétences diffère selon les pays, mais en général, les Français jugent leurs capacités en matière de gestion des incidents de cybersécurité plus élevées que celles de leurs voisins. En effet, trois quarts des répondants en France (75 %) estiment leurs aptitudes à prévenir et détecter les menaces cyber comme excellentes ou plutôt bonnes.

En matière de budget consacré à la cyberdéfense, plus de la moitié (57 %) des PME européennes indiquent qu'elles augmenteront leurs dépenses au cours de l'année, contre seulement 17 % qui prévoient de les réduire.

De même, les pays où le niveau de menace cyber est considéré comme plus élevé, allouent davantage de ressources à la cybersécurité : en France, 58 % des entreprises envisagent d'augmenter leur budget en 2024, comparé à 44 % aux Pays-Bas.

Quels sont les domaines prioritaires pour ces budgets ? Plus de la moitié (52 %) prévoient d'investir dans des formations régulières de sensibilisation pour leurs employés, 50 % envisagent de renforcer la sécurité de leurs systèmes et applications basés sur le cloud, et 49 % comptent effectuer des audits réguliers.

Parmi les 17 % de dirigeants de PME qui ont pleinement confiance en leurs systèmes de défense, une proportion nettement plus élevée prévoit d'investir davantage dans l'établissement d'une culture, d'une structure et de processus de cybersécurité (53 % contre 39 % parmi les moins confiants) et dans la sécurisation de leur supply chain, y compris l'éducation de leurs partenaires (49 % contre 40 %). Presque tous les dirigeants confiants (93 %) disposent également d'un plan de défense en cybersécurité ; seuls 65 % des moins confiants en ont un.

Cependant, malgré ces budgets en augmentation, plus d'un tiers (35 %) des répondants estiment que leur budget de cybersécurité ne reflète pas adéquatement le niveau de menace auquel ils sont confrontés. Ce pourcentage augmente à 46 % chez les répondants du secteur de la santé et à 58 % dans les secteurs de l'automobile et de l'aviation.

La confiance dans les compétences varie d'un pays à l'autre, même si, dans l'ensemble, les Français jugent leurs compétences en matière de cybersécurité plus élevées que les pays voisins.

Prévention	**69%**	**75%**	**69%**	**72%**
Détection	**65%**	**75%**	**73%**	**66%**
Réponse	**68%**	**74%**	**72%**	**70%**
Rétablissement	**74%**	**72%**	**71%**	**68%**

Classement le plus élevé

«On croit souvent qu'une stratégie de cybersécurité doit être coûteuse pour être efficace, et que plus on multiplie les couches de protection, mieux on est protégé. Pourtant, ce n'est pas forcément vrai. En vous concentrant sur les menaces les plus critiques pour votre entreprise et en établissant une base solide (protection des endpoints, sensibilisation, surveillance informatique, etc.), vous pourrez prévenir la plupart des cybermenaces. Par ailleurs, il existe de plus en plus d'offres complètes de cybersécurité disponibles sur le marché via un partenaire de confiance unique, comme Docaposte en France.»

Anouck Teiller, Chief Strategy Officer chez Harfanglab

CONSEILS POUR GÉRER UNE CYBERCRISE

Les PME peuvent grandement bénéficier de la collaboration avec un leader européen en cybersécurité, qui peut les aider à gérer une crise cyber. Adopter une approche de gestion basée sur les risques peut s'avérer judicieux pour les organisations, car cette approche renforce leur résilience, améliore leur sécurité globale et leur permet de naviguer efficacement dans le paysage complexe de la cybersécurité. Parmi les avantages de cette approche, on trouve :

1 **UNE APPROCHE PROACTIVE** : La gestion basée sur les risques permet aux organisations d'anticiper et de traiter les cyber-risques avant qu'ils ne deviennent des crises.

2 **UNE OPTIMISATION DES RESSOURCES** : En priorisant les risques en fonction de leur impact potentiel, les organisations peuvent allouer leurs ressources plus efficacement, en se concentrant d'abord sur les domaines les plus critiques.

3 **RÉSILIENCE**: La gestion basée sur les risques renforce la résilience des organisations en leur permettant d'anticiper et de réduire les menaces cyber, diminuant ainsi la probabilité et l'impact des perturbations sur leurs opérations.

4 **AMÉLIORATION CONTINUE** : En instaurant une culture d'amélioration continue, les organisations peuvent évaluer et adapter régulièrement leurs mesures de cybersécurité pour répondre aux menaces en constante évolution et aux besoins changeants de l'entreprise.

> **«Il existe plusieurs façons de renforcer la cyber-résilience, dont l'une est la gestion basée sur les risques. Cela revient à accepter qu'une cybermenace est probable, et à prendre des mesures pour rebondir rapidement. Cette approche repose sur une compréhension approfondie de votre organisation, de votre infrastructure informatique et du paysage des menaces, en concentrant vos efforts sur la réduction ou la prévention des risques les plus dommageables. Elle permet d'économiser des ressources et d'aider les analystes à se focaliser sur l'essentiel. La stratégie TDIR (Détection des Menaces, Investigation et Réponse) est une méthode efficace pour gérer la cybersécurité basée sur les risques.»**
>
> Anouck Teiller, Chief Strategy Officer chez Harfanglab

Les organisations ne peuvent plus se permettre de rester dans la réaction pour protéger leurs précieux actifs. En collaborant avec des partenaires en cybersécurité qui recherchent et analysent activement les nouvelles menaces émergentes, elles peuvent se préparer à se défendre efficacement et de manière optimale.

CONCLUSION

D’après notre étude, il est clair que les organisations tirent les meilleurs bénéfices en collaborant avec des acteurs qui comprennent les enjeux et le contexte culturel et réglementaire européen.

Plutôt que de dépendre de fournisseurs externes, les PME européennes souhaitent accroitre leur autonomie en matière de cybersécurité. Elles veulent pouvoir déployer des outils et des solutions au sein de leur propre infrastructure, ainsi que via le cloud. Ces technologies doivent être une aide et non un obstacle. De plus, les décideurs informatiques doivent pouvoir créer leur propre environnement de confiance et décider qui peut accéder aux données stratégiques de l’organisation.

Enfin, nous savons qu’une cybersécurité solide repose sur une technologie de pointe associée à des compétences humaines, mais notre étude souligne également l’importance d’un troisième pilier : la législation. Les réglementations européennes en matière de cybersécurité et de protection des données offrent aux entreprises un avantage concurrentiel en rassurant clients et partenaires sur la sécurité de leurs données.

La puissance réside dans l’information. Les PME européennes doivent comprendre quels types de menaces les ciblent le plus, et où se situent leurs vulnérabilités. Il est donc essentiel de collaborer avec des champions européens de la sécurité, capables de fournir des renseignements spécifiques aux préoccupations du continent, ce que les partenaires extérieurs ne peuvent pas toujours garantir.

APPENDIX

LA CYBER-RÉSILIENCE EN 7 POINTS-CLÉS

Aussi décevant que cela puisse paraître, anticiper toutes les cybermenaces et incidents potentiels est tout simplement impossible. Chaque organisation doit accepter que la menace est constante et fait partie intégrante de la vie numérique. C'est pourquoi la cyber-résilience est essentielle. Il est crucial de se concentrer sur la capacité de l'organisation à résister, répondre et se rétablir après des perturbations tout en maintenant ses fonctions et services critiques.

Dans un environnement cyber en constante évolution, renforcer la cyber-résilience aidera les organisations et leurs équipes de sécurité à naviguer et s'adapter plus efficacement aux menaces dynamiques. Nous pensons qu'il y a sept points clés à considérer.

1. PRÉVENTION ET PROTECTION

Renforcer la protection de votre infrastructure est essentiel pour réduire les risques d'intrusion, d'espionnage, de vol de données ou de demande de rançon. Pour cela, il est important de mettre en place des outils de prévention et de protection contre les cybermenaces, tels que l'EDR, les antivirus de nouvelle génération, les outils de surveillance informatique et les pare-feu. Adoptez également des mesures comme l'authentification multi-facteur (MFA) et une approche zéro confiance.

De plus, il est important de maintenir à jour tous vos logiciels, applications et systèmes d'exploitation afin d'éviter les vulnérabilités.

Toutes ces actions de prévention et de protection doivent également être appliquées par vos fournisseurs et prestataires tiers : assurez-vous qu'ils respectent les meilleures pratiques et les règles de sécurité, afin qu'ils ne représentent pas un point d'entrée dans votre système d'information.

Pour pouvoir vous rétablir le plus rapidement possible, vous devez avoir une connaissance parfaite de votre système d'information et segmenter correctement votre parc informatique en fonction de l'importance de vos actifs. La segmentation permettra de limiter l'impact d'une attaque, car les intrus ne pourront pas se déplacer latéralement ; et la cartographie du système d'information facilitera l'identification de l'origine et de la propagation de l'incident, ainsi que l'isolation des parties concernées si nécessaire.

2. DÉTECTION ET RÉPONSE

Comme mentionné précédemment, investir dans des ressources et des technologies à jour est essentiel pour protéger vos actifs informatiques contre des menaces en constante évolution. Vous pourrez ainsi détecter et répondre rapidement aux incidents de cybersécurité. Cela implique l'utilisation d'outils de surveillance et d'analyse ainsi que des équipes de réponse aux incidents (internes ou externes) pour enquêter et atténuer les menaces rapidement.

Il est important de noter que les outils de détection et de réponse sont majeurs et qu'ils sont encore plus efficaces lorsqu'ils sont déployés dans le cadre d'une approche globale de la cybersécurité. Il est donc dans votre intérêt de vous appuyer sur des solutions ouvertes et compatibles avec les API, permettant de collecter, d'accéder et de corréler les données relatives aux événements de sécurité. Il est également capital de se tourner vers des solutions capables de détecter à la fois les menaces connues et inconnues – grâce à l'IA – et de les bloquer automatiquement.

3. RÉTABLISSEMENT ET CONTINUITÉ

Planifiez et mettez en œuvre des stratégies pour récupérer après les cyber-incidents et maintenir la continuité de vos activités. Cela inclut des processus et des plans solides de sauvegarde et de récupération pour restaurer les systèmes et les données critiques, stockés dans un environnement isolé et sécurisé.

Toutefois, il ne suffit pas de planifier : il est également crucial de tester régulièrement ces plans. Cela permet d'identifier les services et outils essentiels à redémarrer en priorité en cas d'incident, ainsi que ceux qui pourraient être désactivés. Il est important d'anticiper les interruptions potentielles et de comprendre comment elles pourraient affecter votre capacité à communiquer et à gérer efficacement une crise.

Cette approche est indispensable pour remettre en marche votre système d'information et vos activités le plus rapidement possible en cas d'attaque. Elle est facilitée par les fonctionnalités de surveillance informatique et la capacité d'outils comme les EDR à collecter et agréger les données relatives à l'activité de votre parc informatique.

4. ADAPTABILITÉ ET APPRENTISSAGE

Les organisations doivent se préparer aux incidents, en tirer des leçons, mettre à jour leurs politiques et procédures, et renforcer leur posture de sécurité au fil du temps. Autrement dit, elles doivent évaluer et adapter continuellement leurs mesures de cybersécurité en fonction de l'évolution des menaces, ce qui nécessite une veille constante du contexte et des nouvelles menaces.

Pour y parvenir, il est important de disposer d'un plan de réponse aux incidents prêt à être déployé en cas d'attaque. Des exercices réguliers permettront de vérifier l'efficacité de vos processus et de s'assurer que tous les membres impliqués dans la gestion de crise connaissent leurs rôles et responsabilités. Cette agilité est centrale pour réagir efficacement à une attaque, prendre les bonnes décisions au bon moment pour une récupération rapide, et tirer des leçons de l'incident afin de renforcer la protection.

5. COLLABORATION ET COMMUNICATION

Établir des canaux de communication et des mécanismes de collaboration efficaces, tant en interne qu'en externe, est majeur pour la cyber-résilience. Cela implique une coordination efficace entre les différents départements de l'organisation, ainsi que le partage de renseignements sur les menaces et des meilleures pratiques avec les partenaires externes et les pairs de l'industrie.

Par ailleurs, en brisant les silos internes pour faciliter la communication entre les équipes de sécurité et les autres départements, une réponse plus rapide et plus efficace en cas d'incident de sécurité est garantie. En matière de communication externe, la collaboration et la transparence sont également essentielles pour assurer une réponse rapide, cohérente et transparente vis-à-vis des clients, de la presse, des investisseurs et des autres parties prenantes en cas d'attaque ou d'incident de sécurité. Chaque intervenant interne doit être en mesure d'identifier les ressources ou les personnes à contacter, les circuits de validation que l'information doit suivre, ainsi que les canaux par lesquels elle doit être diffusée.

6. FORMATION ET SENSIBILISATION DES EMPLOYÉS

Vos collaborateurs jouent un rôle majeur dans la prévention des attaques d'ingénierie sociale (social engineering) et le maintien de la cyber-résilience. C'est pourquoi il est essentiel de former les employés aux meilleures pratiques en matière de cybersécurité et de promouvoir une culture de sécurité au sein de l'organisation. En effet, l'erreur humaine reste la principale cause des violations de données, avec 31 % des entreprises identifiant cette cause, selon une étude de Thales en 2023.

Pour maintenir un haut niveau de vigilance, planifiez régulièrement des formations sur la cybersécurité et organisez des simulations de phishing. La cybersécurité est un domaine riche et fascinant, applicable à une multitude de secteurs, de la technologie à la géopolitique. Vous trouverez sans doute des approches qui parleront à vos équipes, quelles que soient leurs compétences et leurs centres d'intérêt.

7. GOUVERNANCE ET LEADERSHIP

Mettre en place des structures de gouvernance solides, des politiques claires et un engagement fort de la direction en matière de cybersécurité nécessite des rôles et responsabilités bien définis, des processus de gestion des risques efficaces et le soutien sans faille de la direction. Il est essentiel que la culture de la cybersécurité émane du sommet de la hiérarchie. Les décideurs doivent montrer qu'ils prennent ce sujet au sérieux. Qu'ils gèrent cette responsabilité eux-mêmes ou la délèguent, la cybersécurité doit être une priorité constante, pas seulement en temps de crise, mais de façon continue, en impliquant toutes les équipes.

Le respect des obligations légales et réglementaires est également crucial pour garantir un niveau de sécurité optimal (conformité NIS2, RGPD, etc.). Pour cela, il est important de réaliser régulièrement des audits de sécurité afin d'évaluer les risques et d'identifier les vulnérabilités potentielles, permettant ainsi de prioriser les actions à mener par nos équipes techniques et de sécurité.

Enfin, comprendre les menaces auxquelles l'organisation est confrontée est indispensable pour savoir quels risques doivent être couverts et pour pouvoir répondre avec les ressources adéquates en cas de besoin.

harfanglab.io Inside the Lab @harfanglab HarfangLab

CONTACT

contact@harfanglab.fr