Tribune : les ressorts économiques des solutions EDR et MDR

Par Oliver Schonschek, analyste de la sécurité et influenceur chez IDG

Analyse ROSI
Comment mesurer le coût de la cybersécurité ?

kaspersky BRING ON THE FUTURE

Tribune : les ressorts économiques des solutions EDR et MDR
Pourquoi est-il intéressant d'investir dans des solutions de détection et de réponse

Par Oliver Schonschek, analyste de la sécurité et influenceur chez IDG

En quoi les investissements dans la cybersécurité sont-ils payants ? Les responsables de la sécurité informatique doivent régulièrement répondre à cette question pour justifier leurs dépenses ou pour motiver, preuve à l'appui, leur prochaine demande de budget.

Mais mesurer l'importance de la cybersécurité n'est pas une mince affaire, car il ne s'agit pas d'un placement lucratif, mais d'un investissement qui contribue à éviter des pertes.

C'est d'autant plus compliqué que la mise en place de garde-fous ne s'accompagne pas d'une garantie de résultat. Des cyberattaques peuvent survenir même lorsque des mesures de sécurité informatique robustes ont été prises. D'après une étude récente de l'entreprise de cybersécurité Kaspersky, 38 % des grandes entreprises ont été victimes d'au moins une cyberattaque ciblée en 2020.

Et ce, malgré le fait que plus de la moitié d'entre elles (52 %) avaient un service de sécurité informatique dédié et que 20 % disposaient d'un centre opérationnel de sécurité (SOC) interne chargé de surveiller en permanence les incidents de sécurité et d'y répondre.

Pour certaines entreprises, cela soulève non seulement la question du montant du budget à investir dans la cybersécurité, mais aussi de l'efficacité d'un tel investissement.

« De nombreux clients investissent des millions dans une protection informatique de base, mais négligent de tirer le meilleur profit de cet investissement », explique Uwe Kissmann, Managing Director des services de cyberdéfense d'Accenture dans la région EMEA. « En bref, il s'agit simplement de trouver le bon équilibre sur le plan économique : comment m'assurer que les investissements déjà réalisés en matière de cybersécurité puissent exprimer tout leur potentiel, et comment veiller à tirer le meilleur parti de nos investissements futurs ? »

Dans cette optique, l'expert en sécurité et ancien responsable de la sécurité informatique Kissmann a quelques conseils à donner :

« Il est crucial d'investir non seulement dans la protection statique, mais aussi de fournir des ressources, des processus et des technologies qui permettent de détecter sans problème les passerelles envisageables. Cela doit aller de pair avec la mise au point d'une stratégie de réponse claire en cas d'attaque. Prendre des mesures de protection tant statiques que dynamiques en proportions égales permet de maximiser les bénéfices des investissements dans la cybersécurité. »

Détection et réponse : la protection doit devenir davantage proactive

Le fait qu'une entreprise ne soit pas parvenue à déjouer une cyberattaque ne signifie pas que ses investissements dans la cybersécurité aient été inutiles. Il s'agit là d'une vision erronée de la sécurité.

Il convient de garder à l'esprit que toute entreprise risque un jour d'être victime d'une attaque réussie. La cybersécurité ne doit donc pas se limiter à la protection contre les attaques, mais aussi inclure des mesures de détection et de défense.

La cybersécurité a pour objectif de détecter les cyberattaques réussies aussi rapidement que possible et de limiter leurs conséquences potentielles.

D'après l'enquête internationale de Kaspersky « Rapport économique sur la sécurité informatique en 2021 : gestion d'une complexité informatique qui tend à croître »[1], le coût moyen d'une violation de données est actuellement de 106 577 $ pour les petites et moyennes entreprises.

Les grandes entreprises doivent s'attendre à des pertes encore plus élevées. Par exemple, les entreprises interrogées au cours de l'étude ont déclaré qu'un incident de sécurité informatique leur coûtait en moyenne 1,06 million de dollars à l'échelle de l'entreprise.

Toutefois, il y a quelques bonnes nouvelles. L'an passé, l'impact était important même lorsque les incidents de sécurité étaient découverts rapidement. Ainsi, lorsqu'un incident de sécurité informatique passait inaperçu pendant une semaine, les coûts augmentaient considérablement.

L'Enquête mondiale de Kaspersky sur les risques liés à la sécurité informatique pour les entreprises (ITSRS) est une enquête internationale menée auprès de décideurs d'entreprises du secteur informatique. Elle a été réalisée aux mois de mai et juin 2021 à partir d'un total de 4 303 entretiens avec des entreprises de plus de 50 salariés. Kaspersky mène cette enquête une fois par an.

« Notre étude montre une inversion bienvenue de cette tendance : les entreprises ont amélioré et accéléré leurs capacités de détection des incidents de cybersécurité. Bien que les coûts ultérieurs restent d'un montant colossal en cas de dommages, ils peuvent être réduits grâce à une détection précoce et améliorée. Vous pouvez pour cela faire appel à des experts en sécurité informatique extérieurs et utiliser des solutions appropriées », explique Bertrand Trastour, GM chez Kaspersky France et Afrique du Nord, de l'Ouest et du Centre.

Pour détecter rapidement un incident et se défendre de manière à limiter son impact financier, les entreprises doivent veiller à disposer de capacités de détection et de réponse robustes. Cela vaut tout particulièrement au niveau des terminaux, car ils sont la cible de la plupart des cyberattaques.

Les EDR (Endpoint Detection and Response) sont des solutions de sécurité des terminaux qui collectent, agrègent, stockent et analysent des données système et des données d'utilisation depuis les terminaux surveillés. L'analyse des terminaux fournit des indications sur les événements suspects et avertit de possibles incidents de sécurité informatique, tels qu'une tentative de piratage d'un terminal.

Contrairement aux technologies classiques de protection contre les programmes malveillants, un EDR détecte les potentielles attaques non pas à partir des signatures, mais en déterminant le comportement attendu de chaque terminal et en surveillant l'éventuelle apparition d'anomalies. Cela facilite également la détection de techniques d'attaque inconnues, car celles-ci modifient le comportement des processus, des fonctions et des applications des terminaux. Les services gérés d'EDR sont appelés MDR (Managed Detection and Response).

« L'environnement de risque des entreprises s'est considérablement complexifié suite à leurs efforts de transformation numérique et aux changements imposés par la pandémie sur le lieu de travail », explique Bob Bragdon, SVP/Managing Director chez CSO, au sujet du besoin de nouvelles approches de la sécurité. « Les organisations qui conservent une approche réactive face aux risques de sécurité accuseront un impact direct sur leurs bénéfices, dont le coût sera toujours supérieur à un investissement dans une bonne protection en amont. »

Bob Bragdon conseille aux entreprises de « se concentrer sur les fondamentaux. Assurez-vous que vos solutions sont à jour, qu'elles sont correctement configurées, et adoptez un modèle basé sur le risque pour classer vos investissements technologiques par ordre de priorité. La plupart des attaques ciblant le terminal, il serait judicieux de commencer par des solutions EDR, des systèmes MDR et une expertise externe. »

Conformité : l'identification précoce des incidents contribue aussi à répondre aux exigences en matière de déclarations

L'étude sur la cybersécurité en 2020 d'IDC indique une augmentation des budgets alloués à la cybersécurité pendant la pandémie de coronavirus.

Les problèmes de conformité poussent eux aussi les entreprises à accroître leurs budgets de sécurité informatique. « C'est du moins ce que l'on observe chez nos clients en matière de sécurité informatique, mais aussi de protection des données, de droit de la chaîne d'approvisionnement et de contrôles KYC, entre autres domaines », explique l'avocate Mareike Gehrmann, qui est spécialisée en droit de l'informatique.

Les solutions EDR et MDR offrent la possibilité de détecter et de contrer plus rapidement les attaques, et plus particulièrement les violations de la protection des données qui en découlent. Cela permet aussi de réduire voire d'éviter les sanctions et les amendes prévues par le RGPD (Règlement général sur la protection des données) en cas de signalement tardif ou de non-signalement d'une violation de données.

En cas de violation de données, les sanctions et les amendes du RGPD sont suffisamment élevées pour menacer la viabilité des PME. Les autorités de contrôle peuvent par exemple imposer des amendes pouvant atteindre soit 20 millions d'euros, soit 4 % du chiffre d'affaires annuel mondial total généré au cours de l'exercice fiscal précédent, selon le montant qui est le plus élevé.

Une aide extérieure pour lutter contre les pénuries de compétences et garder les charges de travail sous contrôle

Le besoin de nouvelles approches de la sécurité s'exprime également dans d'autres domaines. Les cyberattaques sont de plus en plus complexes et sophistiquées, alors même que les entreprises sont confrontées à une pénurie de professionnels de la sécurité et qu'elles ne disposent que de connaissances très limitées concernant le panorama des cybermenaces en constante évolution. Cela vaut autant pour les moyennes entreprises que pour les plus grandes.

Afin de combler leurs lacunes en termes d'expertise et de professionnels de la sécurité, les entreprises sont toujours plus nombreuses à faire appel à des prestataires de services de cybersécurité.

« En matière de détection et de réponse, les experts hautement spécialisés et, surtout, disposant à chaque instant d'informations à jour sont très demandés », explique l'expert de la sécurité Uwe Kissmann. « Un hacker professionnel parvient généralement à échapper aux radars. Avant de risquer de se faire prendre, il s'arrange toujours pour rester dans l'ombre. Jusqu'à ce qu'un jour, les entreprises tombent des nues en découvrant que des inconnus ont sillonné leurs systèmes pendant des années sans jamais se faire remarquer. »

Pourtant, ces attaques pourraient être détectées, comme Kissmann le sait bien : « Souvent, cependant, les signaux d'alerte sont ignorés ou mal interprétés. C'est là que des experts surveillant des systèmes 24 heures sur 24, 7 jours sur 7, et disposant de connaissances très spécialisées et à jour peuvent apporter leur aide. »

L’aide extérieure est précieuse : elle optimise la détection et la réponse

S’agissant de la sécurité informatique, une aide extérieure s’avère particulièrement utile lorsque la détection et la défense contre les cyberattaques peuvent être optimisées et accélérées.

Pour les moyennes entreprises, le recours à une solution MDR (Managed Detection and Response) donne accès à des « experts en cybersécurité extérieurs » qui permettent de prendre des mesures de sécurité supplémentaires sans avoir à embaucher de nouveaux salariés.

L’externalisation de la détection et de la réponse peut aider les moyennes et grandes entreprises à améliorer leur détection et leur défense : les systèmes MDR protègent même contre les menaces les plus sophistiquées grâce à une surveillance proactive permanente, à l’expertise de spécialistes et à la threat intelligence externe.

Kaspersky Managed Detection and Response offre tous les avantages clés d’un centre opérationnel de sécurité (SOC) externalisé. Il ne nécessite pas de compétences spécialisées des équipes internes en matière de détection des menaces et d'analyse des incidents, ce qui en fait une solution idéale pour les moyennes entreprises.

En complément de ce service sont proposées des technologies de détection, une expertise complète en threat hunting et la réponse aux incidents par des experts en sécurité. En outre, ce service est équipé de la solution AI Analyst, qui évalue automatiquement les attaques et permet aux analystes du centre de sécurité de se concentrer sur les signaux d’alerte les plus importants.

« Les organisations qui n’ont pas d’équipe de sécurité dédiée doivent envisager d’investir dans des solutions EDR et MDR », recommande Bertrand Trastour. « Forts d’une vaste expertise de détection et d’investigation des attaques ciblées, les professionnels du centre de sécurité externe sont en mesure de remarquer toute activité suspecte sur le réseau d’entreprise, de l’analyser et de signaler un éventuel incident. Ainsi, une attaque est détectée de façon précoce et le client évite la catastrophe que représenterait par exemple une attaque de ransomware. »

Les entreprises disposant d’un SOC en interne peuvent également tirer parti des solutions gérées de détection et de réponse : « Un service MDR peut proposer un second avis même si l’organisation dispose déjà de son propre centre opérationnel de sécurité », ajoute Bertrand Trastour.

Les grandes entreprises voient souvent l’externalisation de la détection et de la réponse comme une extension du SOC ou du service de sécurité informatique interne. De par sa nature, le SOC interne dispose d’une visibilité limitée car sa veille stratégique dans ce domaine dépend de l’infrastructure et des capteurs de sécurité placés sous sa propre surveillance.

Analyse ROSI
Challenge : comment mesurer le coût de la cybersécurité ?

D'après l'ENISA, l'Agence de l'UE pour la cybersécurité, l'analyse **ROSI** peut apporter une réponse.

ROSI, ou « Return On Security Investment », désigne le retour sur investissement de sécurité.

Ainsi, un investissement de sécurité est jugé rentable si l'effet d'atténuation des risques est supérieur aux coûts attendus.

Les effets d'atténuation des risques expriment les bénéfices d'un investissement de sécurité. Autrement dit, c'est une « réduction des valeurs à risque » qui découle de l'atténuation du risque associé aux pertes de valeur financière, d'après l'ENISA.

La formule du ROSI a été mise au point par une équipe de l'université d'Idaho sous la direction du chercheur Huaqiang Wei. Cette équipe s'est servie de métriques existantes du secteur de l'investissement en sécurité informatique qu'elle a combinées avec des théories propriétaires, avant d'attribuer des valeurs à tous les facteurs, qu'il s'agisse d'actifs matériels ou immatériels.

ROSI = R - (R-E) + T

ou bien

ROSI = R – ALE

R : coûts annuels engagés pour répondre à tous les incidents liés à la sécurité.

E : économies financières annuelles résultant de la réduction du nombre d'incidents liés à la sécurité grâce à la mise en place de la solution de sécurité.

T : coût annuel de l'investissement en sécurité.

ARO : probabilité qu'un risque survienne au cours d'une année (taux d'occurrence annuel)

SLE : perte financière attendue en cas de survenue d'un risque (espérance de perte unique)

ALE : espérance de perte annuelle

*ALE = SLE*ARO*

Exemple de calcul :

L'entreprise Muster GmbH envisage d'investir dans une solution de sécurité informatique. Chaque année, Muster GmbH est victime de cinq cyberattaques (ARO = 5). Le directeur de la sécurité estime que chaque attaque entraîne environ 15 000 euros de pertes (SLE = 15 000). Supposons que la solution de sécurité déjoue au moins 80 % des attaques (taux d'atténuation = 80 %) et qu'elle coûte 25 000 euros par an (15 000 euros de licence + 10 000 euros pour la formation, l'installation, la maintenance, etc.). Le calcul du retour sur investissement de sécurité pour cette solution est le suivant :

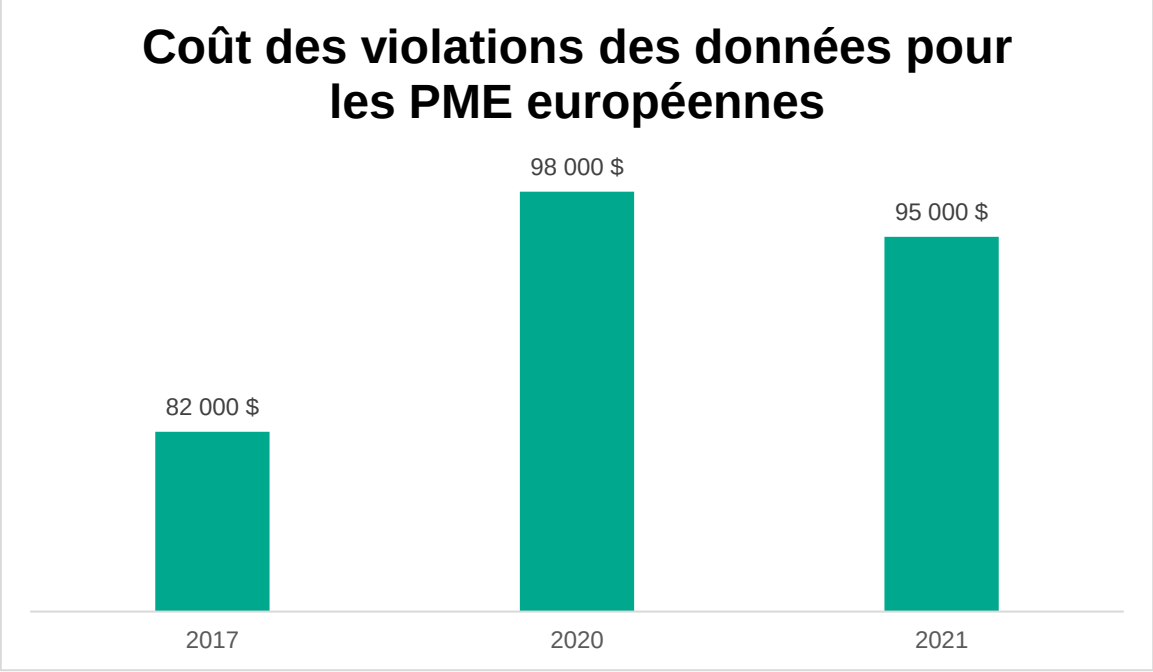
ROSI = ((5 * 15 000) * 0,8 – 25 000) / 25 000 = 140 %

D'après le calcul du ROSI, cette solution de sécurité est rentable et donc économiquement viable.

À combien s'élèvent les coûts induits par des incidents de sécurité informatique par rapport aux dépenses effectuées en amont pour les contrer ?

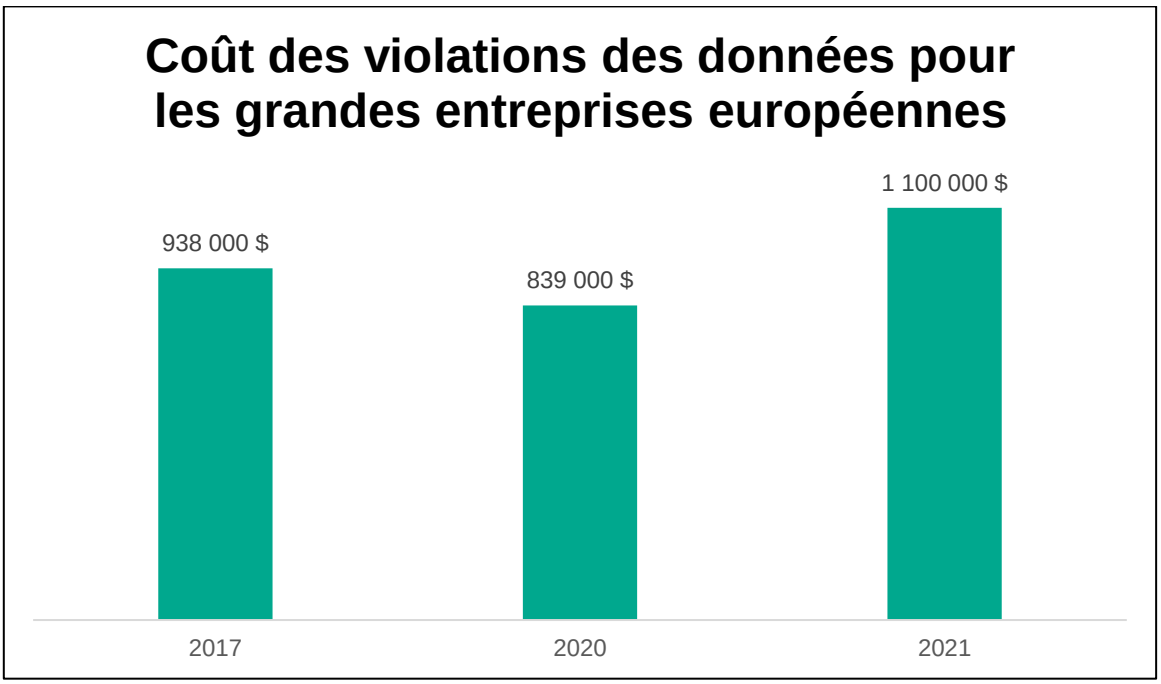
D'après l'enquête internationale de Kaspersky « Rapport économique sur la sécurité informatique en 2021 : gestion d'une complexité informatique qui tend à croître »[2], le coût moyen des incidents de sécurité informatique pour les moyennes et grandes entreprises correspond aux graphiques ci-dessous.

Ainsi, depuis 2017, le coût individuel des violations de données pour les PME s'est stabilisé :



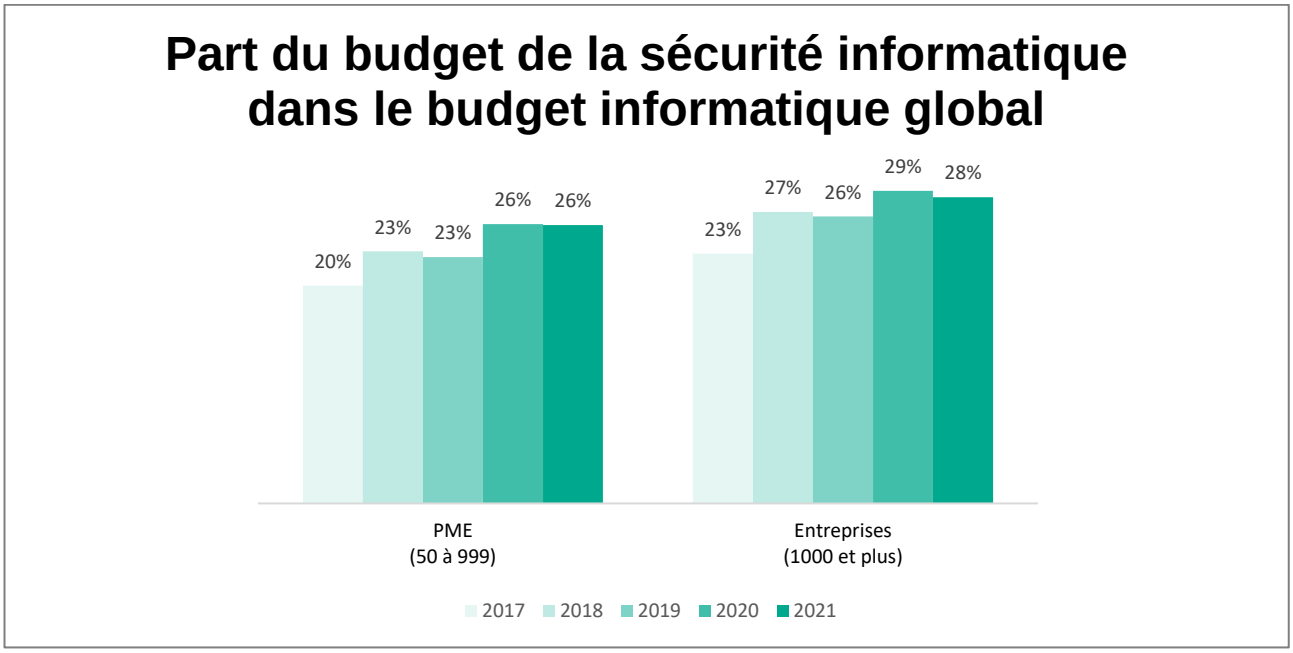
[2] L'Enquête mondiale de Kaspersky sur les risques liés à la sécurité informatique pour les entreprises (ITSRS) est une enquête internationale menée auprès de décideurs d'entreprises du secteur informatique. Elle a été réalisée aux mois de mai et juin 2021 à partir d'un total de 4 303 entretiens avec des entreprises de plus de 50 salariés. Kaspersky mène cette enquête une fois par an.

Pour les grandes entreprises, les coûts sont les suivants :



« Notre étude montre que des approches à la pointe de la sécurité, telles que les solutions EDR et MDR, fonctionnent bien. Pour les entreprises sondées, les coûts induits par des incidents de sécurité informatique ont diminué par rapport aux années précédentes. Ces dernières années, la volonté croissante d'investir a eu des retombées positives, avec une baisse des pertes financières liées aux incidents de cybersécurité », affirme Bertrand Trastour.

Depuis 2017, les budgets alloués à la sécurité informatique ont augmenté parmi les PME et les grandes entreprises du monde entier. Ils représentent désormais plus d'un quart du budget informatique total.



« Il est vital que les PME et les grandes entreprises réalisent des investissements stratégiques pour survivre dans un contexte de menaces à la complexité accrue. Elles doivent investir dans l'externalisation de l'expertise et des services, dans des solutions performantes telles que les systèmes EDR ou MDR, ainsi que dans des couches de sécurité adaptées à leur activité, comme la protection dans le cloud », explique Bertrand Trastour.

Certains CISO se servent de la méthode ROSI, d'autres non. Il s'agit au final d'une décision individuelle.

« En ce qui concerne le conseil stratégique des cadres dirigeants, la méthode ROSI (entre autres approches) est au cœur de la discussion », indique le directeur d'Accenture Uwe Kissmann. « Dans bien des cas, les participants veulent voir l'efficacité et la pertinence de leur stratégie de cybersécurité exprimées en chiffres sur un tableur Excel. Cela permet de déterminer plus facilement l'efficacité de l'allocation des budgets de cybersécurité à long terme. »

Kissmann explique l'importance de la perspective économique : « Dans le cas de la cybersécurité, la meilleure approche consiste à ajouter un versant financier à une logique principalement axée sur la technologie. Ici, le ROSI est d'une grande aide car il crée le fondement économique d'une protection efficace dans la durée. Toutefois, nous devons garder à l'esprit que les méthodes de quantification sont souvent insuffisantes lorsque l'on parle d'informatique. Par conséquent, cette approche doit être complétée par d'autres éléments pertinents. »

Stefan Wittjen, CISO chez Vivantes Netzwerk für Gesundheit GmbH, a un avis divergent : « Pour ma part, je trouve le débat autour du ROSI trop théorique. Je ne suis pas obligé de me plier à la dictature des chiffres dans mon quotidien, et j'en suis ravi. Si nos hôpitaux étaient obligés de fermer leurs portes en raison d'incidents liés à des mesures de sécurité inadéquates, la rentabilité financière des investissements réalisés importerait peu. »

« Les investissements dans la cybersécurité, en particulier dans la détection et la réponse, ont une véritable utilité. Ces services peuvent également être externalisés à moindre coût à des experts en sécurité extérieurs comme nous-mêmes », explique Bertrand Trastour. « Cette solution pèse moins lourd sur les budgets de sécurité tout en détectant les cybermenaces de manière plus efficace et plus rapide, ce qui réduit considérablement les dommages indirects. »

kaspersky

www.kaspersky.fr/
www.securelist.com