KASPERSKY lab

Sensibilisation à la cybersécurité : il est temps d'ouvrir les yeux !

10 raisons pour les revendeurs informatiques d'intégrer la sensibilisation à la sécurité informatique à leur offre

www.kaspersky.fr
#truecybersecurity

Introduction

De nos jours, la plupart des entreprises savent qu'elles ne peuvent plus se contenter d'utiliser un bon logiciel de protection des terminaux. En outre, les nouveaux cadres juridiques comme le Règlement Général sur la Protection des Données (RGPD) imposent une protection accrue pour les systèmes informatiques et une meilleure compréhension de la protection des données. Cependant, respecter ces exigences sans un portefeuille doté des outils nécessaires s'avère généralement difficile et chronophage.

Pour les partenaires informatiques, cette situation présente de nouveaux défis mais leur offre également de formidables opportunités de se positionner non seulement en tant que fournisseur de logiciels pour les entreprises, mais aussi en tant qu'auditeur et consultant en sécurité. Ce livre blanc présente dix raisons d'ajouter une formation de sensibilisation à la sécurité informatique à votre portefeuille.

Voici quelques-uns des défis auxquels vous êtes susceptible de faire face :

Des exigences de sécurité accrues et une nouvelle législation

Les exigences croissantes en matière de sécurité informatique pèsent tout autant sur les entreprises que sur les revendeurs, et de nombreuses questions restent souvent sans réponse. La mise en œuvre du RGPD s'apparente le plus souvent à un puits sans fond. Comment régler le plus simplement possible les problèmes de ce genre et, mieux encore, conseiller vos clients de manière professionnelle ?

Le marché offre de nombreuses solutions, mais quelles sont celles qui sont le plus adaptées aux besoins de vos clients ?

En matière d'innovations en termes de sécurité, les fabricants tentent souvent de surpasser la concurrence. Comment trouver la meilleure solution, à la fois pour vos clients, et pour vous en tant que revendeur ? L'impressionnante diversité des solutions disponibles augmente le risque de perdre de vue le contexte et d'oublier l'essentiel.

Un important investissement initial en formation est-il justifié ?

Dès que vous avez trouvé une solution, les coûts grimpent en flèche. En tant que revendeur, quels sont vos besoins exacts en matière de formation et avez-vous du temps pour vous y consacrer ? Quel genre de résultats attendez-vous ? Ces résultats justifient-ils une prise de risque ? Le fabricant met-il à votre disposition des programmes de formation et un support ?

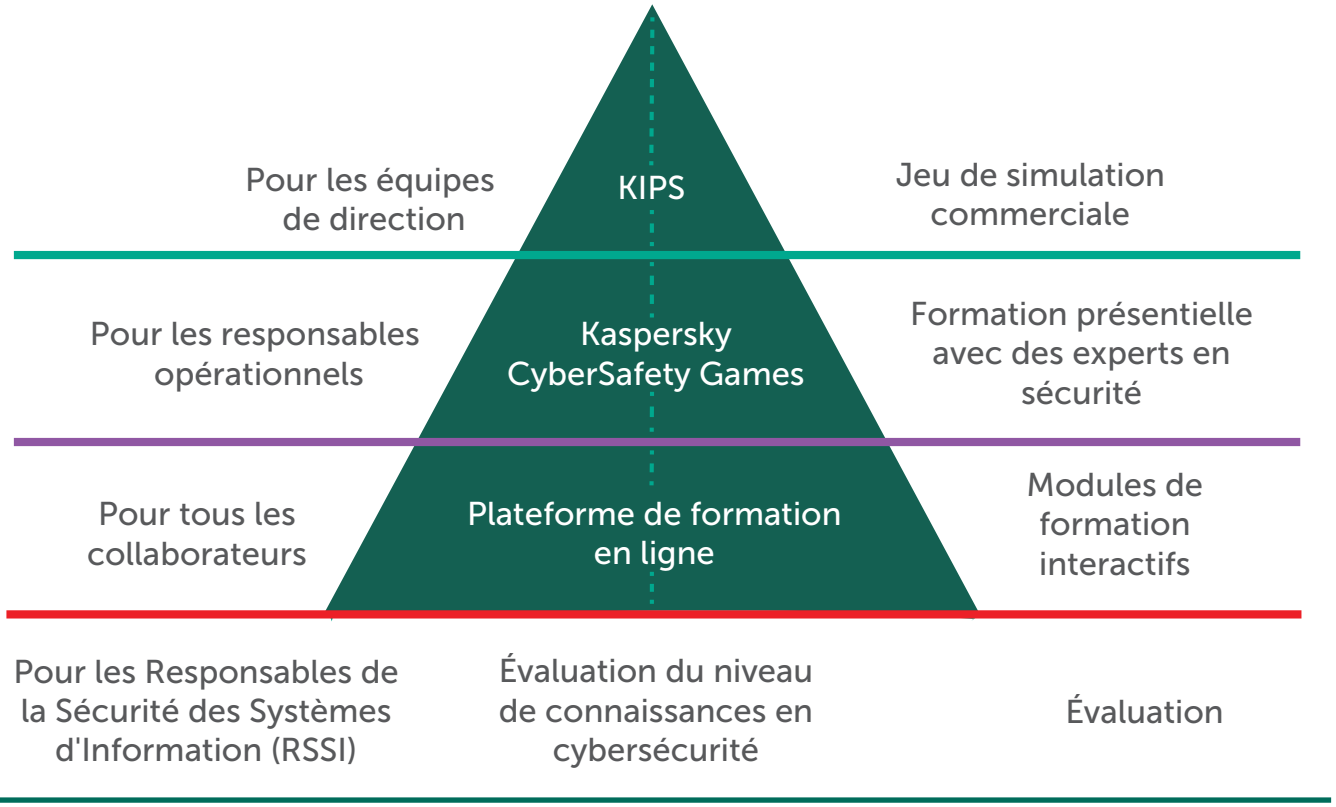
Des programmes de licence exaspérants

Il peut parfois sembler plus simple de rédiger une thèse que de travailler avec un programme de licence. Se familiariser avec ces programmes peut rapidement tourner au cauchemar. En tant que partenaire, vous n'avez pas de temps à perdre avec un processus de facturation complexe, surtout si votre portefeuille comporte plusieurs fabricants.

Selon une étude[1] réalisée par Kaspersky Lab et B2B International, 52 % des entreprises estiment que leurs salariés mettent en péril leur stratégie de sécurité informatique par négligence ou par manque de connaissances.

Elles redoutent tout particulièrement les salariés qui partagent des informations inappropriées sur leurs appareils mobiles (47 %), la perte physique d'appareils mobiles (46 %) et l'utilisation inappropriée de ressources informatiques (44 %).

[1] The human factor in IT security: How Employees are Making Businesses Vulnerable from Within (Le facteur humain en matière de sécurité informatique : les salariés représentent un risque interne pour les entreprises), juin 2017



Kaspersky Lab propose des formations dédiées pour chaque branche de l'entreprise

En examinant ces résultats de plus près, les préoccupations liées à la mauvaise utilisation des ressources informatiques par les salariés varient selon la taille de l'entreprise : Les petites entreprises (entre 1 et 49 salariés) se sentent plus menacées par ce problème que les entreprises de plus de 1 000 salariés. Cela peut s'expliquer par la mise en place de politiques plus strictes par les grandes entreprises

Je suis convaincu, mais comment obtenir l'adhésion de mes clients ?

Dans un monde idéal, le fabricant montrerait au revendeur les problèmes à résoudre du point du vue du client. À quoi devrait penser le client dans cette situation ? Qui est affecté par une cybermenace spécifique, et pour quelle(s) raison(s) ? Qui est votre interlocuteur principal en matière de cyber-sécurité ? Une fois l'adhésion du client obtenue, tout doit se dérouler de manière fluide. Pour cela, vous devez définir clairement les processus d'achat et de commande à suivre, et désigner un interlocuteur en cas de question.

J'ai déjà tant de choses à faire, comment pourrais-je libérer des ressources supplémentaires ?

De toute évidence, l'augmentation des ventes est toujours considérée comme une bonne chose. Mais cette augmentation entraîne-t-elle également une augmentation proportionnelle des dépenses ? Plus vite vous obtiendrez l'adhésion de vos clients, plus il vous sera facile de mener à bien vos opérations commerciales. Et moins vous dépenserez en service après-vente, plus vous générerez de bénéfices. Vous devriez donc vous concentrer sur des projets qui offrent une marge élevée et génèrent une forte demande. En outre, vous devriez toujours pouvoir vous appuyer sur votre distributeur, qui en tant que spécialiste externe, vous aidera à développer votre activité. Cela peut par exemple prendre la forme de campagnes marketing, de services, de budget co-Marketing (MDF), ou encore de support client sous la forme de réunions ou d'événements.

Sécurité des terminaux : je suis déjà équipé

Heureusement, la plupart des entreprises sont désormais équipées d'un logiciel antivirus. Cela étant, les choses ont changé. Les entreprises ont besoin de concepts de sécurité plus exhaustifs et vous vous retrouverez en concurrence directe avec d'autres fournisseurs de sécurité. Néanmoins, il existe de nombreuses manières d'engager un dialogue avec un nouveau client, quelle que soit la solution de sécurité qu'il utilise.

Raison 1 : le risque vient des salariés

Il y a quelques années à peine, l'erreur humaine était à l'origine de plus de **80 %** des incidents de cybersécurité.[1] Même si une récente étude de Kaspersky Lab montre une nette amélioration de la situation, avec seulement **46 %** d'incidents ayant pour cause une erreur humaine, cette même étude montre également que, dans environ **40 %** des entreprises étudiées, les salariés tentent de dissimuler les incidents de cybersécurité qu'ils provoquent par peur des conséquences.[2] C'est un problème grave : les entreprises perdent chaque année plusieurs millions dans la récupération d'incidents causés par leurs salariés. Les coûts associés sont considérables, principalement en raison de la nouvelle législation RGPD. Les entreprises ont donc tout intérêt à réduire ce risque au minimum.

Le plus souvent, les programmes de formation traditionnels ou sur site échouent à inculquer aux salariés les changements de comportement requis, ou à les motiver suffisamment pour renforcer leur sensibilisation à la sécurité informatique. L'impact de ces programmes, pourtant très chers comparés aux formations en ligne, est nul ou limité dans le temps.

Les programmes de formation sur ordinateur, calibrés pour chaque salarié, fournissent les connaissances d'une manière claire, et ont un impact à long terme. De plus, les connaissances acquises par le biais d'une formation en ligne sont facilement mesurables. Cela génère non seulement une attitude positive envers la question de la sécurité informatique au sein de l'entreprise, mais permet également d'ancrer fermement le concept de sécurité informatique dans l'esprit de l'ensemble des salariés.

[1] Indice IBM 2015 relatif à la veille stratégique en matière de sécurité, enquête 2015 sur les violations de la sécurité des informations. Gouvernement du Royaume-Uni, en partenariat avec InfoSecurity Europe et PwC.

[2] https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Raison 2 : le marché est énorme

Le marché des formations de sensibilisation sur ordinateur augmente d'environ 50 % par an (selon les principales analyses du marché). Là encore, on peut s'attendre à une hausse de la demande à l'avenir.

Selon une récente étude, seules **3 %** des entreprises estiment qu'une solution de protection des terminaux seule constitue une protection efficace contre les cybermenaces. Elles pensent plutôt que les salariés eux-mêmes ont un rôle crucial à jouer dans la protection de l'entreprise. D'ailleurs, presque **50 %** des entreprises considèrent que des salariés peu ou pas formés représentent un risque de cybersécurité majeur. Néanmoins, le manque de budget reste en première place.

Kaspersky Lab a donc lancé sur le marché une série de solutions de formations assistées par ordinateur. Celles-ci sont basées sur les dernières techniques d'apprentissage et concernent tous les niveaux de l'entreprise.

Raison 3 : toute entreprise est tenue par la loi de prendre des mesures de sécurité

Depuis la mise en place du RGPD, toute entreprise est obligée de se conformer au principe de « Privacy by Design » (respect de la vie privée dès la conception). Avant toute chose, elles doivent former leurs salariés au traitement des données et aux méthodes permettant d'éviter ou d'éliminer les risques de perte de données. Pour cela, elles peuvent choisir entre une session unique de formation sur site pour laquelle les salariés doivent simplement confirmer leur présence par une signature, ou une plateforme de formation s'intégrant à une politique de sensibilisation durable qui profite réellement aux salariés. Cette deuxième solution permet de plus à l'entreprise de démontrer de manière transparente qu'elle satisfait aux exigences réglementaires et d'encourager ses salariés à protéger les données.

[3] https://gdpr-info.eu/issues/privacy-by-design/

Impact financier moyen des actions inappropriées par des salariés négligents ou mal informés[1]

Pour les petites et moyennes entreprises

- Divulgation inappropriée des données — 88 000 €
- Perte d'appareils mobiles exposant l'entreprise à des risques — 99 000 €
- Perte d'appareils ou de supports contenant des données — 81 000 €
- Utilisation inappropriée des ressources informatiques par les salariés — 68 000 €

Pour les grandes entreprises

- Incidents impliquant des appareils « non informatiques » connectés — 1,6 M€
- Perte d'appareils ou de supports contenant des données — 1,1 M€
- Utilisation inappropriée des ressources informatiques par les salariés — 581 000 €
- Partage inapproprié de données sur des appareils mobiles — 464 000 €

Les violations de données en chiffres[2] :

- En 2017, 61 % des victimes de violation de données étaient des entreprises de moins de 1 000 salariés
- 81 % des violations liées au piratage exploitent des mots de passe volés, faibles ou faciles à deviner
- 43 % des violations de données ont eu lieu sur les réseaux sociaux
- 66 % des programmes malveillants ont été installés à partir de pièces jointes malveillantes

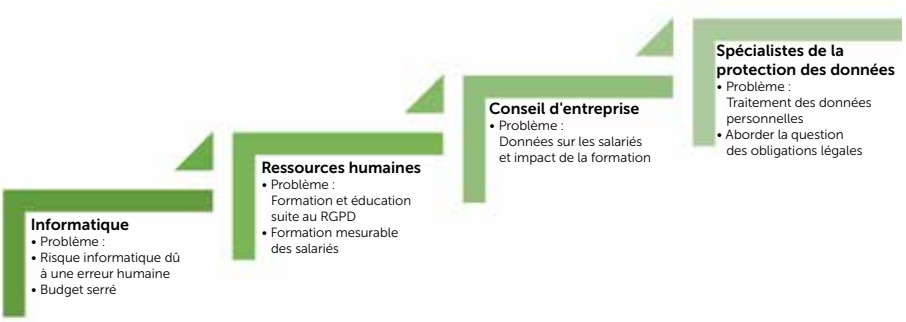
[1]« Rapport sur les risques informatiques mondiaux 2017 ». Kaspersky Lab et B2B International

[2]« Rapport 2017 d'enquêtes sur la violation des données », Verizon

Raison 4 : un budget serré importe moins

Selon plusieurs études, les entreprises se disent prêtes à investir dans la sécurité informatique, mais y renoncent souvent faute de budget. Ce constat est particulièrement vrai pour les PME. Néanmoins, cela implique que ces formations soient dispensées par l'entreprise. Si le service informatique voit bien sûr un intérêt direct à ce type de formation, il en va de même pour les ressources humaines et le responsable de la protection des données (DPO). C'est également là que le budget formation peut se trouver. Concrètement, cela signifie que lors de vos discussions initiales avec votre client, vous pouvez lui préciser que le budget requis peut provenir des ressources humaines, ce qui soulagera le service informatique.

Le diagramme ci-dessous vous présente les secteurs d'activité concernés par la sensibilisation à la sécurité informatique, qui doivent donc être impliqués dans la prise des mesures appropriées :



Raison 5 : un facilitateur idéal

Si vous adoptez l'approche de « sécurité des terminaux » de manière indépendante, il vous sera probablement difficile d'y parvenir sans un minimum de dépenses. Comme nous l'avons déjà expliqué, de nombreuses entreprises sont déjà équipées d'une solution. En général, vous ne pourrez conclure un accord avec ces entreprises qu'en leur proposant un prix imbattable et à condition que leur solution actuelle ne soit pas satisfaisante. En revanche, sur la question de la sensibilisation à la sécurité informatique, vous n'aurez qu'à enfoncer des portes ouvertes. 50 % des entreprises pensent que la mise en place de formations est difficile, mais en raison du RGPD, l'immense majorité d'entre elles comptent désormais sur celles-ci pour développer la sensibilisation à la sécurité informatique.

Avec Kaspersky Security Awareness Platform, vous pouvez proposer une solution simple à administrer, ne grèvant pas le budget du service informatique, et offrant une réelle valeur ajoutée à tous les services. Les perspectives sont excellentes. Mieux encore, une fois cette première étape franchie, de nouvelles opportunités s'offriront à vous.

Raison 6 : un potentiel énorme pour les ventes additionnelles et les montées en gamme

Dès lors que vous ajoutez une entreprise à votre base clients, vous pouvez mieux positionner l'ensemble de votre portefeuille auprès de celle-ci, car vous connaissez ses besoins, son architecture informatique et sa volonté d'investir. Si votre client est satisfait, il sera heureux de découvrir vos autres services. En conséquence, vous pourrez même devenir son nouveau fournisseur matériel ou logiciel. Les services vous aident à compléter votre gamme de produits. Vous pouvez ainsi organiser des réunions trimestrielles pour discuter des résultats de la formation et planifier le trimestre suivant.

Raison 7 : vos clients ne recherchent pas un fournisseur, mais un consultant

La sécurité informatique est complexe. Les PME en particulier manquent à la fois de connaissances et de ressources dans ce domaine. Vous pouvez donc vous positionner non seulement comme un fournisseur, mais également comme un consultant en sécurité informatique pour vos clients. Vous êtes en effet en mesure de simplifier l'informatique en l'expliquant à chaque salarié. La formation de sensibilisation à la sécurité informatique de Kaspersky Lab vous aide à développer, configurer et déployer, dans plusieurs langues et selon un calendrier bien défini, un concept global de formation personnalisée auprès des différents services de votre client. De cette manière, vous pouvez offrir un service très apprécié qui dynamisera votre activité.

Bien sûr, les besoins de chaque client sont différents, mais les partenaires Kaspersky Lab peuvent suivre un concept de base qui, une fois créé, est applicable à d'autres clients. Les experts de Kaspersky Lab et nos distributeurs sont heureux de contribuer au développement de votre activité.

Raison 8 : un cycle de vente court

La plupart des projets ont un cycle de vente d'au moins six mois, mais, dans les faits, ces cycles durent plutôt douze mois. En règle générale, Kaspersky Security Awareness Platform vous permet de facturer un projet client au cours des trois premiers mois. La durée de mise en œuvre est très courte, les dépenses sont gérables et la disponibilité de la solution est garantie. En outre, le modèle de licence est extrêmement simple : une licence = un salarié.

Dans les mois à venir, nous continuerons de développer les services de Kaspersky Lab et nous proposerons une autre option de licensing, en complément des options traditionnelles. Les fournisseurs de services managés (MSP) pourront ainsi distribuer la solution à leurs clients par le biais d'un modèle souple et évolutif.

Raison 9 : des coûts avantageux

Par rapport à une formation traditionnelle, la solution Kaspersky Automated Security Awareness Platform permet de faire des économies considérables et de prolonger la formation des salariés à faible coût. Une session de formation présentielle représente un coût de plusieurs milliers d'euros pour une PME, mais son impact n'est ni durable ni mesurable. Personne n'aime rester assis dans une salle de réunion toute la journée pour se former sur un sujet aride et technique.

Avec Kaspersky Automated Security Awareness Platform, vos clients profitent de plus de 30 modules de formation différents. Les salariés disposent d'une année entière pour utiliser la plateforme. Plus intéressant encore, la formation est interactive : le système affiche des scénarios pratiques du quotidien dans lesquels le salarié est directement impliqué. Par exemple, pour 100 utilisateurs, la plateforme ne coûte pas plus cher que deux sessions de formation physiques par an. En complément des modules de formation, les entreprises ont également accès à des simulations d'attaque par phishing, des évaluations et des tests de connaissances avec des questions prédéfinies et personnalisées pour déterminer le niveau de connaissances des salariés.

Raison 10 : support et accès optimisés

Toutes les entreprises doivent aujourd'hui être impliquées dans la sensibilisation de leurs salariés à la cybersécurité. Elles sont donc à l'écoute de vos propositions en la matière, quel que soit leur secteur d'activité (énergie, fabrication, commerce, industrie, infrastructures critiques, etc.) et leur nature (agence gouvernementale, prestataires de services financiers ou toute autre organisation devant se conformer au RGPD). La solution Kaspersky Automated Security Awareness Platform intéressera tous ceux qui doivent gérer ou organiser la formation des salariés.

Résumé

Les entreprises sont de plus en plus perplexes face à la complexité des systèmes informatiques modernes. Dans le même temps, elles souhaitent réaliser des économies tout en veillant à la bonne marche de leurs opérations. Dans ce contexte, la sécurité informatique représente une priorité absolue. Les salariés d'une entreprise doivent impérativement apprendre à reconnaître rapidement les cybermenaces potentielles et savoir y répondre de manière appropriée. Néanmoins, près de **50 %** des entreprises dans le monde déplorent le manque de formation de leurs salariés ou l'absence d'outils de formation appropriés. Cette situation constitue un sérieux risque de sécurité, car plus de **46 %** des incidents de cybersécurité sont imputables à une erreur humaine. les entreprises perdent chaque année plusieurs millions dans la récupération d'incidents causés par leurs salariés. Les programmes de formation traditionnels ou sur site ne parviennent pas à motiver suffisamment les salariés pour les inciter à modifier leur comportement. En tant que partenaire Kaspersky Lab, vous pouvez utiliser la solution Security Awareness Platform pour résoudre ce problème.

Le marché exige une approche inédite, mais offre également aux partenaires de formidables opportunités pour acquérir et fidéliser de nouveaux clients, voire devenir leur conseiller en sécurité attitré. Grâce à une solution très simple, vous pouvez considérablement renforcer votre relation avec vos clients.

Utilisez Kaspersky Lab pour faire vos premiers pas dans ce marché lucratif.
À bientôt !

Jusqu'à	Moins de	Jusqu'à	Plus de	Plus de
90%	**50%**	**93%**	**30x**	**86%**
de réduction des incidents de sécurité informatique	de réduction du coût des incidents de sécurité informatique Taux de	des utilisateurs appliquent les connaissances acquises dans des scénarios du quotidien	de retour sur investissement en matière de sensibilisation à la sécurité informatique	des participants recommandent la formation de sensibilisation à la sécurité informatique

Présentation de la solution

Kaspersky Security Awareness Platform

Kaspersky
Cybersecurity
Awareness Training

Plus d'informations :
https://www.kaspersky.fr/enterprise-security/security-awareness

Version démo de la plateforme :
https://www.kaspersky.fr/enterprise-security/cybersecurity-awareness/demo

Vous souhaitez commencer ?
Contactez-nous ici.

La plateforme de formation en ligne de Kaspersky Lab est conçue pour l'ensemble des salariés d'une entreprise. Sans quitter leur ordinateur, les participants utilisent des exercices interactifs et des scénarios typiques du quotidien pour découvrir les menaces informatiques potentielles et apprendre à les gérer. Des simulations d'attaque par phishing et des modules de formation sur un thème spécifique (navigation sécurisée, sécurisation des mots de passe, protection des données, etc.) forment les salariés et les aident à mieux réagir face aux cybermenaces potentielles. Sensibilisez vos clients à la sécurité informatique avec Kaspersky Lab !

En quelques mots :

- **32 modules d'apprentissage** d'une durée de 10–20 minutes chacun
- **Modules sur des thèmes variés : RGPD, ransomwares, sécurisation des mots de passe, sécurité de la messagerie,** etc.
- **Disponible dans 35 langues** (allemand, anglais, italien, espagnol, etc.)
- Évaluez votre propre niveau grâce à des **tests de connaissances**
- **Simulations d'attaque par phishing** avec plusieurs modèles modifiables
- **Fonctions étendues d'analyse et de création de rapports**
- **Options d'administration** simples et exhaustives

Kaspersky Lab

Cybersécurité pour les entreprises :
https://www.kaspersky.fr/enterprise-security
Actualités dédiées aux cybermenaces :
www.securelist.com
Actualités dédiées à la sécurité informatique :
business.kaspersky.com

#truecybersecurity
#HuMachine

www.kaspersky.fr