KASPERSKY lab

RGPD : plus que des cases à cocher

Les solutions de cybersécurité ne peuvent pas assurer la conformité de façon indépendante, mais elles fournissent une protection efficace contre la violation de données et la fuite de données sensibles.

www.kaspersky.fr

#truecybersecurity

RGPD : plus que des cases à cocher

« Aucune confidentialité sans sécurité » est un principe de longue date en matière de protection des données. Alors que le Règlement général sur la protection des données de l'UE devient réalité, il est temps de regarder comment les technologies de cybersécurité peuvent soutenir la protection élargie des données et les objectifs de confidentialité du Règlement.

Données personnelles : une vache à lait pour les cybercriminels

Les données à caractère personnel sont littéralement partout.

Les gens soumettent régulièrement des informations à caractère personnel à toutes sortes d'organisations, souvent sans questionner ou comprendre pourquoi ou comment celles-ci seront utilisées, ou à quels tiers inconnus elles seront partagées.

En 2017, 23 % des organisations soumises au RGDP ont déclaré avoir connu une cyberattaque dans les 12 mois précédents.[1]

Nous avons tous fait défiler un vague contrat de licence de l'utilisateur final (CLUF) et cliqué sur « Accepter », sans réellement savoir ce qu'il advient de nos données. En rendant accessibles leurs services à la condition d'accepter ce contrat, de nombreuses organisations obligeaient effectivement les utilisateurs à prendre le risque que leurs données tombent en de mauvaises mains. Malheureusement, cela arrive souvent.

Alors que la majorité des organisations font de leur mieux pour protéger les données qu'elles recueillent, cela se produit souvent sans une réelle détermination outre que récupérer des données qui « pourraient s'avérer utiles ».

Avec la meilleure volonté du monde, l'absence de processus établis, combinée avec une connaissance limitée des risques et des responsabilités associés, signifie souvent que les données sont recueillies et enregistrées sans précautions de sécurité. Pire encore, elles sont souvent partagées avec (ou vendues à) des tiers sans mettre en place un accord de protection des données, ou sans l'accord expresse ou la connaissance de la personne concernée.

Malheureusement, le type de données à caractère personnel qui est utile à votre entreprise est également lucratif pour les cybercriminels : des programmes de fidélité aux données de paiement, date de naissance et dossiers médicaux, tout ce qui contribue à personnaliser l'expérience client de votre entreprise ou à prendre soin de vos employés est très attrayant pour les cybercriminels. En fin de compte, ces données deviennent une sorte de devise criminelle, échangée et commercialisée sur les marchés noirs du Darknet.

À compter du 25 mai 2018, si quelque chose comme cela arrive, il ne s'agira pas seulement d'un regrettable problème pour les personnes concernées par ces données, cela sera également votre problème.

1 Marsh : Préparation pour le RGPD : un indicateur de la gestion des risques cybernétiques (octobre 2017)

Quatre petites lettres, une grande initiative de protection des données

59 % des entreprises supposent que leur sécurité informatique sera compromise et admettent la nécessité de se préparer à ces événements.[2]

Violation des données ? Pénalités

À la suite d'une violation massive des données de leurs clients en 2015, la société de télécommunications britannique Talk Talk s'est vue infliger une amende record de 400 000 £ par le Information Commissioner's Office (Bureau britannique du commissaire à l'information).

Le montant de l'amende était élevé car il a été constaté que la violation aurait pu être évitée si l'entreprise avait pris les mesures nécessaires pour protéger les données des clients.

En vertu de la pénalité maximale du RGPD de 4 % du chiffre d'affaires, cette amende de 400 000 £ pourrait atteindre 60 millions de livres si la loi était appliquée dans sa pleine mesure. Au minimum, des audits, des contrôles et un examen des processus seraient impliqués, ce qui coûte de l'argent.[3]

Les sujets d'actualité avec 4 % du chiffre d'affaires global d'amende et l'obligation de notification de violation de 72 heures attirent beaucoup d'attention. Mais il convient de préciser que le RGPD est pour vous l'occasion de faire le point sur ce que vous faites avec les données à caractères personnel que vous recueillez, et de vous demander pourquoi vous le faites.

C'est également le moment idéal de reconsidérer l'approche de votre organisation en matière de cybersécurité, car tandis que les technologies de sécurité ne peuvent assurer une conformité de manière indépendante, elles jouent un rôle de soutien clé pour aider les entreprises à atteindre leurs objectifs de protection des données.

Ce que c'est, ce que cela n'est pas...

Malgré le grand nombre de documents, de guides pratiques et d'autres publications qui ont suivi son annonce, la compréhension de base de nombreux aspects du RGPD reste vague. Certains responsables de niveau C continuent de croire que la législation ne s'applique pas à eux, car « Nous n'avons pas ce type de données ». D'autres pensent qu'il s'agit d'un exercice de case à cocher unique avant de poursuivre leur activité professionnelle comme d'habitude.

Malheureusement, tous se trompent :

- Vous avez des salariés, n'est-ce pas ? Les informations que vous recueillez et traitez sont généralement des données à caractère personnel qui les concernent et tombent sous le RGPD. Chaque entreprise qui recueille, traite et/ou conserve des données à caractère personnel, y compris des informations sur les salariés relatives à une transaction ou à une activité dans l'UE (ou qui les transmet à des tiers) est tenue de les protéger.

- Le RGPD n'est pas normatif, il s'agit d'un cadre. Il n'y a pas de liste de tâches à cocher avant d'arriver au paradis de la protection des données.

Alors que le RGPD prévoit les règles à suivre pour la conformité, peu d'informations sont fournies quant à la façon d'y parvenir. Chaque organisation est libre de décider en grande partie des techniques à mettre en œuvre pour elle-même. Le point essentiel est que, parce que la protection des données est un processus, c'est quelque chose que les entreprises doivent continuellement développer.

Il n'y a aucune approche normalisée pour évaluer la conformité. Les cases à cocher ont leurs limites. Les circonstances (et les risques associés) changent et les listes sont rarement exhaustives, de sorte que dans une approche universelle, les points faibles peuvent être négligés.

En fin de compte, c'est ce que fait votre entreprise en vue d'éviter tout incident, parallèlement à votre stratégie de détection anticipée et de repérage, qui vous apportera une grande aide avec le RGPD.

Les solutions et technologies de nouvelle génération de Kaspersky Lab peuvent aider votre organisation à atteindre ses objectifs de cybersécurité dans le cadre de sa stratégie globale de conformité au RGDP.

Examinons ce que cela signifie d'un point de vue pratique.

2 Kaspersky Lab : Rapport sur les risques mondiaux liés à la sécurité informatique 2017

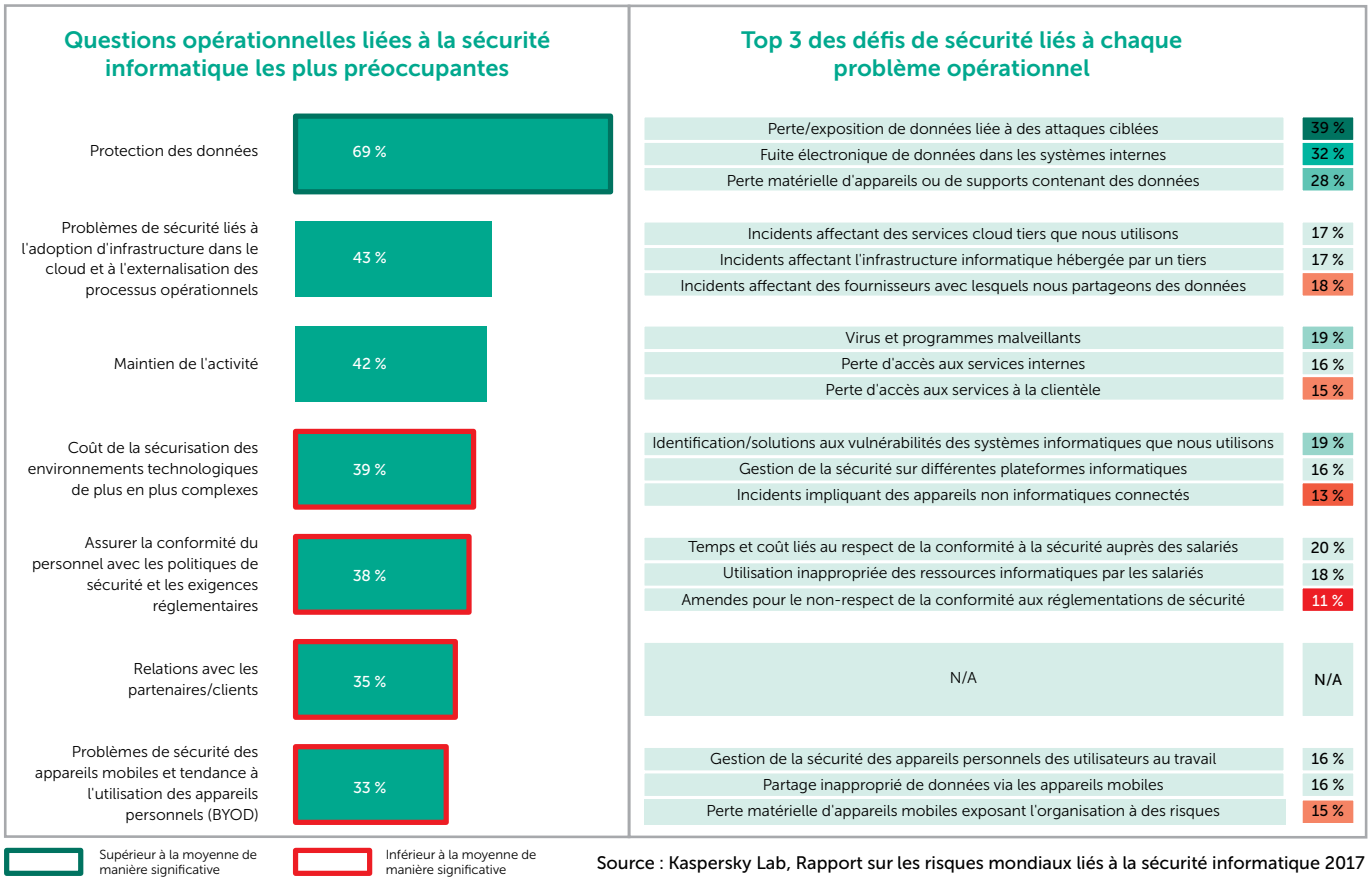
3 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/

Il vaut mieux prévenir que guérir

Les actions humaines - non intentionnelles et délibérées - jouent un rôle important dans la violation de données à caractère personnel. Mais la principale cause des incidents de sécurité aux informations d'identification personnelles reste les cyberattaques qui, outre leur accroissement en termes de volume, changent constamment. C'est pourquoi la cybersécurité joue un rôle fondamental dans la stratégie de prévention de violation et de protection des données.

Soixante-neuf pour cent des professionnels de l'informatique déclarent que la protection des données est leur première préoccupation, avec 38 % affirmant que le fait de veiller à ce que le personnel se plie aux politiques de sécurité et aux exigences réglementaires est une préoccupation.

Préoccupations principales du secteur informatique



Source : Kaspersky Lab, Rapport sur les risques mondiaux liés à la sécurité informatique 2017

La sécurité du traitement – Article 32 du RGPD

L'article 32 du RGPD appelle à des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque lors du contrôle ou du traitement de données à caractère personnel. Ces technologies sont les suivantes :

- Pseudonymisation et chiffrement des données à caractère personnel
- Des mesures pour soutenir la confidentialité, l'intégrité, la disponibilité et la résilience des services et systèmes de traitement
- Capacité de rétablir la disponibilité et l'accessibilité des données à la suite d'un incident
- Capacité à effectuer des tests réguliers et une évaluation des capacités organisationnelles et techniques en vue de sécuriser les données et la manipulation

La cybersécurité joue un rôle important dans la protection des données et pour garantir la résilience du système.

Si l'on considère qu'en 2017, 24 % des entreprises ont signalé la perte, la fuite ou l'exposition de données à la suite d'une attaque de programme malveillant[4], il est facile de voir pourquoi une stratégie de cybersécurité efficace joue un rôle de soutien essentiel dans le respect du RGPD et la réduction globale des risques.

Et l'un des meilleurs endroits pour commencer à renforcer les défenses informatiques de l'entreprise est le terminal. Voici pourquoi...

4 Kaspersky Lab, Rapport sur les risques mondiaux liés à la sécurité informatique 2017

En commençant par la fin (terminal)

Lorsqu'il s'agit d'améliorer la sécurité informatique et la stratégie de protection des données, la protection des terminaux est un excellent point de départ. Cet endroit constitue aujourd'hui une zone de défense de l'entreprise qui peut être améliorée, et ce sans affecter ou dépendre de l'avancement d'autres procédés ou de nouveaux procédés.

- Les terminaux restent aujourd'hui la cible numéro un pour la majorité des cyberattaques, et l'email constitue le vecteur numéro des programmes malveillants pour les entreprises[5].
- Ils peuvent devenir une « fenêtre » pour les données sensibles traitées par votre entreprise, même si ces données se trouvent sur un serveur distant.
- En tant que composant principal de votre réseau informatique, les terminaux situés au même endroit doivent être surveillés afin d'alerter en temps opportun toute activité suspecte. Même ceux qui ne sont pas directement impliqués dans le traitement des données à caractère personnel peuvent constituer une menace s'ils sont connectés au même réseau, car les attaques de programme malveillant peuvent se propager et compromettre ainsi toute l'infrastructure de traitement des données.

49 % des entreprises ont connu une attaque de programme malveillant en 2017, soit une augmentation de 11 % par rapport à l'année précédente[6].

Dans cet environnement, les taux de détection comptent vraiment. Avec plus de 300 000 nouvelles variantes de programmes malveillants détectés chaque jour, même une différence de 0,9 % dans la capacité de détection des menaces peut se traduire par des centaines de milliers de programmes malveillants au cours d'une année. Étant donné que les programmes malveillants les plus développés appartiennent généralement aux derniers 1-2 % des attaques, cette couche de détection supplémentaire peut faire la différence entre une cyberattaque gérée et une attaque qui détruit votre entreprise, en particulier pour les petites entreprises.

Les solutions de détection de terminal les plus efficaces ne se composent pas d'une seule couche de prévention et de détection. Elles utilisent plusieurs niveaux de technologies de nouvelle génération capables de détecter, de bloquer et de réduire les menaces inconnues, même les plus élaborées.

65 % des entreprises attaquées par un ransomware en 2017 ont perdu accès à une quantité importante de leurs données. Un tiers ne les a jamais revues[8].

Kaspersky Endpoint Security for Business combine la sécurité la plus récompensée[7] et la plus éprouvée au monde avec plusieurs couches de technologies de sécurité de nouvelle génération pour protéger les terminaux des entreprises contre tous les types de menaces. Notre moteur d'analyse comportementale est alimenté par une technologie de machine learning dynamique unique et d'un système de détection des menaces assisté dans le cloud, afin de réduire les menaces connues, inconnues et avancées, ainsi que les attaques plus développées telles que les ransomwares qui constituent une menace directe pour la disponibilité et l'intégrité des données à caractère personnel.

Les bloquer avant leur chargement

52 % des entreprises déclarent que la négligence de l'utilisateur final est la plus grande faiblesse dans leur stratégie de sécurité informatique[9].

Empêcher une attaque avant qu'elle ne cause des dégâts est un aspect clé de la résilience et du renforcement du système. À cette fin, la recherche et la résolution des vulnérabilités et des failles dans les applications logicielles clés peuvent aider à empêcher les cybercriminels d'exploiter les logiciels d'entreprise largement utilisés pour accéder aux données à caractère personnel et les voler.

Pourquoi est-ce important ? Réfléchissez-y : les attaques par phishing, les ransomwares, les pièces jointes malveillantes, les logiciels espions ne sont que des exemples de cyberattaques pour voler des données qui ont lieu là où les utilisateurs finaux cliquent sans réfléchir. Il suffit d'un seul email bien camouflé avec une pièce jointe convaincante pour causer une violation de données grave.

Le **système de prévention des intrusions hébergé sur l'hôte avec pare-feu individuel** (HIPS) dans Kaspersky Endpoint Security for Business fournit une couche supplémentaire de résilience. Il détecte et bloque l'activité d'un programme malveillant ou indésirable en temps réel, sans entraver les performances des applications légitimes. Basées sur les dernières informations sur les menaces basées dans le cloud, les

5 Verizon : rapport d'enquêtes sur la violation des données, 2017

6 Kaspersky Lab, Rapport sur les risques mondiaux liés à la sécurité informatique 2017

7 https://www.kaspersky.fr/top3

8 Kaspersky Security Bulletin : Faits marquants de l'année 2017

9 Kaspersky Lab, Rapport sur les risques mondiaux liés à la sécurité informatique 2017

applications se voient attribuer l'une des quatre catégories de confiance qui régissent le type d'accès dont elles disposent pour accéder aux éléments sensibles du système. Du point de vue du RGPD, cela peut fournir une sécurité supplémentaire en limitant l'accès aux fichiers/répertoires sélectionnés par les applications avec de faibles niveaux de confiance.

Le système de **gestion des correctifs et vulnérabilités** de Kaspersky Lab (inclus dans Kaspersky Endpoint Security for Business Advanced) ajoute un niveau de sécurité supplémentaire à vos défenses. Il trouve et corrige les applications vulnérables avant que leurs vulnérabilités ne puissent être exploitées. Grâce à l'automatisation qu'il génère, les équipes informatiques peuvent être libérées de la charge que représente la mise en place de correctifs à temps. La planification vous permet de repousser les correctifs non urgents hors des heures ouvrées, réduisant ainsi la pression sur l'infrastructure.

Pour une véritable protection multi-niveaux, la technologie de **protection contre les vulnérabilités** basée sur le terminal de Kaspersky Lab peut réduire même les vulnérabilités « zero-day » précédemment inconnues, en s'appuyant sur les capacités du moteur d'analyse comportementale pour couvrir le plus grand éventail de types de vulnérabilités.

Ne recueillez pas les données si vous ne pouvez pas les protéger : le stockage

Les terminaux sont les lieux où les données à caractère personnel et les personnes se rencontrent, et les risques associés doivent être réduits. Mais même une fois le nombre de salariés de confiance réduit pour gérer les informations d'identification personnelle (en les conservant avec des processus conformes au RGPD), il existe toujours des risques associés au lieu et à la méthode de conservation des données. Pour une sécurité renforcée et une meilleure visibilité, des installations de stockage réglementées (telles que les serveurs de fichiers ou les dispositifs de stockage connectés) sont attribuées et soumises à des politiques d'accès strictes et une surveillance continue. Malheureusement, ce rôle hautement sensible fait d'eux une cible lucrative pour les voleurs de données, soulignant ainsi la nécessité d'une sécurité renforcée.

Kaspersky Security for File Server (disponible comme composante de Kaspersky Endpoint Security et Kaspersky Total Security for Business), et **Kaspersky Security for Storage** peuvent fournir une protection complète du stockage des données réglementées. Outre la protection multi-niveaux performante, ces solutions sont conçues en pensant spécialement aux serveurs et aux besoins de stockage de données, garantissant l'impact le plus faible sur les performances ou la stabilité, quelle que soit la charge de travail. Elles incluent un mécanisme unique contre le chiffrement[10] qui bloque les effets d'un ransomware lancé à distance, ce qui peut causer des dommages considérables durables s'il est lancé à partir d'une machine avec un accès réseau au stockage ou aux serveurs de traitement des informations d'identification personnelle.

Protéger les goulets d'étranglement

Les emails et les serveurs proxy représentent deux passerelles par lesquelles les cyberattaques peuvent s'infiltrer dans le réseau informatique d'entreprise ou par lesquelles les données à caractère personnel peuvent fuiter. Même les données envoyées par inadvertance, dû à une erreur humaine, constituent toujours une faille. La protection de ces deux goulets d'étranglement au niveau du périmètre de défense de l'entreprise est cruciale.

Kaspersky Security for Mail Server et Kaspersky Security for Internet Gateway[11] peuvent aider à réduire considérablement ces risques, en arrêtant jusqu'à 95 % des menaces entrantes avant qu'elles n'atteignent le terminal et en éliminant le facteur humain et les attaques ciblant spécialement les terminaux. En outre, le risque posé par les données à caractère personnel entrant ou quittant les systèmes peut être géré en refusant l'accès ou la sortie de certains types de fichier.

10 Kaspersky Security for Storage prend en charge la fonctionnalité anti-chiffrement uniquement pour les stockages connectés NetApp

11 Sont également disponibles comme composante de Kaspersky Total Security for Business

- 18 % des entreprises ont subi des pertes de données à cause de la perte physique d'appareils ou de supports mobiles.
- 16 % ont vu leurs données exposées via la perte physique d'appareils mobiles.
- 15 % des entreprises ont connu le partage inapproprié des données via des appareils mobiles.[12]

Appareils mobiles ou cibles mouvantes ?

Grâce à leurs capacités de stockage, de transfert et de partage des données, les appareils mobiles ont longtemps joué un rôle important dans le traitement des données à caractère personnel et, tout comme d'autres technologies, une attention particulière doit être accordée à leur protection.

Kaspersky Security for Mobile est une composante de Kaspersky Endpoint Security for Business, combinant une protection efficace contre les menaces avec des mesures de conservation sécurisée des données telles que le chiffrement et la séparation des données d'entreprise, ainsi que des outils de gestion à distance. Tout ceci crée une base solide pour une utilisation sécurisée des appareils mobiles, y compris toute utilisation faisant partie de la chaîne de traitement des informations d'identification personnelle.

Le bon côté de chaque cloud

Quarante-trois pour cent des entreprises déclarent que les questions de sécurité liées à l'infrastructure du cloud constituent une préoccupation de sécurité informatique primordiale.[13] Kaspersky Hybrid Cloud Security facilite la sécurisation des charges de travail relatives au traitement des données - notamment les informations d'identification personnelle - indépendamment de l'état physique/virtuel ou de l'emplacement (sur site/cloud). Il offre la même sécurité complète pour les infrastructures de virtualisation, les serveurs et les bureaux virtuels du même type. La majorité des couches de sécurité présentes dans les applications pour les charges de travail physiques sont également disponibles dans des formats spécialement conçus pour les systèmes virtuels.

Formation : un averti en vaut deux

Le RGPD impose la promotion de la sensibilisation à la sécurité et à la confidentialité des données auprès des salariés, notamment, le cas échéant, la formation. La confidentialité constitue de fait la pierre angulaire de la conformité au RGPD pour la plupart des entreprises, ce qui demande une plus grande prise de conscience de la cybersécurité, des menaces par email et d'autres cybermenaces relatives à la sécurité des données.

La plateforme de sensibilisation à la sécurité de Kaspersky Lab favorise la promotion des bonnes pratiques en matière de protection des données sur le lieu de travail grâce à des scénarios ludiques. En contribuant à réduire les risques associés à l'erreur humaine, les entreprises peuvent améliorer leur conformité au-delà des cases à cocher et promouvoir une sensibilisation globale et l'adoption de pratiques plus sûres.[14]

Comprendre les risques

L'article 35 du Règlement comporte des mesures qui peuvent être prises pour réduire les risques, notamment les « garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel ».

Du point de vue de la cybersécurité, cela peut inclure l'évaluation de tout logiciel de traitement de données pour les vulnérabilités ou les risques associés à la façon dont ils ont été mis en œuvre. Là où le traitement des données à caractère personnel constitue un élément critique des processus opérationnels, considérer l'ensemble de l'infrastructure informatique comme une « installation de traitement des données à caractère personnel » est une approche utile pour le succès d'une évaluation des risques. L'expertise de cybersécurité nécessaire pour accomplir cette tâche est rarement disponible en interne. En d'autres termes, de nombreuses organisations travaillent avec des tiers spécialistes en cybersécurité pour atteindre cet objectif.

12 Kaspersky Lab, Rapport sur les risques mondiaux liés à la sécurité informatique 2017

13 Kaspersky Lab, Rapport sur les risques mondiaux liés à la sécurité informatique 2017

14 Les solutions de Kaspersky Lab complètent la formation liée au processus au lieu de la remplacer

La formation

Plus de la moitié des entreprises ont reconnu que les actions du personnel négligeant étaient leur plus grande faiblesse en matière de sécurité informatique. Assurer la formation du personnel sur les menaces existantes et comment s'en protéger est donc évidemment indispensable !

	% des répondants en accord avec chaque déclaration	Changement par rapport à l'année dernière	Changement particulièrement important pour
Nous devons employer davantage de spécialistes ayant une expérience spécifique dans la sécurité informatique, plutôt que des professionnels de l'informatique en général	53 %	+79 %	TPE PME ↑
La plus grande faiblesse de notre stratégie de sécurité informatique est la négligence de nos salariés/utilisateurs	52 %	Nouveau	
Nous pensons que nos salariés ne sont pas suffisamment sensibilisés aux problèmes de cybersécurité qui peuvent mener à des incidents	49 %	Nouveau	
Notre connaissance des menaces de sécurité informatique ciblant spécifiquement notre entreprise est loin d'être idéale	46 %	+5 %	TPE PME ↑
Beaucoup de nos salariés ne suivent pas correctement les politiques de sécurité informatique	44 %	Nouveau	
Nos salariés ne sont pas honnêtes lorsque des incidents de sécurité se produisent. Ils ont tendance à masquer les problèmes pour éviter toute sanction	40 %	Nouveau	

Cela est particulièrement vrai pour les grandes entreprises qui étaient plus susceptibles d'être d'accord avec ces déclarations.

Kaspersky Security Assessment Services peut aider à l'évaluation de la sécurité des applications : contrôler si le logiciel utilisé dans le traitement des données est vulnérable aux abus et à l'exploitation. Les spécialistes de Kaspersky Lab peuvent également réaliser des **tests de pénétration** afin de rechercher les points faibles de votre réseau informatique et fournir les conseils nécessaires pour les réduire. Ceci permet de s'assurer que les systèmes et les processus sont affinés en vue d'une meilleure sécurité, facilitant ainsi une évaluation saine de l'impact sur la protection des données.

La cybersécurité peut soutenir le RGPD

Le RGPD est conçu fondamentalement pour protéger et favoriser la confidentialité des données dans un monde où la technologie a transformé la façon dont les informations à caractère personnel sont recueillies, partagées ou stockées.

Alors que le règlement lui-même s'applique à partir du 25 mai 2018, un délai plus long a été accordé aux organisations afin de faire le point sur leur approche en matière de traitement des données et de mettre en œuvre les changements pour conserver les technologies qu'elles utilisent et le type de données qu'elles recueillent et gèrent.

Pour la plupart des organisations, le RGPD a été l'occasion de revoir et d'améliorer leur traitement des données et, par extension, leur cybersécurité. C'est en soi une bonne nouvelle pour les spécialistes de la cybersécurité qui se plaignent depuis longtemps des entreprises négligeant les dispositifs de protection et les processus qu'ils utilisent pour sécuriser leurs données et systèmes. Le RGPD offre aux entreprises une excellente occasion d'examiner leur situation de cybersécurité d'un point de vue de la sécurité des données. Après tout, ce qui est bon pour la sécurité des données à caractère personnel peut être bon pour la sécurité dans de nombreux autres aspects des activités de votre entreprise. Le portefeuille de solutions de Kaspersky Lab, bien qu'il ne constitue pas une garantie de la conformité au RGPD en soi, est prompt à réduire les risques liés au traitement des informations d'identification personnelle de votre entreprise et toutes les autres cybermenaces auxquelles vous faites face aujourd'hui.

Kaspersky Lab
pour les entreprises : **https://www.kaspersky.fr/enterprise-security**
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **www.securelist.fr**

#truecybersecurity
#HuMachine

www.kaspersky.fr