kaspersky BRING ON THE FUTURE

Travail flexible : comment rester en sécurité et assurer la continuité des activités, notamment en période difficile

Le travail à domicile implique le respect des règles de cybersécurité standards que les salariés appliquent lorsqu'ils travaillent dans un bureau. Cependant, l'utilisation d'ordinateurs portables personnels et de réseaux domestiques est beaucoup plus risquée que le travail au sein d'un réseau d'entreprise sécurisé. En outre, pour le personnel informatique d'une entreprise, la charge de travail augmente considérablement.

La sensibilisation à la sécurité n'a jamais occupé une place aussi importante

Quel que soit le type ou la taille de l'entreprise, les problèmes liés à la cybersécurité sont souvent dus à une utilisation inappropriée des ressources informatiques par les salariés et à l'infection des appareils appartenant à l'entreprise par des logiciels malveillants. Cela signifie que, dans la plupart des cas, les entreprises pourraient réduire le risque d'atteintes à la protection des données en sensibilisant davantage leurs salariés à une utilisation sûre des ressources informatiques.

L'utilisation inappropriée des ressources informatiques par les salariés a une incidence sur 52 % des grandes entreprises et 50 % des PME

L'infection par des logiciels malveillants d'appareils appartenant à des entreprises a atteint 51 % pour les grandes entreprises et 49 % pour les PME

Les incidents résultant d'un partage inapproprié de données au moyen d'appareils mobiles représentent 48 % des incidents pour les grandes entreprises et 43 % pour les PME

Le taux d'infection d'appareils personnels par des logiciels malveillants atteint 48 % dans les grandes entreprises et 47 % dans les PME

Ce genre de comportement, et ces types d'incidents, **peuvent entraîner des coûts importants pour les entreprises…**

Les répercussions financières moyennes d'une atteinte à la protection des données causée par une utilisation inappropriée des ressources informatiques par les salariés s'élèvent à 116 000 $ pour les PME et à 1 195 000 $ pour les grandes entreprises

Quelle que soit la taille de l'entreprise, lorsqu'une attaque de cybersécurité se produit, les sanctions financières sont également variées : pénalités et amendes, augmentation des primes d'assurance, nécessité d'acheter de nouveaux logiciels, obligation d'effectuer des opérations de relations publiques et de mener des formations supplémentaires, et bien d'autres choses encore

Par exemple, en 2019, les conséquences financières moyennes d'une atteinte à la protection des données pour les entreprises comprenaient, entre autres, **182 000 $ pour l'amélioration et la restructuration de l'entreprise**, **140 000 $ pour les formations** et **161 000 $ pour le renforcement des relations publiques**.

Toutes les données utilisées dans ce document reposent sur le rapport de recherche « IT security economics in 2019 » de Kaspersky

« L'une des campagnes de spam les plus importantes que nous ayons enregistrées imite des envois de l'organisation mondiale de la santé. Les attaquants envoient des lettres au nom de l'OMS pour voler des données personnelles et organiser de faux dons pour lutter contre le coronavirus ».

Konstantin Ignatiev,
Responsable du groupe d'analyse du contenu Web de Kaspersky.

Répondre aux menaces actuelles et diverses

Il est clair que les entreprises doivent sérieusement chercher à réduire les risques d'atteinte à la protection des données, et c'est là qu'intervient la formation de sensibilisation à la sécurité.

Alors que **33 % des grandes entreprises** et **27 % des PME** ont connu un incident de sécurité, elles déclarent qu'elles prévoient d'investir davantage dans l'éducation et la formation à la sécurité des salariés afin d'éviter tout problème à l'avenir, en accordant la priorité aux formations parmi les autres mesures de cybersécurité. Il vaut toujours mieux prévenir que guérir.

Si vous avez déjà pensé à lancer une formation de sensibilisation à la sécurité, mais que vous avez mis cette idée de côté, c'est le moment d'agir. Dans un environnement international où toutes les actualités, chaque jour, sont axées sur la pandémie, les cybermenaces n'attendent qu'une opportunité.

Fin janvier de cette année, Kaspersky a découvert **32** fichiers malveillants diffusés sous forme de documents liés au coronavirus.

Il est temps d'agir

Il n'y a pas de temps à perdre. Commencez à former vos salariés aux problèmes de cybersécurité aujourd'hui afin de modifier leur comportement et protéger votre entreprise.

Mémo pour l'ensemble du personnel :

Voici un mémo que vous pouvez envoyer dès maintenant à vos salariés et spécialistes en informatique

- ☑ Organisez régulièrement des formations de sensibilisation à la sécurité.
- ☑ Assurez-vous que tous les appareils ayant accès aux réseaux et aux données de l'entreprise sont protégés par une solution de sécurité, idéalement gérée par un administrateur de l'entreprise.
- ☑ Assurez-vous que l'ensemble des informations confidentielles présentes sur les smartphones, les tablettes et les ordinateurs portables sont stockées sous forme chiffrée.
- ☑ Sécurisez votre réseau Wi-Fi domestique ! Modifiez votre mot de passe et configurez un réseau invité pour vos amis et ceux qui vous rendent visite en utilisant le plus haut niveau de chiffrement disponible.
- ☑ Configurez une authentification à deux facteurs.
- ☑ Utilisez un VPN.
- ☑ Soyez particulièrement vigilant : attention aux emails et aux sites de phishing.
- ☑ Si vous utilisez vos appareils personnels à des fins professionnelles, assurez-vous que le pare-feu et le logiciel antivirus sont installés et mis à jour, de même que les programmes et les systèmes d'exploitation.
- ☑ N'utilisez pas votre adresse email personnelle à des fins professionnelles. Tenez-vous-en aux ressources de l'entreprise lorsque vous échangez des documents et d'autres informations.

Fiche pratique pour vous aider à assurer la continuité de vos activités :

- ☑ Commencez par les règles simples et essentielles présentées ci-dessous pour réduire le risque de cyberincidents.
- ☑ Formez tous les salariés de votre entreprise en leur transmettant les compétences nécessaires en matière de cybersécurité. Bien entendu, nous vous recommandons vivement la formation Kaspersky Security Awareness. Une dizaine de minutes suffisent pour lancer le programme, et vos salariés pourront commencer à apprendre et à appliquer ces compétences essentielles dès le premier cours.
- ☑ Formez vos spécialistes informatiques généralistes en leur transmettant les compétences pratiques nécessaires pour reconnaître une éventuelle attaque et collecter des données relatives aux incidents grâce à la formation Cybersécurité pour les services informatiques en ligne (CITO).
- ☑ Laissez Kaspersky vous montrer comment gérer les communications de crise en cas d'incident de sécurité, notamment en concevant et en utilisant les ressources appropriées. La formation la plus avancée 'Communications d'incidents Kaspersky' permet aux cadres supérieur, et aux professionnels de la sécurité des informations et de la communication d'entreprise de coopérer efficacement lors d'un incident.

Actualités sur les cybermenaces :
www.securelist.com
Kaspersky Security Awareness :
kaspersky.fr/awareness
Essai gratuit : k-asap.fr

www.kaspersky.fr

© 2020 AO Kaspersky Lab.
Les marques déposées et les marques de service sont la propriété de leurs détenteurs respectifs.