KASPERSKY lab

CES MENACES QUI VIENNENT DE L'INTÉRIEUR

Comment sensibiliser vos employés à la cybersécurité pour protéger votre entreprise

L’humain est le maillon faible
de n’importe quelle organisation,
car il offre parfois aux cybercriminels
des moyens d’infiltrer votre entreprise.
Mais vos employés peuvent également
s’avérer être votre première et meilleure
ligne de défense.
Avec la mise en place d’un programme
solide de sensibilisation à la sécurité
informatique, votre entreprise sera
capable de protéger ses informations
les plus sensibles.

73%

Pourcentage des entreprises qui ont été confrontées à un incident de sécurité interne en 2015. Les principales menaces proviennent des vulnérabilités de logiciels et d'actions accidentelles des employés, y compris le partage ou la fuite de données par mégarde.[1]

Vos employés sont votre première ligne de défense

La plupart des sociétés considèrent leurs employés comme étant leur atout le plus précieux. Ils représentent le moteur de l'entreprise.

Parallèlement, la plupart des cybercriminels voient vos employés comme la solution de facilité. Une étude de Kaspersky Lab a récemment démontré que **42% des pertes de données confidentielles étaient dues aux employés**, il s'agit de la cause principale.[2] Les cybercriminels connaissent et exploitent cette faille au quotidien. S'ils veulent accéder aux informations de vos clients, aux documents de vos employés ou aux futurs plans de croissance, les tactiques d'ingénierie sociale visant les salariés sont souvent les méthodes les plus simples pour infiltrer une société.

Mes employés sont plus intelligents que ça.

La dure réalité est que des employés bien intentionnés menacent la sécurité de vos données au quotidien, en général sans qu'ils ne s'en rendent compte. Une étude a en effet récemment montré que 28% des employés avaient admis qu'ils avaient téléchargé un fichier contenant des données sensibles dans le Cloud.[3] Le tout combiné à un mot de passe peu sûr et à une attaque sous forme d'ingénierie sociale et même les meilleurs employés peuvent nuire à la sécurité de votre entreprise.
Dans le cas d'une fraude intentionnelle, où les employés utilisent pour leur propre intérêt les ressources et finances de l'entreprise, les petites et moyennes entreprises peuvent perdre jusqu'à 40 000$ en moyenne, tandis que ce chiffre pour les grandes entreprises dépasse les 1,3 million de dollars.[4]
Beaucoup d'employés ont une fausse impression concernant les problèmes de sécurité informatique ou croient qu'ils n'ont pas de rôle à jouer. En mettant en place un système de défense sur plusieurs niveaux comprenant la sensibilisation des employés, votre entreprise peut s'assurer que ces derniers comprennent l'importante responsabilité qu'ils ont à jouer concernant la protection des données et la sécurité de l'entreprise.

[1] « Enquête sur les risques informatiques mondiaux 2015 » rapport de Kaspersky Lab
[2, 4] The Threat Within: 3 Out Of 4 Companies Affected By Internal Information Security Incidents
[3] Humans: Still the weakest link in the enterprise information security posture"

21%

Pourcentage des entreprises affectées par des menaces internes, qui ont perdu des données de valeur, ce qui a eu des répercussions sur leurs affaires.[5]

Les questions de sécurité concernent toute l'échelle hiérarchique

Bâtir une culture d'entreprise fondée sur une prise de conscience de l'importance de la cybersécurité commence par le sommet de la pyramide hiérarchique.

Les conseils d'administration et cadres dirigeants doivent comprendre que s'ils négligent la cybersécurité, c'est à leurs risques et périls. La communication sur ce sujet est un élément fondamental pour la construction de cette culture.

Lors d'un récent sondage réalisé auprès de responsables de la sécurité informatique, 38% des entreprises ont indiqué que leur conseil d'administration encourage la sensibilisation des salariés à la sécurité des informations, en identifiant et en leur communicant les risques majeurs. 37 % ont signalé que la participation du Conseil d'administration mène à une augmentation du financement du programme de sécurité informatique.[6] Leur engagement fait la différence.

Avec un pourcentage de 43% de PDG considérant la cybersécurité comme étant essentielle à leurs entreprises[7], nul doute que les choses sont en train d'évoluer. Les failles de sécurité rendues récemment publiques ont certainement contribué à ce changement de mentalité. Il est important de s'appuyer sur cette prise de conscience en faisant de la sensibilisation une priorité à tous les niveaux, en maintenant les dirigeants informés des problèmes de sécurité informatique et leur faire comprendre le rôle qu'ils ont à jouer en sensibilisant et en informant leurs employés.

En d'autres termes, la cybersécurité ne concerne pas que les cadres. Sensibilisez tous vos employés et votre ligne de défense n'en sera que plus forte contre les menaces.

[5] *"Enquête sur les risques informatiques mondiaux 2015" rapport de Kaspersky Lab*

[6,7] *"The 2016 Global State of Information Security Survey", en partenariat avec PwC, CIOmagazine, CSO, Octobre 2015*

31%

Pourcentage des cyberattaques ayant visé des entreprises de moins de 250 employés, selon le département de la Sécurité intérieure des États-Unis.

Toutes les entreprises, quelle que soit leur taille, sont une cible

Les cybercriminels se moquent de qui vous êtes. Que vous soyez une petite société de 100 personnes ou un fournisseur de service de taille moyenne (SaaS). A partir du moment où vous avez accès aux données d'une grande entreprise, vous devenez une cible principale.

Dans de nombreux cas, les petites entreprises sont fournisseurs de grandes entreprises et ainsi ont accès à des informations confidentielles privilégiées. De plus, beaucoup de petites entreprises n'ont pas le temps ou les ressources pour combattre les menaces de sécurité. Etant donné que les grandes entreprises continuent de bâtir leur périmètre de sécurité et de sensibiliser leurs employés sur ce qu'il faut éviter, les petites et moyennes entreprises deviennent les cibles des cybercriminels en quête de vulnérabilités.

Avec un coût moyen estimé à 38 000$ pour les petites et moyennes entreprises, la plupart ne sont pas préparées face à la perte d'une telle somme causée par une fuite de données.[8]

Que peuvent donc faire les petites et moyennes entreprises pour minimiser les risques ?

En mettant en place une stratégie de sécurité sur plusieurs niveaux qui prend en compte les technologies dont elles ont le plus besoin, tout comme prévoir du temps et des ressources nécessaires à la sensibilisation des employés, les petites entreprises peuvent s'assurer qu'elles ne seront pas la porte ouverte à des fuites importantes de données de leurs clients.

[8] *"Enquête sur les risques informatiques mondiaux 2015", rapport de Kaspersky Lab*

60%

60%. Pourcentage des entreprises qui ont vu leur fonctionnement sévèrement affecté suite à une faille de sécurité.[9]

Les méthodes d'attaques fréquentes

La créativité est l'arme secrète des cybercriminels.

Chaque année, Kaspersky Lab identifie toujours plus de tactiques innovantes utilisées par les cybercriminels pour obtenir des informations sur votre entreprise par le biais de vos employés. Jetons un coup d'œil aux méthodes les plus répandues, et que chacun de vos employés devraient connaître.

L'ingénierie sociale

La confiance est la monnaie sur laquelle l'ingénierie sociale est fondée. Elle piège les employés en les poussant à rompre les procédures normales de sécurité, une méthode efficace qui s'est avéré la cause principale de nombreuses attaques récentes de grandes entreprises. Beaucoup d'employés partent du principe qu'ils sont protégés de ces types d'attaques ciblées lorsqu'ils utilisent leur ordinateur de bureau. Nous recommandons d'adopter une approche « Faites confiance, mais vérifiez ». Les employés doivent se sentir en toute confiance au moment d'utiliser l'équipement de leur entreprise, cependant si quelque chose demeure suspect, ils doivent suivre leur instinct et alerter leurs collègues du service informatique.

Phishing

La majorité des attaques ciblées sont diffusées via des e-mails adressés aux employés. Les hackers essayent de les piéger en leur faisant ouvrir des e-mails de phishing dans le but de cliquer sur des liens dangereux. Les attaques ciblées qui ont récemment été rendues publiques, ont affecté des dizaines de millions d'utilisateurs et ont en général commencé par le biais d'un simple e-mail envoyé aux employés. Bien que ces attaques ne soient pas très sophistiquées, elles ont été incroyablement fructueuses en infectant des entreprises tous secteurs confondus.

Dites à vos employés d'être en alerte et qu'ils se posent certaines questions, telles que :

- Est-ce que l'e-mail indique une URL mais se réfère en réalité à une autre ?
- Est-ce que le message demande des informations personnelles ?
- Est-ce que les informations en en-tête correspondent bien à l'expéditeur ?

En étant en alerte et en contactant le service informatique, les employés peuvent arrêter des menaces préjudiciables avant qu'elles ne franchissent le seuil de votre entreprise.

Les attaques de point d'eau

L'idée même de l'attaque de point d'eau est de trouver et d'infecter les sites que les employés visitent le plus souvent. Lorsqu'un employé ouvre un site infecté, le code injecté dans le corps de la page redirige le navigateur vers un site malveillant contenant un kit d'Exploits. La plupart des employés sont surpris d'apprendre qu'il ne suffit que d'une simple visite sur un site pour être infectés. Cliquer sur « Autoriser » ou « Confirmer » exécute souvent le code malveillant et dissimule l'attaque à l'équipe de sécurité informatique.

[9] *"Enquête sur les risques informatiques mondiaux 2015", rapport de Kaspersky Lab*

36%

Pourcentage des entreprises qui ont subi un piratage de mobile en 2015.[10]

La sécurité du BYOD (Bring your own device)

Trouver le juste milieu entre les préférences des employés concernant les dispositifs de l'entreprise et la sécurité informatique n'est pas chose facile. Un facteur clé entre en jeu : l'engagement des employés vis-à-vis de la politique de sécurité.

Une récente étude a démontré que plus de 60% des employés des petites et moyennes entreprises utilisent des téléphones de l'entreprise pour travailler depuis chez eux ou lorsqu'ils sont en voyage. De plus, 94% des employés ont indiqué qu'ils connectaient leur ordinateur portable ou leur mobile à des réseaux Wi-Fi non sécurisés lorsqu'ils se trouvaient en déplacement.[11]

Les produits de sécurité mobile de Kaspersky Lab ont détecté une augmentation par 3 des programmes malveillants entre le 1er et le 3ème semestre 2015. Avec le phénomène du BYOD devenant la norme dans la majorité des entreprises, ce nombre est en passe d'augmenter et les cybercriminels en saisiront les opportunités.

Manifestement, les employés ont besoin de comprendre les risques pour permettre de les limiter. Les entreprises quant à elles doivent prévoir le temps et les ressources nécessaires. En sensibilisant vos employés à la sécurité mobile et en mettant en place la technologie adéquate, votre entreprise pourrait éviter d'être la nouvelle cible d'entrée des cybercriminels.

Lors d'une récente étude menée auprès de responsables de la sécurité informatique dans des grandes entreprises, **les appareils mobiles représentent le domaine touché par le plus grand nombre d'incidents de sécurité en 2015**.[12]

[10, 12] *"The 2016 Global State of Information Security Survey", en partenariat avec PwC, CIOmagazine, CSO, Octobre 2015*

[11] *Small and Midsized Businesses Learn to Protect Their Digital Assets During National Cyber Security Awareness Month*

87%

Pourcentage des incidents dus aux pertes de données qui ont requis une aide supplémentaire de la part de professionnels tiers, y compris de consultants en sécurité, d'avocats et de cabinets en gestion des risques.[13]

Construire son programme de sensibilisation

La sensibilisation des employés vis-à-vis de la cybersécurité n'est pas à prendre à la légère. Il s'agit de l'élément fondamental de la prévention. Un pourcentage clé montre que pour 56% des entreprises victimes de pertes de données, un tel incident a terni leur image et leur réputation[14] , les risques associés à la passivité sont immenses et durables.

La meilleure façon de commencer est de tenir informée le plus possible votre équipe informatique concernant les tendances actuelles et les risques pour ensuite mettre en place certaines règles essentielles, telles que :

- ✓ S'assurer que tous les utilisateurs connaissent et appliquent la politique de sécurité de l'entreprise
- ✓ Informer les utilisateurs des éventuelles conséquences des menaces répandues sur Internet, telles que le phishing, l'ingénierie sociale et les sites malveillants
- ✓ Enseigner aux utilisateurs de faire appel à l'équipe informatique pour signaler n'importe quel incident
- ✓ Garder le contrôle sur les droits d'accès des utilisateurs et les privilèges, ils ne doivent être donnés qu'en cas de nécessité
- ✓ Enregistrer tous les droits et privilèges accordés aux utilisateurs

- ✓ Analyser les systèmes et réseaux non utilisés à la recherche de vulnérabilités
- ✓ Détecter et analyser les réseaux et les applications vulnérables
- ✓ Mettre à jour les applications et composants vulnérables. Non actualisé, un logiciel vulnérable pourrait être restreint ou interdit

Plusieurs de ces mesures peuvent être automatiques. Par exemple, si la politique de sécurité est enfreinte, un message d'avertissement est affiché. La technologie des systèmes de gestion peut être utilisée pour chercher des réseaux ou des dispositifs non autorisés, ainsi que des vulnérabilités et mises à jour automatiques d'applications vulnérables.

[13, 14] *"Enquête sur les risques informatiques mondiaux 2015", rapport de Kaspersky Lab*

ESSAYEZ KASPERSKY LAB

Découvrez comment Kaspersky Lab peut protéger votre entreprise contre les malwares et la cybercriminalité grâce à notre version d'essai. Téléchargez la version complète de nos produits et découvrez comment ils protègent avec succès les infrastructures informatiques, les postes de travail ainsi que les données confidentielles.

RECEVEZ VOTRE VERSION GRATUITE AUJOURD'HUI

REJOIGNEZ-NOUS

Regardez-nous sur YouTube

Aimez notre page sur Facebook

Consultez notre blog

Suivez-nous sur Twitter

Rejoignez-nous sur LinkedIn

Pour en savoir plus :
http://www.kaspersky.fr/business-security/small-to-medium-business

À PROPOS DE KASPERSKY LAB

Kaspersky Lab est l'une des plus grandes entreprises privées mondiales spécialisées en cybersécurité. La société fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité pour les utilisateurs de terminaux informatiques (IDC, 2014). Depuis 1997, Kaspersky Lab fait figure de précurseur dans le domaine de la sécurité informatique, fournissant des solutions de sécurité numérique efficaces aux grandes entreprises, PME et particuliers. Kaspersky Lab est une entreprise internationale qui opère actuellement dans près de 200 pays et territoires du monde entier et protège plus de 400 millions d'utilisateurs.

Contactez Kaspersky Lab dès aujourd'hui pour en savoir plus sur Kaspersky Endpoint Security for Business et nos autres solutions et services de sécurité informatique
kaspersky.fr/business-security/small-to-medium-business
marketing@kaspersky.fr

© 2016 AO Kaspersky Lab. Tous droits réservés. Les marques déposées et marques de services appartiennent à leurs propriétaires respectifs. .

KASPERSKY lab
LE POUVOIR DE PROTÉGER