kaspersky

Livre blanc

La sensibilisation des collaborateurs à la sécurité informatique.

Il est temps d'ouvrir les yeux !

#truecybersecurity
www.kaspersky.fr

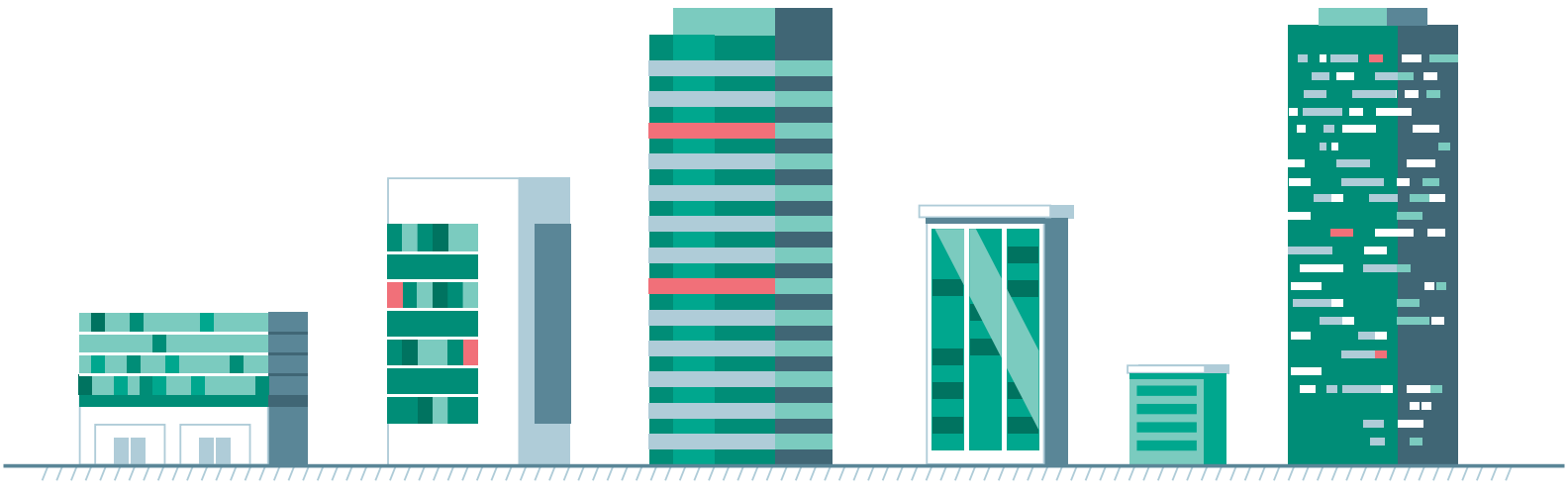
Introduction

Le facteur humain est un enjeu majeur de la cybersécurité en entreprise : faites de vos salariés les 1ers remparts de l'entreprise contre les menaces.

Au cours des dernières années, la plupart des organisations ont installé des filtres anti-phishing avancés et des pare-feux, et déployé des outils spécialisés pour atténuer les cybermenaces. Les cybercriminels ont donc déporté une partie de leurs attaques directement sur les salariés, considérés comme un possible point d'entrée dans les systèmes informatiques.

Découvrez dans ce livre blanc les différentes techniques utilisées par les cybercriminels pour tenter d'infiltrer les entreprises en utilisant les faiblesses de leurs salariés, mais également les conseils de nos experts pour mettre en place des méthodes simples et pratiques à utiliser au quotidien.

Sommaire



1. Pourquoi une prise de conscience de la direction sur l'importance de la sensibilisation à la cybersécurité est-elle primordiale ?

- Chiffres clés sur les cybermenaces ciblant les entreprises

Selon une étude d'IBM[1], l'erreur humaine est impliquée dans plus de 90 % des incidents de sécurité (clic sur un lien de phishing, consultation d'un site Web suspect, activation de virus ou autres menaces persistantes avancées).

L'enquête réalisée en 2017 par Kaspersky Lab et B2B International[2] appuie ces conclusions. Selon ce rapport, l'utilisation inappropriée des ressources informatiques par les salariés est à l'origine des attaques subies par 39 % des organisations mondiales sur une période de 12 mois.

Plus de 90 % des incidents de sécurité dus à une erreur humaine

L'augmentation du nombre de cyberincidents provoqués par des erreurs humaines est surtout perceptible dans le secteur des Très Petites Entreprises (TPE) : en un an seulement, le pourcentage de petites entreprises (1 à 49 salariés) victimes d'une attaque impliquant une erreur humaine est passé de 25 à 32 % [2].

Plus préoccupant encore, près de la moitié des entreprises (entre 44 et 48 % [2]) ne se sentent pas correctement protégées contre les menaces que font courir l'ignorance, la naïveté ou la malice de leurs propres salariés.

1. L'indice relatif à la veille stratégique en matière de sécurité d'IBM
2. Source : « Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within » (« Facteur humain dans la sécurité informatique : Comment les employés rendent les entreprises vulnérables de l'intérieur »), juin 2017

- Que risquent les entreprises ?

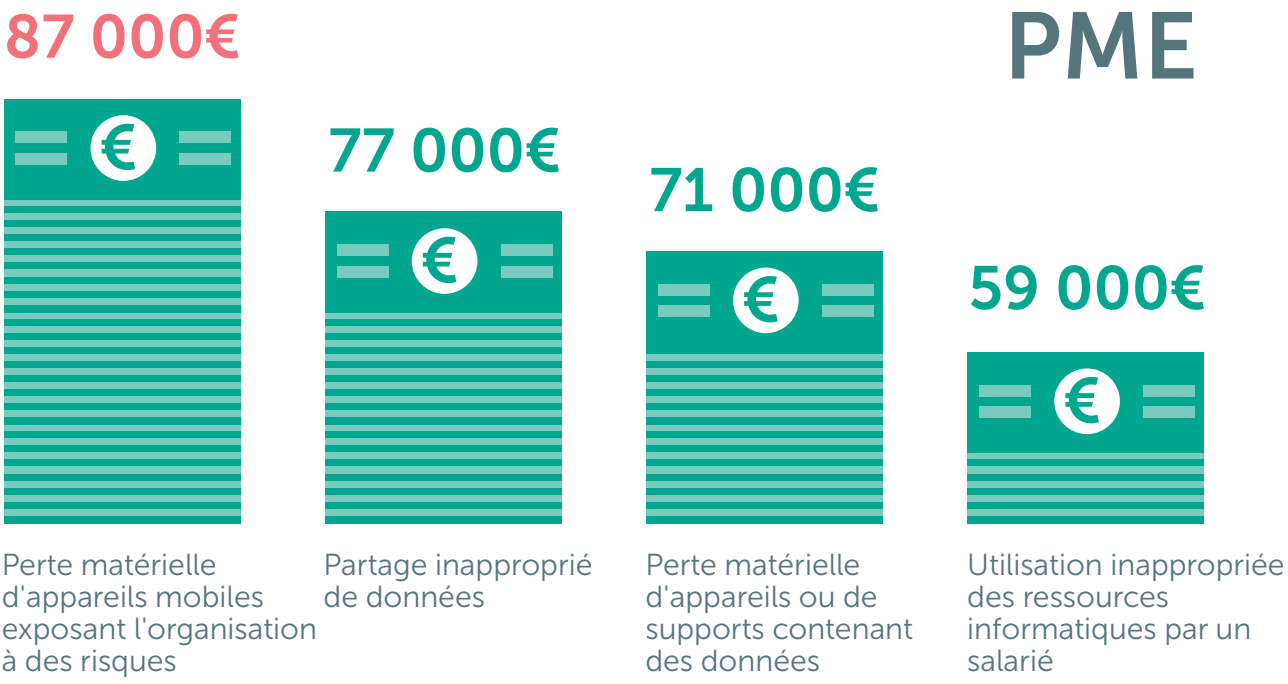
1. Perdre de l'argent

Les cybercriminels réclament souvent une rançon contre la restitution des données. Précision : Kaspersky Lab déconseille aux entreprises infectées de payer les rançons. Premièrement, il n'est nullement garanti que les cybercriminels respectent leur parole et déchiffrent vos données. Deuxièmement, plus ils gagnent d'argent, plus ils sont susceptibles de recommencer. Enfin, les agences de sécurité et les organes de répression travaillent avec acharnement pour trouver et publier des clés de déchiffrement valides[1], il est donc intéressant de rechercher d'éventuelles solutions sur Internet avant de débourser le moindre centime.

De plus, le coût réel d'une attaque doit prendre en compte également les dommages collatéraux dûs à la perturbation temporaire de l'activité de l'entreprise ou à la perte définitive de leurs données :

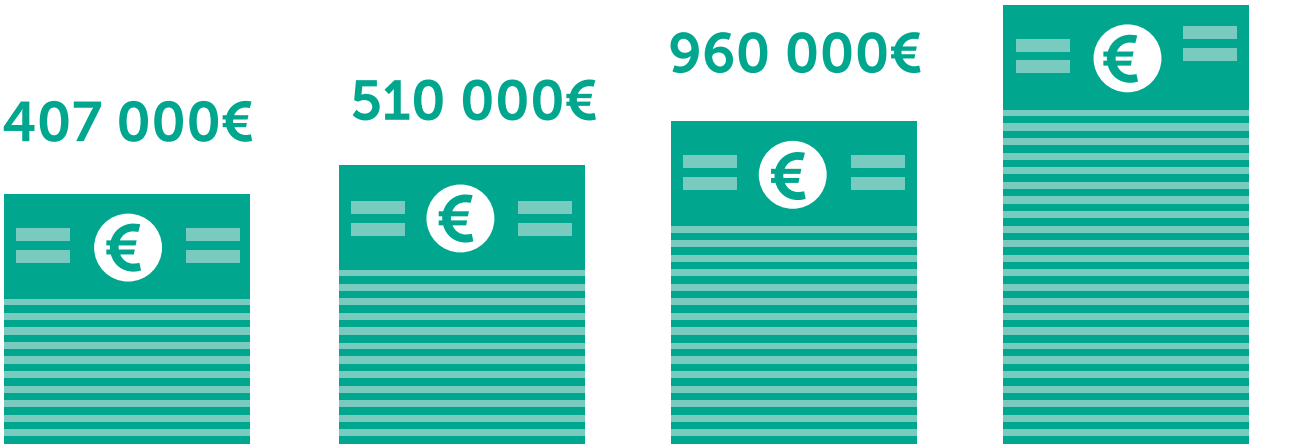
- Impact sur les ventes
- Diminution de la productivité
- Coûts liés à la récupération du système (recrutement de personnel expérimenté ou d'experts externes...)

L'enquête Kaspersky Lab/B2B International[1] nous a permis de calculer l'impact financier moyen des actions inappropriées des salariés :



1. « Rapport de l'enquête sur les risques informatiques mondiaux 2017 ». Kaspersky Lab et B2B International *par exemple : https://go.kaspersky.com/Anti-Ransomware-tool-web-site.html

Grandes entreprises 1,4 M€



Partage inapproprié de données via des appareils mobiles

Utilisation inappropriée des ressources informatiques par un salarié

Perte matérielle d'appareils ou de supports contenant des données

Incidents impliquant des objets connectés

2. La perte permanente de données peut avoir des conséquences encore plus graves :

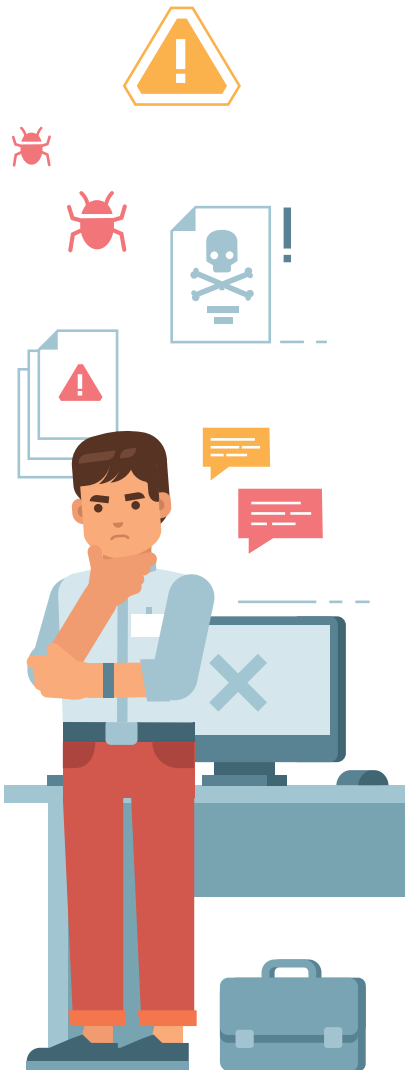
- Nuire de façon permanente à la position concurrentielle de l'entreprise
- Nuire à la réputation de l'entreprise
- Réduire le carnet de commandes à long terme
- Empêcher l'accès permanent à la propriété intellectuelle et aux données de conception et même mettre en péril l'ensemble de l'entreprise

Imaginez perdre l'accès à tous vos registres de ventes, aux dossiers des clients, aux données comptables, aux informations produits et aux données de conception. Comment votre entreprise pourrait-elle faire face à cette situation ? Et, si elle y fait face, quel montant de chiffre d'affaires perdriez-vous pendant que votre équipe tente de tout remettre sur la bonne voie ? Il est clair que chaque entreprise doit faire tout son possible pour éviter de devenir une autre victime d'une attaque de cryptovirus.

3. Méfiez-vous des faux remèdes

Si votre entreprise est attaquée, méfiez-vous des « faux remèdes » qui peuvent être diffusés sur Internet, car ils pourraient s'ajouter à vos problèmes :

- Souvent, ils ne fonctionnent pas, mais prennent juste plus d'argent à la victime
- Certains peuvent même télécharger d'autres programmes malveillants sur le réseau de la victime



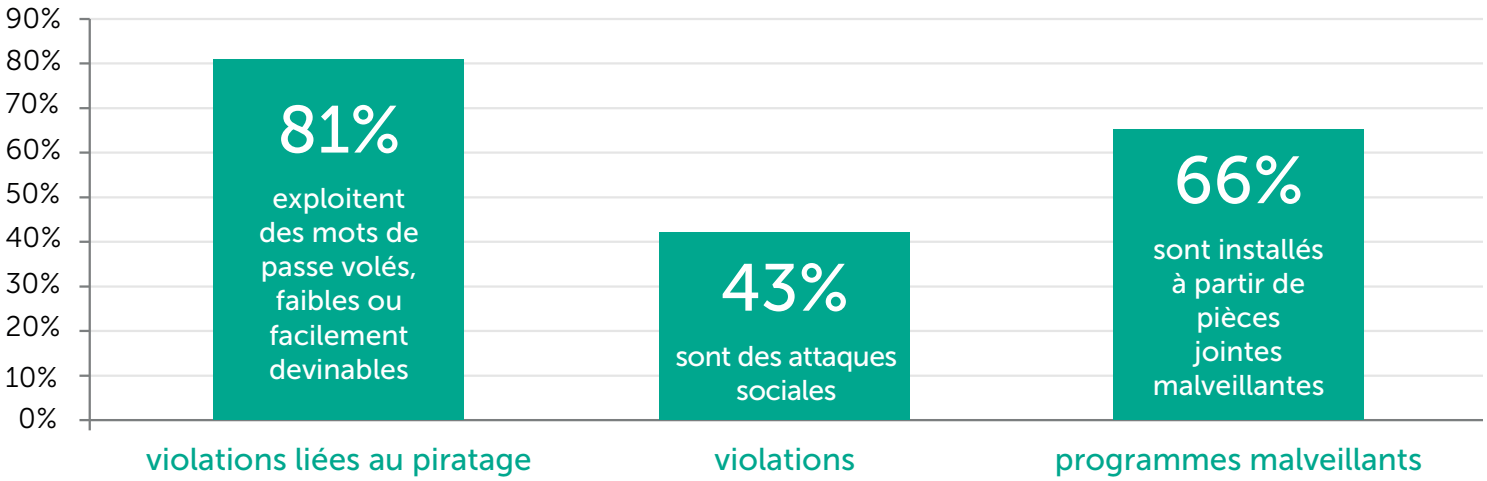
2. Qui les criminels ciblent-ils et pourquoi ?

- Tous les salariés

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 violations de données en chiffres[1]

- 81% des violations liées au piratage exploitent des mots de passe volés, faibles ou facilement devinables.
- 43% des violations sont des attaques sociales.
- 66% des programmes malveillants sont installés à partir de pièces jointes malveillantes.



Lors d'un récent sondage[2] 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. Leur engagement fait la différence.

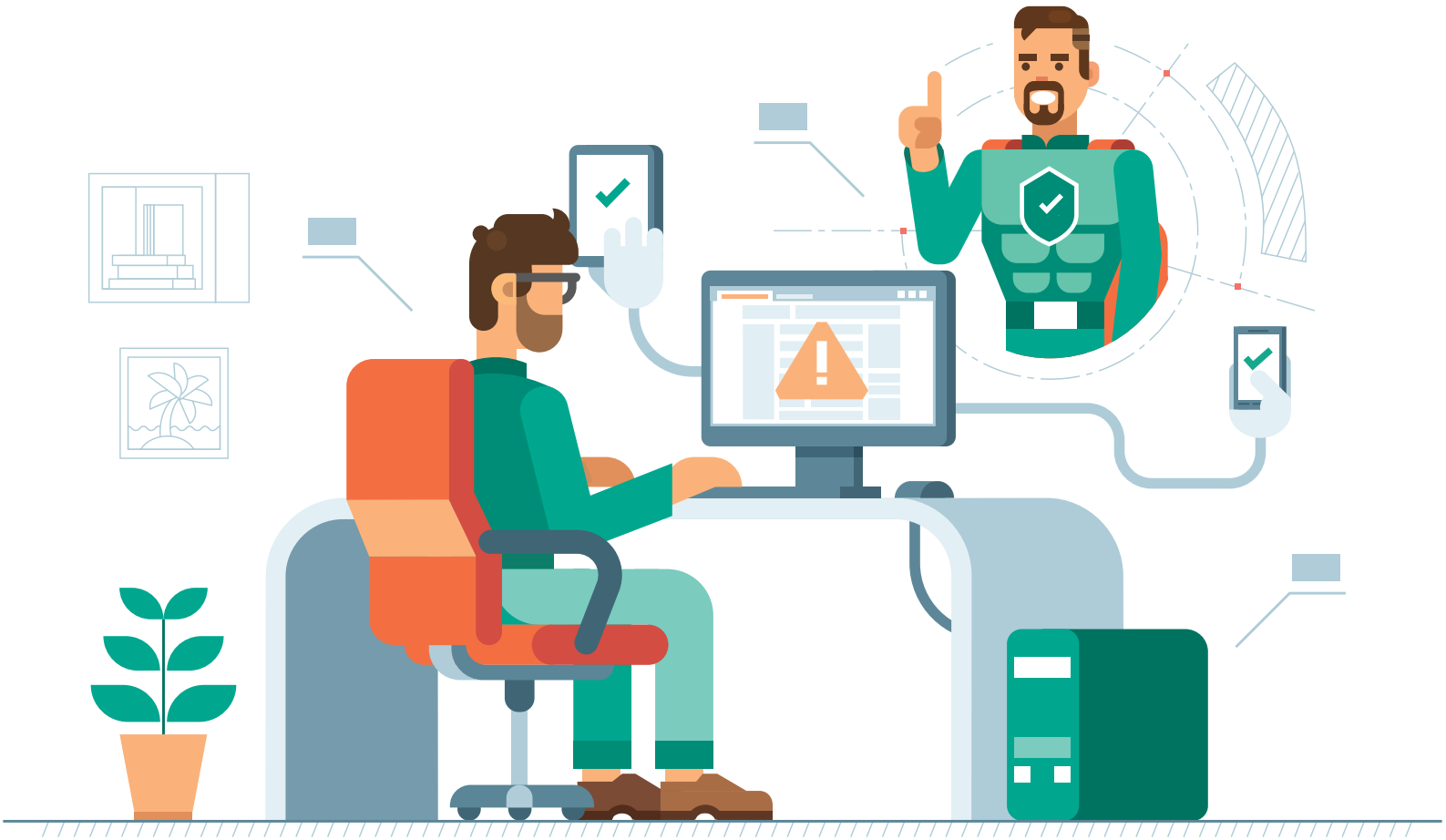
1. « Rapport 2017 d'enquêtes sur la violation des données », Verizon
2. "Enquête sur les risques informatiques mondiaux 2015" rapport de Kaspersky Lab

43 % des PDG considèrent la cybersécurité comme essentielle

Avec un pourcentage de 43% de PDG considérant la cybersécurité comme étant essentielle à leur entreprise[3], 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 en leur faisant comprendre le rôle qu'ils ont à jouer en sensibilisant et en informant leurs salariés.

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



3. "The 2016 Global State of Information Security Survey", en partenariat avec PwC, CIOmagazine, CSO, Octobre 2015

- Toutes les entreprises

Les entreprises de moins de 1000 salariés sont majoritairement les victimes de violation de données.

61% des victimes de violation de données signalées dans le rapport 2017 sont des entreprises de moins de 1 000 salariés[1].

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. 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 mettre en place une sécurité robuste.

Comme les grandes entreprises continuent de bâtir leur périmètre de sécurité et de sensibiliser leurs salariés sur ce qu'il faut éviter, les petites et moyennes entreprises deviennent les cibles des cybercriminels en quête de vulnérabilités.

Avec un coût moyen pour une fuite de données estimé à 33 000€ pour les petites et moyennes entreprises, la plupart ne sont pas préparées face à la perte d'une telle somme[2].

Que peuvent donc faire les TPE/PME 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 salariés, les petites entreprises peuvent s'assurer qu'elles ne laisseront pas fuire les données de leurs clients.

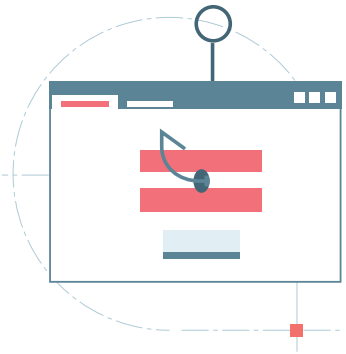
1« Rapport 2017 d'enquêtes sur la violation des données », Verizon [2]"Enquête sur les risques informatiques mondiaux 2015", rapport de Kaspersky Lab

3. Techniques utilisées par les cybercriminels

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 votre personnel ou de vos collègues. Jetons un coup d'œil aux méthodes les plus répandues, et que chacun des salariés de votre entreprise devraient connaître.

- Phishing / Ransomware



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

En pratique, l'utilisateur reçoit un email avec un contenu qui en apparence émane d'une institution telle qu'une banque, les impôts, la CAF ou encore un fournisseur d'accès à Internet. L'utilisateur est invité à effectuer une opération de type changement de mot de passe ou encore activation de compte, mais le site web vers lequel il est dirigé est en fait une copie frauduleuse du site institutionnel.
Le salarié néophyte en informatique ne sait pas faire la différence entre un email frauduleux et une communication officielle et communiquera volontairement les informations requises.
Les banques, les boutiques en ligne et les systèmes de paiement restent les organisations les plus ciblées par ce type d'attaque.

Dites à vos salariés 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 de l'en-tête correspondent bien à l'expéditeur ?

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

- Récupération de mots de passe (trop simples)

Environ 90 %[1] des mots de passe sont vulnérables face au piratage. Beaucoup de gens utilisent des mots de passe trop simples, en pensant que personne n'essaiera d'accéder à leur compte, mais ils se trompent. N'importe quel compte peut être piraté, même si son titulaire pense ne pas représenter un intérêt suffisant pour être ciblé.

Les cybercriminels utilisent des ordinateurs pour tenter de deviner votre mot de passe à raison de milliers de tentatives par minute. Les programmes qui devinent les mots de passe utilisent des dictionnaires prêts à l'emploi et des combinaisons simples de lettres et de chiffres. Les mots de passe longs constitués d'une combinaison de nombres, de symboles et de lettres majuscules et minuscules sont plus difficiles à deviner !

Une fois qu'une personne mal intentionnée détient votre mot de passe, elle peut :

- Emprunter de l'argent auprès de vos amis en votre nom
- Envoyer des malwares à vos contacts
- Publier quelque chose de douteux sur votre page
- Ou même retirer de l'argent de votre compte bancaire.

Il est donc important de savoir comment utiliser les mots de passe de façon adéquate : il doit être suffisamment complexe et à usage unique. En effet, un utilisateur utilisant le même mot de passe pour ses comptes personnels et professionnels pourrait donner accès au réseau de l'entreprise.

- L'ingénierie sociale

La confiance est la ase sur laquelle l'ingénierie sociale est fondée. Elle piège les salariés 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 de salariés partent du principe qu'ils ne seront jamais la cible de telles attaques.

En effet, les salariés se sentent en confiance au moment d'utiliser l'équipement de leur entreprise (c'est à l'entreprise de se doter de solutions de sécurité robustes) cependant, si quelque chose leur semble suspect, ils doivent suivre leur instinct et alerter leurs collègues du service informatique.

L'ingénierie sociale est un type d'atteinte à la sécurité que les escrocs utilisent pour inciter des personnes à leur communiquer des données permettant d'accéder à des informations sensibles. Les auteurs d'attaques d'ingénierie sociale ont le même objectif que les pirates, mais leur action consiste à tromper leurs victimes plutôt qu'à pénétrer les réseaux.
Parfois, les escrocs parviennent à obtenir les informations recherchées en les demandant tout simplement à leurs victimes.

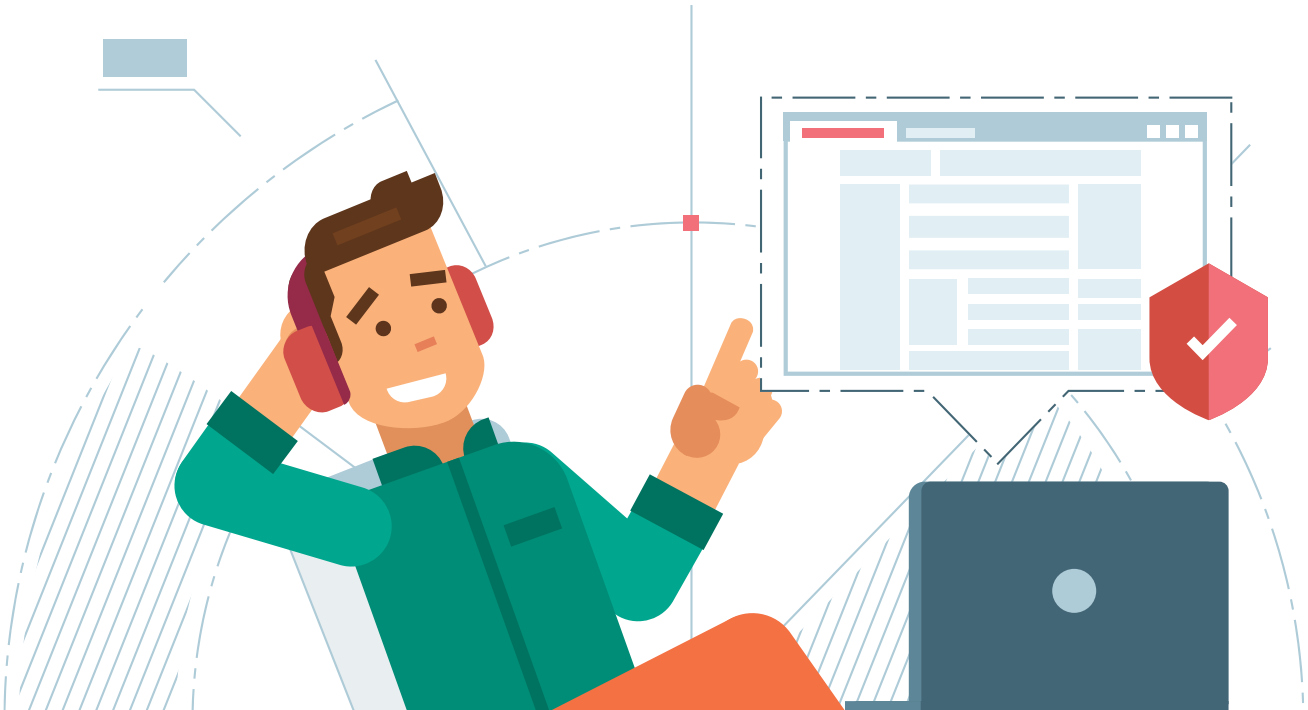
1. Globat IT Risk survey 2014 / Kaspersky Lab, rapport de vulnérablités 2013

- Infection de sites Internet légitimes

Les infections de sites Internet en masse sont devenues l'un des plus grands problèmes auxquels le secteur informatique doit faire face. Pour avoir une idée de son ampleur, il suffit de prendre le nombre de requêtes adressées à notre service d'assistance technique au sujet d'avertissements relatifs à des sites malveillants. En général, les propriétaires des sites Internet se plaignent du blocage erroné de leur site par nos produits et affirment qu'il doit s'agir d'un faux positif car ils n'hébergent aucun contenu malveillant. Malheureusement, ils se trompent dans la majorité des cas et leurs sites renferment bel et bien des scripts malveillants qui ont été injectés dans le code PHP, JS ou HTML d'origine par les auteurs des attaques. En règle générale, ces scripts redirigent les visiteurs du site vers des URL malveillantes où des programmes malveillants attendent d'être téléchargés et exécutés sur l'ordinateur de la victime. Dans la majorité des cas, la victime ne remarque rien de l'exécution du programme malveillant et ne voit qu'un site Internet qui semble fonctionner normalement.

- Création de sites Internet frauduleux (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 salariés visitent le plus souvent. Lorsqu'un salarié 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 salariés 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.



- Exploitation des vulnérabilités des applications

La plupart des entreprises sont maintenant équipées d'une solution d'automatisation de l'installation des mises à jour Microsoft Windows, avec un système de type WSUS.
Cependant peu d'entreprises disposent de solutions de mises à jour des applications tierces telles qu'Adobe Reader, Flash Player, Java ou encore des navigateurs tiers. Or des failles de sécurité sont fréquemment découvertes dans ces applications et les vulnérabilités sont exploitées par des codes malveillants.
Lorsque l'utilisateur dispose de tous les privilèges sur son système, ce qui en soit est déjà un problème de sécurité, on ne peut pas compter sur lui pour mettre à jour ces applications tierces.

L'inaction de l'utilisateur face aux mises à jour proposées est exploitée comme faiblesse pour que les auteurs de codes malveillants parviennent à leur objectif.

Les pirates profitent du fait que les utilisateurs ne désinstallent pas les applications qui ne sont plus supportées, donc plus mises à jour mais qui fonctionnent toujours. De nombreux utilisateurs installent en effet une application, puis l'oublient.

- Exploitation de failles des réseaux WIFI

Le WiFi gratuit est un point chaud pour les criminels

Les escrocs peuvent pirater les connexions WiFi à accès ouvert et espionner vos activités en ligne. Si vous ne prenez pas des précautions en matière de sécurité, les criminels peuvent voir vos noms d'utilisateurs, mots de passe, courriels et d'autres informations confidentielles.

Les hotspots WiFi sont partout

Une connectivité gratuite et pratique peut être tentante.

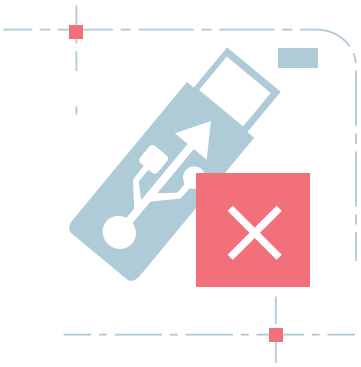
De nombreux salariés sont équipés de périphériques mobiles tels que des smartphones ou des tablettes, depuis lesquelles ils consultent leur messagerie et échangent des données personnelles ou professionnelles.

Plusieurs dangers guettent les utilisateurs :

1. Avec la mise à disposition de WiFi gratuit dans les lieux publics, les salariés sont tentés d'envoyer des emails professionnels et de partager des informations sensibles.
2. La valeur de ces périphériques en fait un objet recherché et donc parfois volé. Il arrive aussi que le salarié égare son matériel, ce qui peut aussi engendrer de la perte d'informations confidentielles.

Si l'utilisation d'un WIFI gratuit est indispensable, veillez à utiliser un VPN. Il vous permettra de chiffrer le trafic entre votre appareil et les sites que vous visiterez.

- Infection via des périphériques amovibles



Souvent, le salarié connecte ses périphériques personnels sur diverses machines en dehors de l'entreprise, ces ordinateurs pouvant être infectés par des codes malveillants développés pour se propager automatiquement sur tous nouveaux périphériques amovibles connectés.

Lors de la connexion du périphérique infecté sur le réseau de l'entreprise, le malware infecte automatiquement la machine hôte et a ensuite la possibilité de se propager sur les autres machines.

Le virus Stuxnet s'est initialement introduit dans des installations nucléaires iraniennes via une clé USB, avant de se propager dans des installations russes de la même manière. Des programmes malveillants ont même été détectés dans une station spatiale internationale.

Kido, autrement connu sous les noms de Conficker et Downadup est un malware qui exploitait notamment les périphériques amovibles pour se propager. Il a causé des dégâts importants en entreprise et persiste encore dans certaines d'entre elles à ce jour.

- Arnaque au Président

Le faux ordre de virement (FOVI) est devenu, depuis peu, l'arnaque la plus redoutable en France pour les entreprises. Cette escroquerie en plein essor aurait permis de détourner quelques 250 millions d'euros depuis 2010. L'art du FOVI consiste à abuser un salarié ou un assistant comptable afin d'exiger un virement bancaire.

Quelques
250 millions
d'euros détournés par le
FOVI depuis 2010

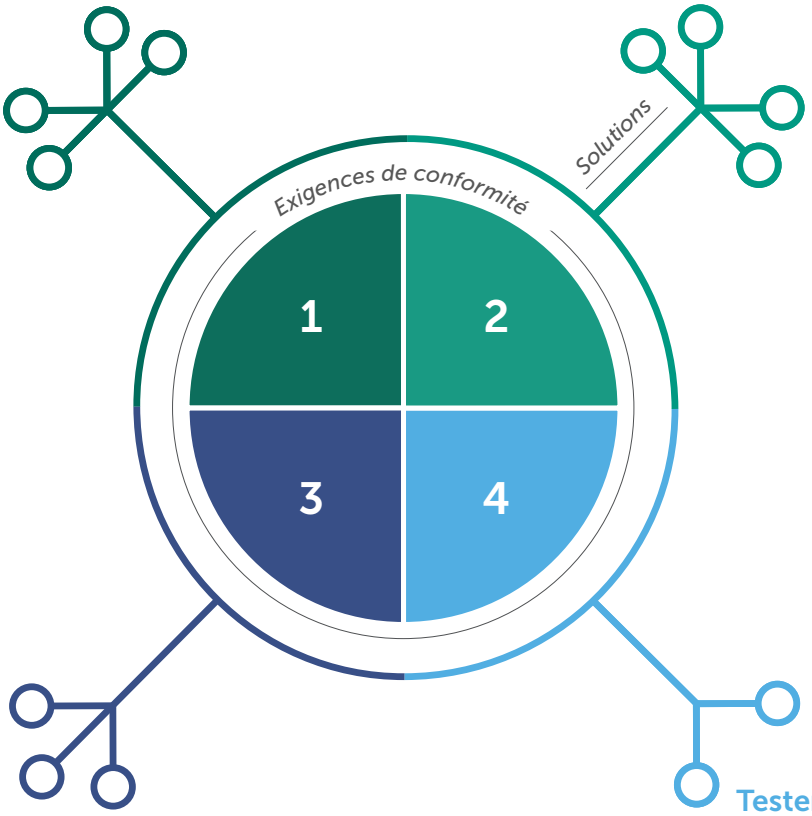
Afin de rassurer les entreprises ciblées, les voleurs créent un compte bancaire sur le site internet La Poste afin d'utiliser le service payant de la lettre recommandée. Ce compte, créé sous une fausse identité, leur permet de régler des envois postaux et ainsi faire parvenir aux entreprises ciblées un courrier matérialisé. Les escrocs n'hésitent pas à créer une véritable structure juridique afin de paraître plus crédibles, tel a été le cas pour l'attaque sur Google.

4. Ces différentes menaces imposent aux entreprises d'importants challenges

- Mettre en place la solution de sécurité la plus adaptée aux besoins de votre entreprise
- Déterminer quels sont vos besoins en matière de formation et quels résultats vous en attendez
- La réglementation RGPD impose également de respecter certains principes

Proposer des formations de sensibilisation

Détecter les attaques aussi vite que possible



Signaler toute attaque aux régulateurs dans un délai de 72 heures

Tester les mesures, y accéder et évaluer leur efficacité de manière régulière

5. 10 règles simples à mettre en place dans votre entreprise

Nos experts vous proposent 10 règles simples, de bon sens, à mettre en place, pour protéger votre entreprise de façon efficace :

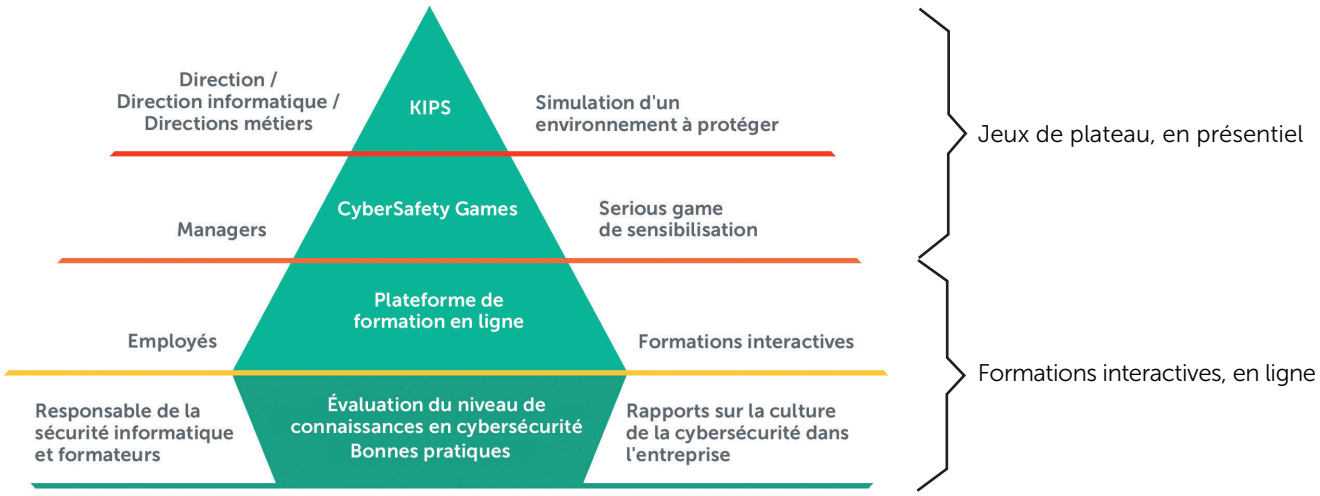
1. Installez une solution de sécurité fiable et utilisez toutes ses fonctionnalités, notamment la recherche de vulnérabilités, le déploiement automatique des patchs et la détection rapide des virus.
2. Protégez les salariés partout où ils travaillent. Avec le développement du travail mobile, appliquer des mesures de sécurité au seul matériel présent au bureau n'est plus suffisant.
3. Rédigez de façon claire et précise une politique de sécurité interne et communiquez-la largement (mails, réunions d'information, affichage dans les locaux).
4. Éliminez toute situation pouvant laisser la place aux comportements à risque : interdisez les applications non répertoriées (bloquer par défaut les applications inconnues).
5. Sensibilisez vos collaborateurs au fait qu'ils travaillent pour une entreprise dont les données et les informations ont beaucoup de valeur sur le marché noir de la cybercriminalité, par la communication et la formation.
6. Précisez les conséquences éventuelles d'une attaque : demande de rançon, vol de données sensibles, coût de récupération des systèmes...
7. Enseignez aux utilisateurs à faire appel à l'équipe informatique pour signaler n'importe quel incident
8. Réalisez des simulations d'attaques de phishing pour tester la réactivité de vos collaborateurs à ces types d'attaques.
9. N'affichez pas la liste de tous les salariés sur le site Web de votre entreprise.
10. Formez votre personnel aux menaces informatiques, à l'aide de cas concrets, facilement applicables dans leur quotidien

Nous vous proposons un exemple de poster sur les bonnes pratiques de sécurité, que vous pourriez afficher dans les lieux de passage de votre entreprise.

Télécharger le poster

6. Les solutions proposées par Kaspersky Lab

Des formations pour tous les profils de l'entreprise, sous forme de jeux de plateau ou de formations interactives en ligne.



Testez notre nouvelle plateforme de formation en ligne : Kaspersky Automated Security Awareness Platform

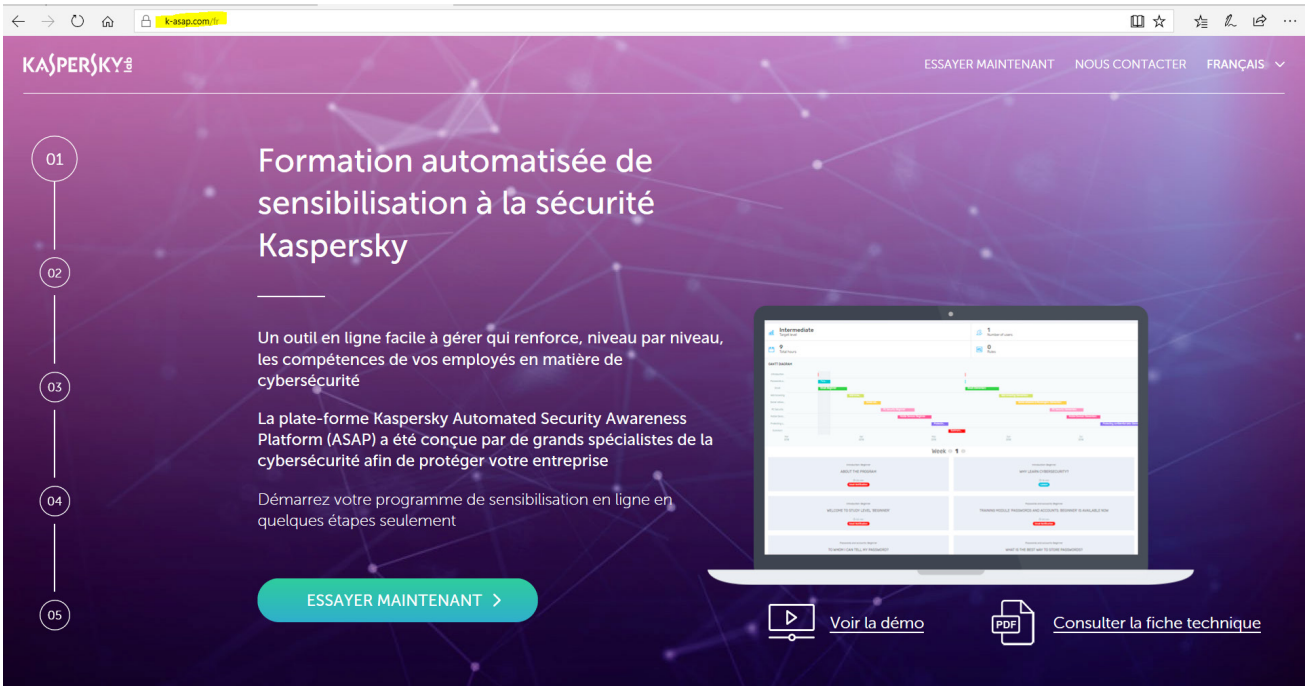
La plateforme de formation en ligne de Kaspersky Lab est conçue pour l'ensemble des salariés d'une entreprise.

Sans quitter leur ordinateur, les participants expérimentent des exercices interactifs et des scénarios typiques du quotidien pour découvrir les menaces informatiques potentielles et apprendre à les gérer.

Kaspersky® Automated Security Awareness Platform

Des simulations d'attaques 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.

- Un outil de de sensibilisation à la sécurité totalement automatisé (peu d'interventions de l'administrateur nécessaires)
- Un outil en ligne facile à gérer qui renforce, niveau par niveau, les compétences de vos salariés en matière de cybersécurité
- La plateforme Kaspersky Automated Security Awareness Platform (ASAP) a été conçue par de grands spécialistes de la cybersécurité afin de protéger votre entreprise, avec :
    - 32 modules d'apprentissage d'une durée de 10–20 minutes chacun
    - Des thèmes variés : RGPD, sécurisation des mots de passe, sécurité de la messagerie, etc.
    - Un module de simulations d'attaques par phishing
    - Des fonctions étendues d'analyse et de création de rapports



Testez Kaspersky Security Awareness Platform :
https://www.k-asap.com/fr
Ou contactez-nous pour toute question :
Commercial@kaspersky.fr / marketing@kaspersky.fr

#truecybersecurity
#HuMachine

www.kaspersky.fr