SÉCURITÉ INFORMATIQUE : L'UTILISATEUR FINAL EST SOUVENT LE MAILLON FAIBLE

Comment communiquer auprès de vos utilisateurs pour renforcer votre sécurité ?

kaspersky.fr/business
#securebiz

KASPERSKY lab

PRÉVENTION DES ATTEINTES À LA SÉCURITÉ INFORMATIQUE ET AUX DONNÉES

À l'heure où les réseaux d'entreprise gagnent en complexité, maintenir leur sécurité s'avère de plus en plus difficile. En effet, les utilisateurs se connectent à des réseaux publics non sécurisés et exécutent toutes sortes d'applications sur différents appareils, personnels comme appartenant à l'entreprise. Dans ce contexte, les données d'entreprise sensibles sont désormais accessibles – et vulnérables – à partir d'un nombre sans précédent de terminaux.

Les considérations à prendre en compte sont nombreuses et pour être efficaces, vos politiques de sécurité doivent maintenir sous contrôle les appareils, les applications et même les comportements de tous les utilisateurs. Mieux encore, elles doivent être réalistes.

Bien que cette tâche puisse sembler gigantesque au premier abord, elle peut se révéler plus simple que vous ne le pensez. Ce guide a justement pour but d'en simplifier certains aspects. Vous y trouverez des conseils clairs et pratiques pour protéger votre réseau et vos données, ainsi qu'apporter à vos employés les connaissances dont ils ont besoin pour se préserver tout en protégeant l'entreprise.

AU SOMMAIRE :

- Employés : Les bonnes pratiques en matière de sécurité informatique
- Applications : Faire des correctifs une priorité
- Mobilité : Protéger les employés, partout où ils travaillent
- Appareils : Fermer la porte aux programmes malveillants
- Web et médias sociaux : Le bon équilibre entre contrôle et liberté

EMPLOYÉS : LES BONNES PRATIQUES EN MATIÈRE DE SÉCURITÉ INFORMATIQUE

LA SITUATION

Thomas est le PDG de l'entreprise. Il a besoin de rester connecté en permanence. Outre un ordinateur portable, il utilise donc son smartphone d'entreprise et sa tablette personnelle pour travailler.

Bien évidemment, ces appareils contiennent des informations sensibles. Thomas est conscient que ces données doivent être protégées, c'est pourquoi il a défini un mot de passe et un code PIN. Le même mot de passe que celui qu'il utilise pour se connecter à ses comptes de messagerie et de médias sociaux. Et le même code PIN que celui de sa carte bancaire.

Cet exemple est typique de mauvaises habitudes en matière de sécurité. Si un seul des comptes personnels de Thomas est piraté, cette intrusion peut ouvrir la porte à une perte conséquente de données d'entreprise.

FAIT

59%

des individus ne stockent pas leurs mots de passe de manière sécurisée

Source : Infographie Kaspersky Lab sur les mots de passe

L'ANALYSE

Quels que soient les systèmes de défense que vous avez mis en place, il vaut toujours mieux prévenir que guérir. En vous assurant que tous les employés prennent des mesures de base pour se protéger, vous pouvez réduire significativement le risque d'une atteinte à la sécurité.

Aussi simple qu'efficace, le fait d'utiliser un mot de passe différent pour chaque compte a un impact important. Mais nous sommes humains. Et au mépris des mises en garde, nous cédons souvent à la facilité. **Ainsi, 63 % des personnes utilisent des mots de passe faciles à deviner et 39 % le même mot de passe pour tous leurs comptes.**

Il peut également arriver que certains employés ne soient pas conscients des risques qu'ils prennent. Vous identifiez probablement la menace liée aux liens douteux et aux pièces jointes suspectes dans les e-mails. Or, tout le monde ne réalise pas nécessairement ce danger dans votre entreprise.

C'est pourquoi il est important d'allier sensibilisation et systèmes de contrôle pour faire adopter et respecter par tous dans l'entreprise une véritable politique de sécurité.

CONSEILS PRATIQUES

1

Vous êtes en mesure de contrôler la taille, la complexité et l'usage répété des mots de passe. Par conséquent, utilisez votre politique pour dissuader les employés de céder à la facilité.

2

Assurez-vous que les employés connaissent les caractéristiques du phishing et des adresses Web potentiellement dangereuses. Encouragez-les à ne pas ouvrir les liens issus de sources inconnues, à ouvrir les liens dont ils ne sont pas certains dans une fenêtre distincte et à vérifier la cohérence des URL.

3

Personne ne devrait ouvrir des fichiers de sources inconnues, qu'ils soient d'ordre personnel ou professionnel. Cette règle doit être un élément clé de votre politique de sécurité.

CONSEIL IMPORTANT

Les mots de passe doivent comporter au moins huit caractères et combiner lettres majuscules et minuscules, chiffres et caractères spéciaux.

CONSEIL IMPORTANT

Avant de cliquer, les employés doivent passer le curseur de la souris sur les liens pour vérifier qu'ils mènent bien au site attendu.

APPLICATIONS : FAIRE DES CORRECTIFS UNE PRIORITÉ

LA SITUATION

Comme tout comptable qui se respecte, Maria est très occupée. Surtout aujourd'hui. Elle n'a pas le temps d'attendre que les mises à jour d'applications s'installent. Elle clique donc sur « Me rappeler ultérieurement » et s'attaque à des tâches plus urgentes.

Maria utilise d'anciennes versions de Microsoft Office, Adobe Acrobat et de la plupart des autres applications qui lui sont nécessaires. Mais elles fonctionnent correctement, si bien que lorsque des rappels apparaissent, elle les ignore tout bonnement.

Elle parvient à venir à bout de son planning chargé et même à quitter le bureau à l'heure, pour une fois. Elle rentre chez elle satisfaite et sereine, sans savoir que le programme qu'elle a téléchargé sur un site de partage de fichiers quelques heures auparavant était infecté par un programme malveillant dont le code a déjà exploité les failles de ses applications non corrigées et s'est répandu sur tout le réseau.

L'ANALYSE

Bien que cela n'empêche pas les employés de réaliser leurs tâches quotidiennes, choisir de ne pas mettre à jour les logiciels augmente le risque d'une atteinte à la sécurité. La majorité des programmes malveillants sont conçus pour tirer profit des vulnérabilités présentes dans les applications. Et plus on attend avant d'installer les correctifs, plus on laisse de temps aux cyber-criminels pour exploiter ces failles.

En fait, dans la plupart des cas où des attaques sont perpétrées par le biais d'une application, un correctif était déjà disponible. Dans un sens, c'est plutôt positif : cela signifie que la situation aurait pu être évitée relativement facilement. Par conséquent, vous devez faire en sorte de rechercher et déployer tous les correctifs disponibles ainsi que de supprimer les logiciels indésirables ou inutiles de votre réseau.

FAITS

49%

des personnes ne procèdent pas régulièrement à l'installation des correctifs ou à la mise à jour des logiciels et systèmes d'exploitation

Source : Enquête 2014 sur les risques informatiques au niveau mondial

58%

des entreprises n'ont pas pleinement mis en œuvre un contrôle des applications

Source : Enquête 2014 sur les risques informatiques au niveau mondial

CONSEILS PRATIQUES

1

Rechercher les correctifs disponibles et les classer par ordre de priorité prend beaucoup de temps, sans compter le fait de les déployer. En utilisant les fonctionnalités de **gestion des vulnérabilités et des correctifs de Kaspersky Endpoint Security for Business**, vous pouvez automatiser ce processus, de manière à réduire à la fois votre charge de travail et les risques pour votre entreprise.

2

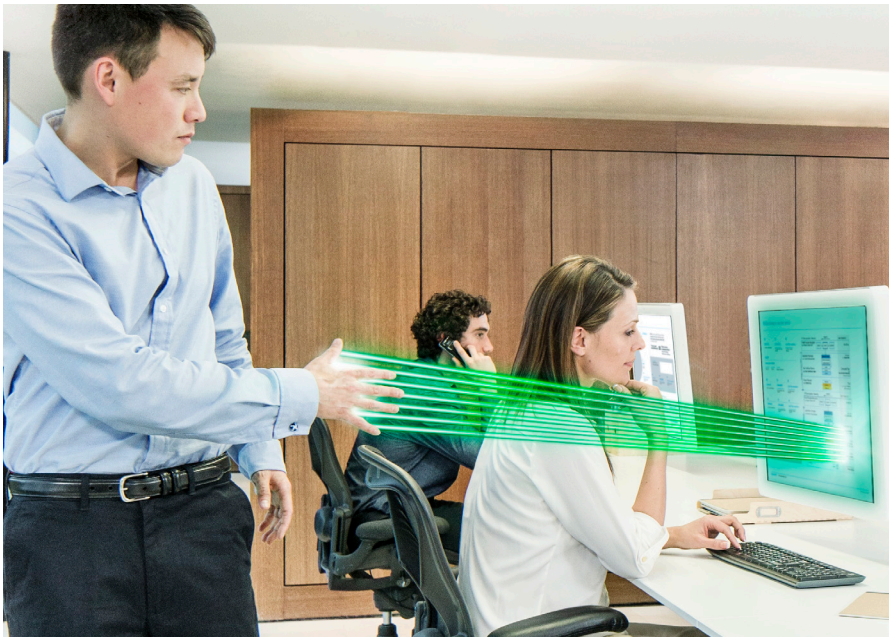
Donnez-vous les moyens de détecter et bloquer les applications et logiciels indésirables qui ont pénétré votre réseau. Avec **Kaspersky Endpoint Security for Business**, vous bénéficiez à la fois d'une bonne visibilité et d'un contrôle de tous les logiciels utilisés par vos employés, pour identifier, enregistrer et suivre le matériel et les périphériques amovibles plus facilement.

3

Munissez-vous des outils nécessaires pour faire appliquer vos politiques relatives aux applications. Grâce au **contrôle des applications**, vous pouvez autoriser, bloquer et réguler des applications, tandis que les contrôles « Blocage par défaut » vous permettent d'éliminer automatiquement certaines applications de votre réseau. Ajoutant un niveau de protection supplémentaire, le contrôle des privilèges des applications surveille et restreint toute application dont le comportement semble suspect. Ainsi, même si un programme est compromis, vous pouvez toujours l'empêcher d'entreprendre des actions malveillantes.

CONSEIL IMPORTANT

Vous pouvez désactiver le bouton « Me rappeler ultérieurement » pour éviter que les mises à jour critiques ne soient ignorées.



APPAREILS : FERMER LA PORTE AUX PROGRAMMES MALVEILLANTS

LA SITUATION

Thomas s'est rendu à une conférence. Il a noué plusieurs relations intéressantes et il est impatient de passer en revue certaines des informations qu'on lui a fournies sur une clé USB.

Dès son retour au bureau, il saisit son lecteur MP3 en cours de chargement, connecte la clé USB et charge les fichiers sur le réseau.

Complètement absorbé par les opportunités susceptibles de découler des conversations entretenues au cours de la journée, il ne prend pas le temps de réfléchir à ce que ces fichiers pourraient contenir et il clique sur « Ouvrir ».

L'ANALYSE

Tout comme les URL, les fichiers et les pièces jointes, les appareils physiques peuvent être utilisés pour transmettre des programmes malveillants. À moins de le vérifier avant de l'ouvrir, il est impossible de connaître le contenu d'une clé USB. Et même si la clé porte le logo de l'entreprise, cela ne signifie pas pour autant qu'elle ne présente aucun danger.

Les clés USB ne sont pas les seules à poser problème. Tout appareil ayant été en contact avec un réseau inconnu peut être infecté. Par conséquent, même si la clé USB de Thomas est sans danger, le lecteur MP3 qu'il était en train de recharger peut lui aussi présenter un risque. En fait, les supports amovibles tels que les clés USB et les cartes SD représentent 30 % des infections par des programmes malveillants.

Là encore, il existe des mesures automatiques que vous pouvez mettre en place pour empêcher vos employés d'adopter des comportements à risques. Et si leur niveau de connaissance leur permet alors d'exercer une prudence appropriée, vous pouvez réduire significativement la probabilité qu'un programme malveillant n'infiltre votre réseau.

FAIT

« Les supports amovibles tels que les clés USB et les cartes SD représentent 30 % des infections par des programmes malveillants. »

Source : Blog Kaspersky Lab

CONSEILS PRATIQUES

1. Assurez-vous que les employés vérifient leurs appareils et disques externes avant de les utiliser, même s'ils jugent la source digne de confiance. Il peut être judicieux de désactiver la fonctionnalité d'exécution automatique. De cette manière, seuls les fichiers sélectionnés sont ouverts.

2. Encouragez les employés à appliquer le même raisonnement à leurs appareils personnels. Par exemple, s'ils remarquent un dysfonctionnement de leur smartphone ou s'ils suspectent une infection par un programme malveillant, ils doivent savoir qu'il est important de ne pas connecter leur téléphone à leur ordinateur portable.

3. En utilisant la fonctionnalité de contrôle des appareils de Kaspersky Endpoint Security for Business, vous pouvez spécifier les types d'appareils qui peuvent se connecter à votre réseau ainsi que les opérations qu'ils peuvent effectuer.

4. La fonctionnalité de contrôle des applications vous permet de bloquer les programmes malveillants sur un appareil, même s'ils sont ouverts.

CONSEIL IMPORTANT

Paramétrez votre solution de protection contre les programmes malveillants de sorte qu'elle analyse automatiquement tous les appareils et, selon les besoins de l'employé, qu'elle bloque tous les types d'appareils inutiles.

FAIT

« 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 la station spatiale internationale. »

Source : Communiqué de presse Kaspersky Lab sur Stuxnet

MOBILITÉ : PROTÉGER LES EMPLOYÉS, PARTOUT OÙ ILS TRAVAILLENT

LA SITUATION

Thomas doit faire le meilleur usage de son temps. C'est pourquoi il utilise sa tablette pour accéder à ses e-mails de même qu'aux données des clients lorsqu'il n'est pas au bureau.

Disposant d'un battement de vingt minutes entre deux réunions, Thomas se rend dans un café pour consommer une boisson et apporter des modifications de dernière minute à sa présentation. Il profite du wifi gratuit pour envoyer un e-mail à ses collègues, pour que tout le monde ait accès à la dernière version.

Le fichier contient des informations qui ne doivent pas être partagées avec la concurrence. Il ne vient pas à l'esprit de Thomas que c'est peut-être ce qu'il vient de faire en envoyant le fichier par le biais d'un réseau non sécurisé.

L'ANALYSE

Avec le développement du travail mobile, appliquer des mesures de sécurité au seul matériel présent au bureau n'est plus suffisant. Dans la mesure où les employés sont nombreux à apporter leurs appareils personnels au bureau, il ne suffit plus non plus de protéger les seuls appareils détenus par l'entreprise.

Si ces nouvelles habitudes de travail s'accompagnent de nombreux avantages pour l'entreprise, elles augmentent également la complexité de leur environnement informatique, sans parler de la large disponibilité de réseaux gratuits et non protégés, sur lesquels des données peuvent être interceptées.

Vous ne pouvez ignorer cette réalité. L'usage mobile doit être au cœur de votre politique de sécurité informatique globale. En faisant preuve de proactivité, vous pouvez contribuer à empêcher la perte de données occasionnée par des menaces sophistiquées telles que les programmes malveillants, mais aussi des incidents tels que la perte d'appareils.

FAITS

Près de

1/3 et 1/4

des entreprises ont enregistré des cas de perte/vol de mobiles d'employés

d'entre elles savent qu'elles ont perdu des données de ce fait.

Source : Infographie Kaspersky Lab sur les mots de passe

CONSEILS PRATIQUES

1

Vous ne pouvez pas protéger un appareil dont vous n'avez pas connaissance. Les employés doivent comprendre l'importance de la sécurité mobile et du fait d'informer l'équipe informatique de tous les appareils qu'ils utilisent.

2

Kaspersky Security for Mobile vous permet d'ajouter des solutions de protection contre les programmes malveillants et d'autres technologies de sécurité mobile à vos appareils, tandis que vous surveillez l'administration de tous les appareils de votre réseau grâce à la fonctionnalité de gestion des appareils mobiles (MDM). Étant donné que Kaspersky Endpoint Security for Business inclut la sécurité mobile et la gestion des appareils mobiles, vous pouvez intégrer la sécurité mobile dans votre approche informatique globale sans recourir à une solution distincte et autonome.

CONSEIL IMPORTANT

Assurez-vous que les individus comprennent que seul un réseau sécurisé doit être utilisé pour accéder aux données d'entreprise (y compris les e-mails). Cela ne signifie pas qu'ils ne doivent pas profiter pleinement du wifi gratuit, mais seulement en utilisant un réseau privé virtuel (VPN).

CONSEIL IMPORTANT

La perte d'un appareil ne doit pas rimer systématiquement avec perte de données. Vous pouvez séparer les données d'entreprise des informations personnelles de l'utilisateur. Ces données sensibles peuvent ensuite être chiffrées, pour les rendre illisibles si l'appareil est volé. Le cas échéant, vous pouvez supprimer le conteneur des données d'entreprise, par exemple si l'employé quitte l'entreprise.

FAIT

« Sur les réseaux wifi non protégés, toutes les données peuvent être interceptées et les données à l'écran peuvent être modifiées. Pourtant, 34 % des utilisateurs de wifi public ne prennent aucune mesure spécifique pour se protéger. »

Source : Infographie Kaspersky Lab sur les appareils personnels utilisés sur le lieu de travail

WEB ET MÉDIAS SOCIAUX : DESCRIPTION D'UN ACCÈS CONTRÔLÉ

LA SITUATION

Pendant sa pause déjeuner, Maria prend un moment pour consulter Facebook. Elle fait défiler son fil d'actualité et tombe sur un lien qui lui semble intéressant. L'article n'étant pas conforme à ses attentes, elle le ferme. Le téléphone sonne, elle se déconnecte et se remet au travail.

Malheureusement, le site en question a lancé une attaque éclair et parce qu'elle n'a pas mis à jour son navigateur depuis l'acquisition de son ordinateur portable, Maria n'a reçu aucun avertissement sur le caractère suspect du site. Et parce qu'elles étaient toutes deux ouvertes, sa messagerie professionnelle et sa messagerie personnelle ont été analysées par le programme malveillant, compromettant ainsi des informations financières importantes.

L'ANALYSE

Tout comme l'utilisation d'appareils personnels sur le lieu de travail, les sites de médias sociaux illustrent la manière dont l'entremêlement de nos vies professionnelle et privée peut avoir des répercussions graves en matière de sécurité en ligne. Outre le fait de permettre la propagation de programmes malveillants, ces pratiques sont l'occasion pour les cyber-criminels de recueillir des informations sur des cibles potentielles.

Il est important que les employés comprennent que même lorsqu'ils naviguent à des fins personnelles, les risques qu'ils prennent peuvent affecter l'ensemble de l'entreprise. En encourageant les comportements appropriés, vous pouvez mettre en œuvre une politique qui préserve la sécurité de votre réseau et de vos données sans nuire à la qualité de vie au travail des employés.

FAITS

Médias sociaux : un usage généralisé qui s'étend sur toutes sortes d'appareils

des utilisateurs de médias sociaux accèdent aux sites par des ordinateurs

des utilisateurs de médias sociaux accèdent aux sites par des smartphones

des utilisateurs de médias sociaux accèdent aux sites par des tablettes

Source : Infographie Kaspersky Lab sur les réseaux sociaux

CONSEILS PRATIQUES

1

Expliquez aux employés qu'ils doivent vérifier l'origine de tout contenu qu'ils téléchargent et passer le curseur de la souris sur les liens pour vérifier que l'URL correspond au texte, surtout si le site de destination n'est ni connu ni fiable.

2

Assurez-vous que votre politique couvre la conduite à adopter par les employés sur les sites de médias sociaux. Ils ne doivent jamais partager des informations sensibles, qu'elles soient personnelles ou liées à l'entreprise. Et il leur incombe de passer leurs contacts au crible.

3

Si des sites sont tout simplement inappropriés au travail, ils doivent être exclus de votre politique de navigation. La fonctionnalité de contrôle du Web de Kaspersky Endpoint Security for Business vous permet d'utiliser des bases de données prédéfinies ou personnalisées pour mettre sur liste noire certaines catégories de sites Web à ne pas visiter.

4

Il peut être difficile de détecter certains des subterfuges plus subtils utilisés pour propager des programmes malveillants. Kaspersky Systems Management, qui inclut la gestion des correctifs, peut vous aider à vous assurer que les employés utilisent des versions à jour de leur navigateur, de manière à réduire les risques.

CONSEIL IMPORTANT

Kaspersky Endpoint Security for Business propose des listes noires prédéfinies et personnalisables que vous pouvez utiliser pour interdire des sites selon leur type. Dans la mesure où vous pouvez créer des groupes d'utilisateurs, les restrictions ne s'appliquent pas nécessairement à toute l'entreprise. Si votre équipe marketing a besoin d'utiliser Facebook, mais pas le reste de l'entreprise, vous pouvez limiter l'accès au site à cette seule équipe.

FAIT

Les trois principaux sites de médias sociaux visés par des attaques de phishing sont :

56 % Facebook **8 % Twitter** **3 % Pinterest**

Source : Infographie Kaspersky Lab sur les réseaux sociaux

CONCLUSION

Faire bénéficier votre entreprise de la meilleure protection possible nécessite à la fois l'institution de règles et de la pédagogie. Si les employés ont plus de liberté que jamais, ils ont aussi l'obligation d'assumer plus qu'auparavant la responsabilité de leur propre sécurité.

Ceci dit, vous avez à votre disposition une multitude de moyens pour éliminer les comportements à risques. Grâce à ces outils qui vous aident à faire respecter vos politiques rapidement et facilement, vous pouvez réduire le temps passé à résoudre les problèmes. Autant de temps mis à profit pour prendre du recul sur la situation, afin d'anticiper les dangers et de mettre en place des mesures préventives.

La proactivité est en effet un élément primordial. Vous mesurez déjà les menaces auxquelles vous êtes exposé. À présent, grâce aux conseils de ce guide, vous pouvez prendre des mesures pratiques pour protéger votre entreprise.

PRENEZ DES MESURES SANS PLUS ATTENDRE : ESSAI GRATUIT DE 30 JOURS

Découvrez comment nos solutions de sécurité peuvent protéger votre entreprise des programmes malveillants et de la cyber-criminalité en les essayant gratuitement pendant un mois.

Enregistrez-vous aujourd'hui pour télécharger des versions complètes de nos produits et évaluer leur capacité à protéger parfaitement votre infrastructure informatique, vos terminaux et les données confidentielles de votre entreprise.

EFFECTUEZ UN ESSAI GRATUIT DÈS MAINTENANT

RETROUVEZ-NOUS SUR LES RÉSEAUX SOCIAUX

#securebiz

Visionnez nos vidéos sur YouTube

Rejoignez nos fans sur Facebook

Découvrez le blog d'Eugène Kaspersky

Suivez-nous sur Twitter

Retrouvez-nous sur LinkedIn

Plus d'informations sur : www.kaspersky.fr/business

À PROPOS DE KASPERSKY LAB

Kaspersky Lab est le plus grand éditeur privé mondial de solutions de protection des terminaux. La société fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité pour utilisateurs de terminaux informatiques*. Depuis plus de 17 ans, 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, dont la holding est enregistrée au Royaume-Uni, opère actuellement dans près de 200 pays et territoires du monde entier et offre une protection à plus de 300 millions d'utilisateurs. Plus d'informations sur : www.kaspersky.fr.

* L'entreprise est quatrième en termes de chiffre d'affaires au classement mondial des éditeurs de solution de sécurité des terminaux effectué par IDC en 2012. Ce classement a été publié dans le rapport IDC « Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares » (Sécurité des terminaux dans le monde : prévisions pour 2013-2017 et parts de marché des fournisseurs en 2012), document numéro 242618, août 2013. Ce rapport classait les éditeurs de logiciels selon leurs revenus provenant des ventes de solutions de sécurité des terminaux en 2012.