Everping

Comment sécuriser les ordinateurs de mon entreprise ?

10 bonnes pratiques

Comment sécuriser les ordinateurs de mon entreprise ?

Everping vous partage les 10 bonnes pratiques essentielles pour sécuriser l'ensemble des PCs et Macs de votre entreprise, d'après les meilleurs standards internationaux en sécurité informatique

1 Le déploiement des mises à jour

Mettre à jour le système d'exploitation des ordinateurs (aussi appelé l'OS, de l'anglais Operating System) est un élément central de la protection des ordinateurs. Le déploiement des mises à jour corrige en effet toutes les failles de sécurité identifiées par le passé sur Windows ou MacOS et permet ainsi d'avoir un ordinateur à jour et protégé des dernières failles identifiées.

La mise à jour apporte aussi son lot de nouveautés avec de nouvelles fonctionnalités et une amélioration des anciennes. Elle assure donc la sécurité de votre appareil et permet de tirer le meilleur profit de la technologie en améliorant l'expérience utilisateur !

2 Le chiffrement du disque dur

Le chiffrement du disque dur permet de protéger les ordinateurs en cas de perte ou de vol.
Le chiffrement évite en effet qu'une personne puisse accéder aux données du disque dur, même si cette personne a l'ordinateur entre les mains.
Pour pouvoir accéder à un disque dur chiffré et donc à toute la donnée sur l'ordinateur, il faut obligatoirement avoir la clé de récupération qui a été activée lors du chiffrement du disque.
Attention, le chiffrement du disque dur ne vous protège pas des virus et des malwares !

Comment sécuriser les ordinateurs de mon entreprise ?

Everping vous partage les 10 bonnes pratiques essentielles pour sécuriser l'ensemble des PCs et Macs de votre entreprise, d'après les meilleurs standards internationaux en sécurité informatique

3 Activer le firewall

Un firewall, ou pare-feu, est un logiciel installé sur l'ordinateur qui contrôle les données entrantes et sortantes.
L'utilisation d'un pare-feu au sein d'une entreprise est indispensable. Il permet d'identifier et de bloquer les requêtes indésirables dans les ordinateurs de l'entreprise. Le pare-feu en empêchant les attaquants ou les menaces externes d'accéder aux ordinateurs est donc un élément de sécurité majeur de votre parc informatique

4 Activer la complexité du mot de passe

Afin de mieux protéger vos sessions d'ordinateurs et la donnée qu'il y a dessus, il est recommandé d'activer une complexité sur le mot de passe des ordinateurs de vos collaborateurs.
Par exemple : exiger au moins 8 caractères, 1 caractère spécial, une majuscule, un mot de passe différent des 4 derniers mots de passe etc.
Cela va permettre de créer des mots de passe dits " forts" et ainsi d'éviter qu'un hacker qui aurait l'ordinateur entre les mains puisse trouver - avec un robot ou sans - le mot de passe; et ainsi avoir accès à tout le contenu de l'ordinateur

Comment sécuriser les ordinateurs de mon entreprise ?

Everping vous partage les 10 bonnes pratiques essentielles pour sécuriser l'ensemble des PCs et Macs de votre entreprise, d'après les meilleurs standards internationaux en sécurité informatique

5 Activer la rotation du mot de passe

La rotation des mots de passe sur vos ordinateurs va permettre d'assurer un niveau de sécurité supplémentaire.
Les collaborateurs seront invités à changer régulièrement leurs mots de passe, ce qui limite les risques qu'une personne ayant eu accès au mot de passe d'une façon ou d'une autre puisse toujours avoir accès à l'ordinateur dans le futur.

6 Assurer la mise en place de Gatekeeper

Gatekeeper permet de bloquer sur les Macs l'exécution d'applications non reconnues par Apple. Cela permet d'éviter le lancement d'applications malveillantes sur votre ordinateur qui, bien souvent, installent des adwares ou des logiciels non désirés.
Gatekeeper permet donc de garantir que seuls des logiciels fiables s'exécutent sur les Macs de votre entreprise

Comment sécuriser les ordinateurs de mon entreprise ?

Everping vous partage les 10 bonnes pratiques essentielles pour sécuriser l'ensemble des PCs et Macs de votre entreprise, d'après les meilleurs standards internationaux en sécurité informatique

7 Auto-verrouillage de l'écran

L'auto-verrouillage de l'écran permet de verrouiller votre session lorsque vous n'êtes plus présent devant votre ordinateur. Après 5 min d'inactivité (c'est la durée recommandée), le mot de passe est à nouveau demandé pour ouvrir la session de l'ordinateur.

Que vous soyez dans le TGV, en télétravail ou dans un lieu public, le verrouillage de l'ordinateur permettra d'éviter qu'un inconnu ait accès aux données et fichiers de votre ordinateur !

8 Déploiement d'un anti-virus ou d'un anti-malware

L'antivirus est un élément indispensable de la sécurisation des ordinateurs
L'anti-virus est un logiciel installé sur l'ordinateur, dont la mission est de détecter les logiciels malveillants et protéger l'ordinateur contre les attaques en supprimant les logiciels et virus installés. Les dernières générations d'antivirus (on parle plutôt d'anti-malware désormais, qui protège contre les virus mais aussi d'autre types d'attaques comme les spyware ou les chevaux de troie) permettent également de détecter des activités suspectes simplement à leur comportement, sans que le virus soit déjà référencé ou connu des antivirus traditionnels.
Des antivirus leaders sont par exemple Windows Defender (nativement présent dans Windows), Kaspersky ou Malwarebytes (qui est également un anti-malware). Une console de supervision permettra également le suivi des incidents sur l'ensemble du parc informatique et de recevoir des alertes lorsque des infections sont détectées.

Comment sécuriser les ordinateurs de mon entreprise ?

Everping vous partage les 10 bonnes pratiques essentielles pour sécuriser l'ensemble des PCs et Macs de votre entreprise, d'après les meilleurs standards internationaux en sécurité informatique

9 Confier les droits administrateurs des ordinateurs à un spécialiste IT

Vos collaborateurs doivent ils être administrateur de leurs ordinateurs ? Bien qu'il n'existe pas de bonne ou mauvaise réponse, confier les droits administrateurs de l'ordinateur seulement à un spécialiste IT présente des avantages (et est d'ailleurs parfois demandé pour obtenir une certification en sécurité informatique!).

Enlever les droits administrateurs à la plupart des collaborateurs de l'entreprise va permettre d'éviter que les personnes peu sensibilisées à la sécurité informatique ne réalisent des actions dommageable pour l'ordinateur (comme par exemple installer un logiciel inconnu et malveillant ou bien lancer un programme infecté). A partir du moment où une politique d'entreprise (avec des logiciels autorisés et une bonne préparation des ordinateurs à l'arrivée d'un collaborateur) ainsi qu'un support IT réactif sont présents dans l'entreprise, confier les droits administrateurs à un spécialiste ne pourra être que bénéfique sans ralentir le travail aux quotidiens de vos équipes.

10 Sensibiliser les collaborateurs au Phishing

La sécurisation d'un parc informatique ne peut se faire sans la sensibilisation des collaborateurs qui est complémentaire aux déploiements des meilleures pratiques. Sensibiliser régulièrement les collaborateurs aux phishings est indispensable aujourd'hui.

L'hameçonnage ou phishing est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels (comme des identifiants bancaires ou l'accès à vos emails) dans le but de perpétrer une usurpation d'identité. Le Phishing consiste à faire croire à la victime qu'elle s'adresse à une personne de confiance — banque, La Poste, etc. — afin de d'obtenir des renseignements personnels (mot de passe, numéro de carte de crédit, etc.) et ainsi les utiliser frauduleusement par la suite.

La sensibilisation de vos collaborateurs peut passer par des sessions régulières de formation ou la mise en place de campagne de simulation de Phishing dans votre entreprise !

Pour aller plus loin

Vous souhaitez en savoir plus sur ces bonnes pratiques de sécurité ?

Vous souhaitez renforcer la sécurisation de l'ensemble des PCs et Macs de votre entreprise ?

CONTACTEZ NOUS

WWW.EVERPING.EU/CONTACT

Everping

L'infogérance nouvelle génération