Sortir les PME des GAFAM

Retour d'expérience

OpenPony

Juin 2015

Que sont les GAFAM ?

- Google
- Amazon
- Facebook
- Apple
- Microsoft

Que sont les GAFAM ?

- Google
- Amazon
- Facebook
- Apple
- Microsoft

Et plus généralement :

Toutes les entreprises privatrices et/ou réductrices des droits et libertés des utilisateurs.

Constat 1/3

Enquête IPSOS septembre 2014 auprès de dirigeants de PME :

- 99 % des PME sont équipées en informatique et leurs PC, tablettes et/ou smartphones sont connectés à Internet

Constat 1/3

Enquête IPSOS septembre 2014 auprès de dirigeants de PME :

- 99 % des PME sont équipées en informatique et leurs PC, tablettes et/ou smartphones sont connectés à Internet
- 93 % d'entre elles ont accès au web

Constat 1/3

Enquête IPSOS septembre 2014 auprès de dirigeants de PME :

- 99 % des PME sont équipées en informatique et leurs PC, tablettes et/ou smartphones sont connectés à Internet
- 93 % d'entre elles ont accès au web
- 82 % permettent un accès sans restriction

Constat 1/3

Enquête IPSOS septembre 2014 auprès de dirigeants de PME :

- 99 % des PME sont équipées en informatique et leurs PC, tablettes et/ou smartphones sont connectés à Internet
- 93 % d'entre elles ont accès au web
- 82 % permettent un accès sans restriction
- 80 % utilisent des terminaux mobiles (ordinateur portable, smartphone ou tablette) majoritairement connectés à Internet et donnant accès au réseau de l'entreprise dans plus de 2 cas sur 3.

Constat 2/3

Elles ont conscience de l'exposition de leur système informatique à des risques...

- 9 entreprises sur 10 évaluent l'usurpation des mots de passe et l'utilisation frauduleuse ou malveillante de leurs ressources informatiques comme un risque

Constat 2/3

Elles ont conscience de l'exposition de leur système informatique à des risques...

- 9 entreprises sur 10 évaluent l'usurpation des mots de passe et l'utilisation frauduleuse ou malveillante de leurs ressources informatiques comme un risque
- 7 sur 10 le pensent aussi pour le piratage des données détenues, données entreprises ou données clients

Constat 2/3

Elles ont conscience de l'exposition de leur système informatique à des risques...

- 9 entreprises sur 10 évaluent l'usurpation des mots de passe et l'utilisation frauduleuse ou malveillante de leurs ressources informatiques comme un risque
- 7 sur 10 le pensent aussi pour le piratage des données détenues, données entreprises ou données clients
- 76 % des dirigeants savent qu'ils sont pénalement responsables de l'utilisation d'internet dans leur entreprise.

Constat 2/3

Et pourtant...

- 87 % utilisent une messagerie qui dans 70 % des cas est celui de leur fournisseur d'accès à Internet ou un générique type Google.

Constat 2/3

Et pourtant...

- 87 % utilisent une messagerie qui dans 70 % des cas est celui de leur fournisseur d'accès à Internet ou un générique type Google.
- les 3/4 ne savent pas où sont stockés leurs mails et pièces jointes.

Constat 2/3

Et pourtant...

- 87 % utilisent une messagerie qui dans 70 % des cas est celui de leur fournisseur d'accès à Internet ou un générique type Google.
- les 3/4 ne savent pas où sont stockés leurs mails et pièces jointes.
- 26 % d'entre-elles ne possèdent pas d'anti-virus, seules 36 % ont un antiphising et 52 % un firewall.

Constat 2/3

Et pourtant...

- 87 % utilisent une messagerie qui dans 70 % des cas est celui de leur fournisseur d'accès à Internet ou un générique type Google.
- les 3/4 ne savent pas où sont stockés leurs mails et pièces jointes.
- 26 % d'entre-elles ne possèdent pas d'anti-virus, seules 36 % ont un antiphising et 52 % un firewall.
- plus de 50 % n'ont pris aucune disposition pour se protéger d'éventuelles malveillances (backup, chiffrement des données, politique sécurité...)

Constat 2/3

Et pourtant...

- 87 % utilisent une messagerie qui dans 70 % des cas est celui de leur fournisseur d'accès à Internet ou un générique type Google.
- les 3/4 ne savent pas où sont stockés leurs mails et pièces jointes.
- 26 % d'entre-elles ne possèdent pas d'anti-virus, seules 36 % ont un antiphising et 52 % un firewall.
- plus de 50 % n'ont pris aucune disposition pour se protéger d'éventuelles malveillances (backup, chiffrement des données, politique sécurité...)
- le budget par salarié alloué à la sécurité informatique ne dépasse pas 50 €

Outils fréquemment utilisés

Google	Gmail, GoogleDocs, Hangouts, Agenda, GoogleForms, Maps
Apple	matériel, itunes, icloud, OS
Facebook	pages d'entreprise, messagerie
Amazon	hébergement, interface e-commerce
Microsoft	Windows, Office, Skype, Exchange, Server, bitlocker, hotmail/outlook.com

Outils fréquemment utilisés

Google	Gmail, GoogleDocs, Hangouts, Agenda, GoogleForms, Maps
Apple	matériel, itunes, icloud, OS
Facebook	pages d'entreprise, messagerie
Amazon	hébergement, interface e-commerce
Microsoft	Windows, Office, Skype, Exchange, Server, bitlocker, hotmail/outlook.com

Mais aussi :

- Dropbox
- Oracle / Adobe
- Et encore beaucoup d'autres !

Pourquoi ces outils sont dangereux pour les PME

Avez-vous déjà lu les CGU de ces services ?

Pourquoi ces outils sont dangereux pour les PME

Avez-vous déjà lu les CGU de ces services ?

Petit exemple de Google :

Pourquoi ces outils sont dangereux pour les PME

Avez-vous déjà lu les CGU de ces services ?

Petit exemple de Google :
Lorsque vous importez, soumettez, stockez, envoyez ou recevez des contenus à travers nos Services, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées (des traductions, des adaptations ou d'autres modifications destinées à améliorer le fonctionnement de vos contenus par le biais de nos Services), de communication, de publication, de représentation publique, d'affichage public ou de distribution publique desdits contenus.

Pourquoi ces outils sont dangereux pour les PME

Les droits que vous accordez dans le cadre de cette licence sont limités à l'exploitation, la promotion ou à l'amélioration de nos Services, ou au développement de nouveaux Services. Cette autorisation demeure pour toute la durée légale de protection de votre contenu, même si vous cessez d'utiliser nos Services (par exemple, pour une fiche d'entreprise que vous avez ajoutée à Google Maps).

Pourquoi ces outils sont dangereux pour les PME

Les droits que vous accordez dans le cadre de cette licence sont limités à l'exploitation, la promotion ou à l'amélioration de nos Services, ou au développement de nouveaux Services. Cette autorisation demeure pour toute la durée légale de protection de votre contenu, même si vous cessez d'utiliser nos Services (par exemple, pour une fiche d'entreprise que vous avez ajoutée à Google Maps).

Pour une vision globale des CGU : https://tosdr.org/

Quelles alternatives ?

Seules solutions à ce véritable espionnage industriel :

- Chiffrement
- Logiciels libres

- Et bien sûr la formation utilisateurs aux bonnes pratiques

Pourquoi les logiciels libres ?

Les logiciels libres sont la seule possibilité d'être sûr d'avoir des logiciels soucieux de la vie privée et des droits des utilisateurs.

Pourquoi les logiciels libres ?

Les logiciels libres sont la seule possibilité d'être sûr d'avoir des logiciels soucieux de la vie privée et des droits des utilisateurs.

Les logiciels libres sont programmés, revus, corrigés et audités régulièrement par les membres d'une communauté (souvent bénévole) pour assurer le bon fonctionnement et la sécurité des outils développés.

Pourquoi les logiciels libres ?

Les logiciels libres sont la seule possibilité d'être sûr d'avoir des logiciels soucieux de la vie privée et des droits des utilisateurs.

Les logiciels libres sont programmés, revus, corrigés et audités régulièrement par les membres d'une communauté (souvent bénévole) pour assurer le bon fonctionnement et la sécurité des outils développés.

Les sources sont disponibles à tous ceux qui en ont besoin, souhaitent contribuer ou contrôler la fiabilité du code.

Pourquoi les logiciels libres ?

Les logiciels libres sont la seule possibilité d'être sûr d'avoir des logiciels soucieux de la vie privée et des droits des utilisateurs.

Les logiciels libres sont programmés, revus, corrigés et audités régulièrement par les membres d'une communauté (souvent bénévole) pour assurer le bon fonctionnement et la sécurité des outils développés.

Les sources sont disponibles à tous ceux qui en ont besoin, souhaitent contribuer ou contrôler la fiabilité du code.

Quelles solutions alternatives ?

Privateur	**Libre**
Microsoft/Apple	GNU/Linux
Office	Libre Office
Gmail	autohébergement serveur mail
Hangouts	autohébergement serveur xmpp
Google Maps	OpenStreetMap
Skype	Tox
Dropbox	Serveur OwnCloud
Outlook	Thunderbird

(Liste non exhaustive)

Comment faire adopter les bonnes pratiques ?

Il n'y a pas, malheureusement, de solutions miracles mais voici quelques pistes :

- Adopter vous-même les bonnes pratiques

Comment faire adopter les bonnes pratiques ?

Il n'y a pas, malheureusement, de solutions miracles mais voici quelques pistes :

- Adopter vous-même les bonnes pratiques
- Soyez ouvert au dialogue

Comment faire adopter les bonnes pratiques ?

Il n'y a pas, malheureusement, de solutions miracles mais voici quelques pistes :

- Adopter vous-même les bonnes pratiques
- Soyez ouvert au dialogue
- Pour la Direction : lui rappeler que le libre est gratuit (économies de licences, toussa)

Comment faire adopter les bonnes pratiques ?

Il n'y a pas, malheureusement, de solutions miracles mais voici quelques pistes :

- Adopter vous-même les bonnes pratiques
- Soyez ouvert au dialogue
- Pour la Direction : lui rappeler que le libre est gratuit (économies de licences, toussa)
- Former les utilisateurs aux bonnes pratiques partout où vous êtes avec eux (boulot, repas du midi, afterwork...)

Comment faire adopter les bonnes pratiques ?

Il n'y a pas, malheureusement, de solutions miracles mais voici quelques pistes :

- Adopter vous-même les bonnes pratiques
- Soyez ouvert au dialogue
- Pour la Direction : lui rappeler que le libre est gratuit (économies de licences, toussa)
- Former les utilisateurs aux bonnes pratiques partout où vous êtes avec eux (boulot, repas du midi, afterwork...)
- N'ayez pas peur de dire plusieurs fois les mêmes choses

Comment faire adopter les bonnes pratiques ?

Il n'y a pas, malheureusement, de solutions miracles mais voici quelques pistes :

- Adopter vous-même les bonnes pratiques
- Soyez ouvert au dialogue
- Pour la Direction : lui rappeler que le libre est gratuit (économies de licences, toussa)
- Former les utilisateurs aux bonnes pratiques partout où vous êtes avec eux (boulot, repas du midi, afterwork...)
- N'ayez pas peur de dire plusieurs fois les mêmes choses
- Adaptez votre langage à votre interlocuteur mais ne vulgarisez pas trop. Restez crédible ! (un technicien doit pouvoir montrer qu'il sait de quoi il parle sans prendre son interlocuteur pour un imbécile. Il pourrait se sentir diminué)

Comment faire adopter les bonnes pratiques ?

- Proposez des alternatives libres en parallèle des habitudes en proposant des sessions d'initiation et formation

Comment faire adopter les bonnes pratiques ?

- Proposez des alternatives libres en parallèle des habitudes en proposant des sessions d'initiation et formation
- Mettez en place un wiki avec des tutos d'installation, d'aide

Comment faire adopter les bonnes pratiques ?

- Proposez des alternatives libres en parallèle des habitudes en proposant des sessions d'initiation et formation
- Mettez en place un wiki avec des tutos d'installation, d'aide
- Proposez la mise en place d'un blog pour informer sur les actus numériques au sein de l'entreprise

Comment faire adopter les bonnes pratiques ?

- Proposez des alternatives libres en parallèle des habitudes en proposant des sessions d'initiation et formation
- Mettez en place un wiki avec des tutos d'installation, d'aide
- Proposez la mise en place d'un blog pour informer sur les actus numériques au sein de l'entreprise
- Montrez que la communauté libre n'est pas une secte de barbus autistes !

Pourquoi il est important de perséverer ?

- Faire entrer le libre dans les PME, c'est les faire entrer chez tout le monde.

Pourquoi il est important de perséverer ?

- Faire entrer le libre dans les PME, c'est les faire entrer chez tout le monde.
- Un utilisateur qui apprend l'utilisation des bonnes pratiques en entreprise est un utilisateur qui les expliquera chez lui

Pourquoi il est important de perséverer ?

- Faire entrer le libre dans les PME, c'est les faire entrer chez tout le monde.
- Un utilisateur qui apprend l'utilisation des bonnes pratiques en entreprise est un utilisateur qui les expliquera chez lui
- Rappelez-vous que l'informatique s'est démocratisée grâce aux entreprises, faites entrer les bonnes pratiques chez Monsieur et Madame tout le monde !

Questions ?

Merci !