GUIDE

des bonnes pratiques pour une sécurité informatique optimale

By Conty

Règle n° 1

Identifier les administrateurs / utilisateurs

Certaines personnes peuvent posséder des droits appelés « Administrateur » ou « Utilisateur ».

=> Les « Administrateurs » ont la possibilité de modifier en totalité les paramètres sur les Serveurs ou Ordinateurs.

=> Les « Utilisateurs » ont des accès restreints et ont une utilisation simplifiée de leurs environnements de travail.

- Réserver le droit « Administrateur » au personnes ayant au moins une compétence d'administration réseau basique. Il faut s'appuyer sur un service informatique / prestataire informatique pour la gestion des réseaux.
- Supprimer / désactiver les comptes non-utilisés ou obsolètes.
- Préférer une authentification par utilisateur nommé.

Règle n° 2

Choisir ses mots de passe

Le mot de passe est un outil pour authentifier les utilisateurs des équipements numériques et des données « sensibles »

- Bannir les mots de passe de faible sécurité. Ex : 0000 ; 12345 ; 27081981
- Opter pour des mots de passe compris entre 8 et 12 caractères, comportant des majuscules, des minuscules, des chiffres et des caractères spéciaux (@.\#[)…
- Définir un mot de passe unique pour chaque service / utilisateur.
- Ne pas conserver les mots de passe dans un fichier ou sur des post-it.
- Ne pas pré-enregistrer les mots de passe dans les navigateurs.
- Favoriser l'utilisation d'un logiciel de gestion des mots de passe.

Règle n° 3

Mettre à jour ses logiciels

Des vulnérabilités existent pour chaque système d'exploitation, application, logiciel. Quand elles sont découvertes, les éditeurs les corrigent et « poussent » des mises à jour de leurs solutions.

- Avoir une politique de mise à jour régulières des solutions installées sur le réseau/postes quand ceci est possible.
- Utiliser des sites internet officiels des éditeurs pour le téléchargement des mises à jour.

Règle n° 4

Bien sauvegarder vos données

Aujourd'hui, beaucoup trop d'entreprises ne prêtent pas assez attention à leur système de sauvegarde. Un système de sauvegarde efficace vous permettra de palier à un dysfonctionnement de vos systèmes et aux attaques.

- Effectuer des sauvegardes régulières : quotidiennes et/ou hebdomadaires
- « Externaliser » une copie de sauvegarde de vos données.
- S'informer des lieux de sauvegardes de vos données. Certains métiers obligent à certains types de sauvegardes : médecins, cabinets d'analyse médicale, notaires, mairies, …

Dans 60% des cas, la perte totale de données dans une PME/PMI = disparition de l'entreprise dans les 6 mois !

80 % des entreprises ayant subi un sinistre informatique majeur avec perte de données déposent le bilan dans les 2 années qui suivent

Règle n° 5

Vigilance sur les mails

Les mails et leurs pièces jointes jouent souvent un rôle majeur dans la diffusion des attaques informatiques. Il convient donc d'être méfiant sur les messageries professionnelles et personnelles.

- Vérifier l'identité de l'expéditeur et la fiabilité de son adresse mail
- N'ouvrir que les pièces jointes provenant de personnes de confiance. En cas de doute, n'hésitez pas à vous rapprocher de votre entourage (ou service informatique) pour avis.
- Certains liens figurant dans les mails peuvent vous emmener vers des fichiers / pages internet malveillants. Avant de cliquer sur les liens, vérifier la cohérence de l'adresse de destination en passant votre souris sur ces derniers
- Ne pas répondre à une demande d'information personnelle ou confidentielle lorsque vous avez un doute. Il pourrait s'agir d'attaque par hameçonnage ou phishing.

880 millions d'emails de phishing détectés en 2018

Selon une étude de Vadesecure, 91 % des attaques proviennent de l'ouverture d'emails

Règle n° 6

Sécuriser vos accès wifi

Les connexions filaires sont recommandées pour les réseaux d'entreprises. Cependant vous pouvez être amené à utiliser des réseaux Wifi. Ces réseaux doivent être sécurisés, des personnes malveillantes peuvent s'introduire dans vos systèmes d'information via les technologies sans fil.

- Ne laissez pas votre réseau Wifi sans sécurisation par mot de passe. Chiffrement WPA2 et WPA-AES à activer (éviter le chiffrement Wep)
- Modifier le mot de passe par défaut car il est bien souvent affiché sur la box internet. Changez le régulièrement.
- Lorsque cela est possible, mettre à disposition 2 réseaux wifi distincts: un donnant accès au réseau de l'entreprise, l'autre donnant accès à Internet. Ces deux réseaux n'ayant pas de liaison « informatique ».
- Lorsque vous êtes en mobilité, n'utiliser que des réseaux wifi sécurisés.

Règle n° 7

Scinder les usages professionnels // personnels

Certains utilisateurs utilisent leurs outils professionnels à des fins personnelles ou vice versa. Cette pratique pose des problèmes en matière de sécurité informatique et de sécurisation des données : fuites de données, intrusions, vol ou pertes d'appareils, …

- Scindez les mails professionnels et personnels , évitez les transferts entre vos différentes boites mails.
- N'utilisez pas votre ordinateur professionnel pour des usages personnels (réseaux sociaux, achats en ligne,,,,)
- Evitez de connecter à votre ordinateur professionnel des supports amovibles.
- N'hébergez pas de données professionnelles sur vos outils personnels.

Règle n° 8

Attention aux paiements sur internet

Le développement des commandes via internet n'est plus à prouver. De nombreux sites en profitent pour tomber « amoureux » de vos comptes en banque.

Des vérifications s'imposent :

- Contrôlez l'exactitude de l'adresse du site internet sur lequel vous souhaitez effectuer une commande.
- Au moment du paiement, assurez-vous de la mention « https » est bien présente dans l'adresse du site web.
- Les navigateurs internet vous donnent des indices : cadenas, boutons check, …
- Ne donnez pas vos codes confidentiels de CB, utilisez les codes de confirmation par sms / application, …

Règle n° 9

Il n'y a pas que les ordinateurs…

Aujourd'hui, beaucoup d'entre nous se concentrent sur la sécurisation des réseaux en les associant uniquement aux ordinateurs. Les smartphones et les tablettes tactiles peuvent aussi générer des perturbations dans votre réseau informatique.

- Ne donnez l'accès à ces outils qu'aux personnes de confiance et pour une utilisation professionnelle.
- N'installez que des applications certifiées et officielles.
- En plus du code PIN, demandez à vos utilisateurs de créer des codes d'accès aux différents terminaux et les configurer pour un verrouillage automatique.
- Ne pré-enregistrez pas des mots de passe sur les terminaux.

N°10 - Pour aller plus loin…

Préconisations complémentaires

- Désignez un référent « informatique » dans l'entreprise, c'est **LA** personne qui centralisera les besoins et sera garante des bonnes pratiques
- Rédigez et affichez une charte interne des bonnes pratiques informatiques.
- Assurez-vous de disposer d'antivirus, de pare-feu, de mises à jour régulières des solutions, d'un routeur sécurisant le réseau et les entrées extérieures, d'un système de supervision générale des serveurs, …
- Assurez-vous d'un système de sauvegarde efficace. Préconisation = opter pour un système en local et en externalisé, autonome et supervisé.
- Equipez-vous d'une solution de sécurisation des emails, qui les ouvre dans des serveurs distants (bacs à sable) et vérifie tous les contenus, liens, et PJ, avant transfert dans vos boîtes mails,
- Veillez à l'analyse des supports amovibles qui seraient connectés aux postes.
- Eteignez les ordinateurs quotidiennement afin de procéder à leur réinitialisation ainsi qu'à l'installation des mises à jours.
- Prévoyez un redémarrage programmé des serveurs pour les mêmes raisons.