GUIDE DES BONNES PRATIQUES DE SECURITE INFORMATIQUE

La sécurité de votre réseau, un enjeu majeur

De nos jours, la sécurité est au cœur de notre usage informatique. Chaque faille peut être exploitée et les conséquences sont importantes.
Certaines actions peuvent être facilement mises en place pour limiter les intrusions.

La recette d'une bonne protection

Bien sûr, la sécurité est avant tout logicielle et matérielle. Des solutions sont indispensables, a minima, pour assurer le 1er niveau de sécurité (Antivirus, sauvegardes…)

Une protection logicielle…

Mais elle dépend aussi et surtout d'un bon usage de l'informatique. Des bonnes habitudes sont à prendre au quotidien, pour éviter les erreurs de sécurité propices aux intrusions malveillantes.

… Et une sensibilisation des utilisateurs

Ne négligez pas les aspects humains dans votre réflexion sur la sécurité !

OPTIMISATION DES OUTILS DE SECURITE

Sécurité matérielle : Un rempart aux intrusions

La sécurité matérielle passe par plusieurs outils/actions à mettre en place. En voici une liste non exhaustive :

Mettez l'accent sur la sauvegarde

- Double sauvegardes minimum
- Dont une hors ligne
- Avec un plan de reprise d'activité documenté

Bloquer les virus et les menaces plus évoluées…

- Un antivirus managé en temps réel
- Un boitier de sécurité perfectionné et paramétré avec précision avec un filtrage sur les flux **entrants** et **sortants**
- Une analyse des menaces évoluées
- Et également une protection de vos accès personnels avec un outil de MFA : authentification à plusieurs facteurs

Protection de votre environnement

- Des comptes utilisateurs non administrateur de leurs postes
- Des locaux sécurisés avec des accès restreints (salle informatique ou bureau RH)
- Des PCs utilisateurs maitrisés : chiffrage du disque dur, mises à jour hebdomadaires, interdiction des supports amovibles
- Sécurisation des matériels mobiles : VPN, politique de mot de passe fort

DU BON USAGE DU RESEAU INFORMATIQUE

Sensibilisation des utilisateurs : la clé pour limiter les intrusions

Les meilleurs outils de sécurité ne sont rien si vos utilisateurs ont un comportement préjudiciable avec les outils qu'ils ont à leur disposition. Entre usage et sécurité, choisissons la sécurité !

Usage du Cloud

- Ne pas fournir son mail pro sur des sites privés
- Limiter son usage privé sur le réseau pro
- Ne pas télécharger de fichiers exécutables
- Ne pas consulter de site web non sécurisé
- Ne pas consulter ses données pro via un WiFi public

Protéger son matériel : les bons réflexes

- Signaler toute perte de matériel avec un accès au réseau d'entreprise
- Verrouiller sa session dès qu'on s'absente de son bureau
- Protéger son réseau personnel quand on est en télétravail

Gestion des accès utilisateurs

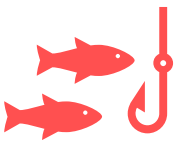
- Garder son mot de passe pour soi, ne pas le divulguer (même sous la pression)
- Si vous devez le faire, 2 règles : le changer après, et ne pas envoyer dans un même mail votre identifiant et votre mot de passe
- Changez souvent votre mot de passe

QUELQUES CONSEILS CONTRE LES INTRUSIONS

Que faire face à une tentative d'intrusion

En bonus, voici quelques conseils à appliquer pour éviter les attaques ciblées par des hackers misant sur la confiance des utilisateurs.

Mails frauduleux ou phishing : ne soyez pas la belle prise



- Méfiez-vous des mails qui vous promettent une somme d'argent, ou qui vous font peur, avec un lien pour redonner vos identifiants
- Vérifiez l'adresse d'expéditeur
- Vérifiez le lien : le nom est sûrement presque pareil que le nom « officiel » : microsaft.com
- Allez sur le site officiel vérifier vos paramètres

Ingénierie sociale : un mot compliqué pour un concept simplissime

- Méfiez-vous des mails ou appels visant à vous soutirer des informations de l'entreprise
- Par exemple : si vous recevez une demande semblant venir de votre direction pour effectuer un virement d'une somme d'argent
- Appelez le pseudo destinataire de la demande ou demandez des détails

Être en alerte, partout, tout le temps !

En étant vigilant, sans devenir paranoïaque, vous pouvez repérer les risques d'intrusion frauduleuses !

koesio