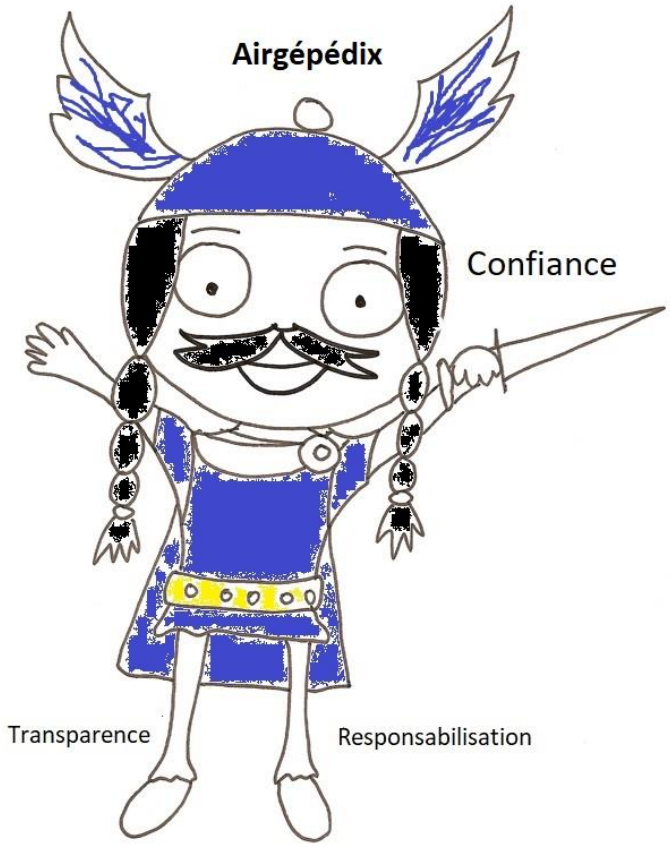
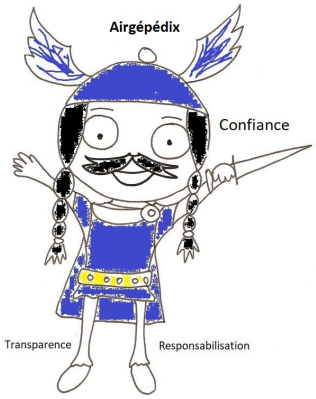


Airgépédix fait un nouveau point sur la sécurité

#BIZDEV34



#BIZDEV34

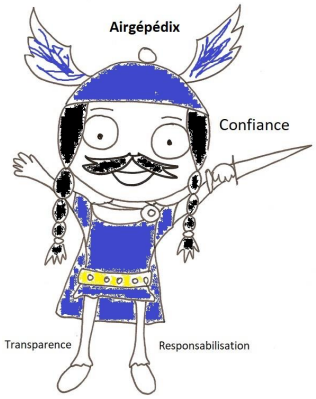
L'année 2020 est l'année record des attaques par ramsoware et attaques informatiques diverses (phising…). Outre les risques de perte d'activité, ces problèmes qui concernent toutes les entreprises quelle qu'en soit la taille introduisent également un risque lié au RGPD.

Ce que dit le RGPD de vos obligations :

Article 32 – Sécurité du traitement

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, **le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité** adapté au risque, y compris, selon les besoins:

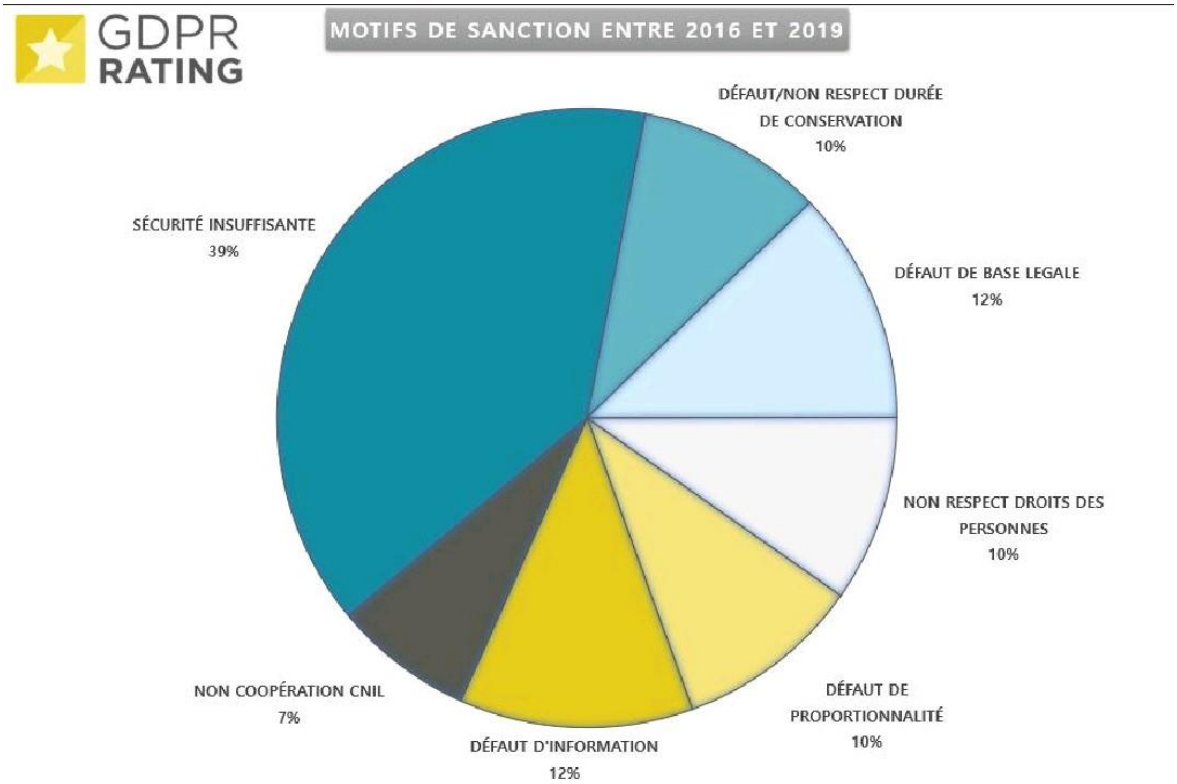
- La pseudonymisation et le chiffrement des données à caractère personnel
- Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement

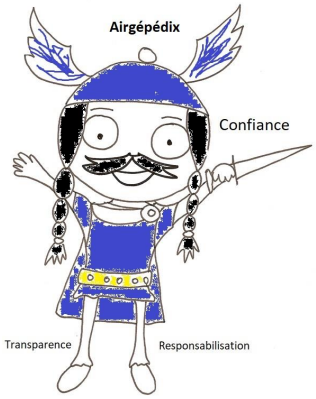


#BIZDEV34

- Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Par ailleurs si nous observons les raisons pour lesquelles la CNIL a le plus sanctionné entre 2016 et 2019 nous observons :



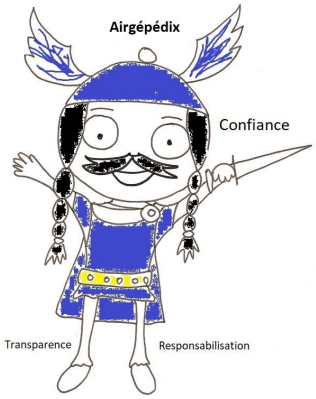


#BIZDEV34

Alors comment limiter ces risques ? Faut-il dépenser des sommes folles ?

Les 12 règles à mettre en place selon l'ANSII (**A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation)

1. Choisir avec soin ses mots de passe
2. Mettre à jour régulièrement vos logiciels
3. Bien connaître ses utilisateurs et ses prestataires
4. **Effectuer des sauvegardes régulières (*)**
5. Sécuriser l'accès Wi-Fi de votre entreprise
6. Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur
7. Protéger ses données lors de ses déplacements
8. Être prudent lors de l'utilisation de sa messagerie
9. Télécharger ses programmes sur les sites officiels des éditeurs
10. Être vigilant lors d'un paiement sur Internet
11. Séparer les usages personnels des usages professionnels
12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique



#BIZDEV34

(*) La seule stratégie de sauvegarde qui vous prémunisse est la règle suivante :

3,2,1 ou c'est 0 !

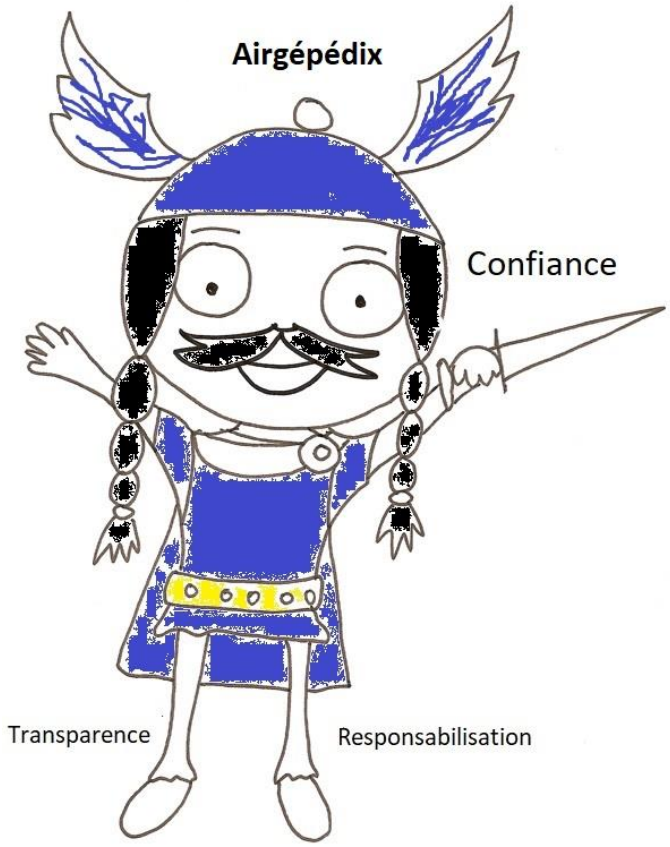
En clair me direz-vous à juste titre ,

- 3 sauvegardes sur au moins
- 2 supports différents dont
- 1 à l'extérieur de l'entreprise (sauvegarde en ligne)

Bien entendu les données sauvegardées sont cryptées et des tests de restauration effectués tous les 6 mois…

… je sais je me répète ☺

L'application de ces 12 règles ne vous coûtera pas beaucoup de sesterces et vous mettra à l'abri de graves déconvenues !



Pour me contacter :

www.bizdev34.fr
francois@bizdev34.fr
06 16 46 35 48

#BIZDEV34