Fiche Info

eWBS
e-Wallonie-Bruxelles Simplification

Sécurité des informations

Toute entreprise ou organisation a besoin de rassembler, compiler et traiter des informations dans son propre système informatique. Chacune crée de la valeur en traitant de l'information nécessaire à l'atteinte de ses objectifs. L'information constitue donc un capital essentiel à tout organisme pour son activité. Elle doit en conséquence être protégée de manière appropriée.

L'information : un patrimoine à protéger

En dehors des locaux et des appareils informatiques, tout ce qui compose le système d'information d'une organisation est immatériel. Différents éléments rendent disponibles et permettent l'utilisation de ce patrimoine immatériel :

- les systèmes informatiques : logiciels, pc, serveurs, imprimantes, téléphones…
- les organisations : personnes, supports papier…
- les locaux : bâtiments, postes de travail, lecteurs de badge…

Tout cet environnement matériel est vulnérable ! Ils représentent en conséquence un danger potentiel pour l'information : les PC portables se volent, les réseaux se piratent, les personnes emportent des données, etc. Les scénarios sont infinis et en constante évolution. La convergence numérique par la multiplication des points d'entrée (tablette, smartphone…) accentue ce phénomène.

Information sécurisée

La sécurité d'une information se traduit à 3 niveaux :

- **Disponibilité :** l'information doit être accessible au moment voulu.
- **Confidentialité :** l'information doit être accessible uniquement par les personnes autorisées à les consulter ou les employer.
- **Intégrité :** l'information ne peut pas être modifiée ou détruite de façon non autorisée.

Que faut-il entendre par risque ?

Un risque sur la sécurité de l'information se définit par la combinaison d'une gravité (ampleur du risque lié à la nature des informations et au caractère préjudiciable des impacts potentiels) et d'une vraisemblance (faisabilité d'un risque). Pour qu'il y ait risque, il faut :

- Une **menace**, représentée par un humain ou un logiciel, malveillant ou non, interne ou externe.
- Une **vulnérabilité** qui sera exploitée par la menace.

Le saviez-vous ?

- 25% des fuites de données sont dues à des utilisateurs internes, par accident ou négligence.
- 100 nouveaux logiciels malveillants sont créés chaque minute.
- « 123456 » est le mot de passe le plus utilisé au monde, juste devant « password ».
- 75% des lignes téléphoniques à usage professionnel utilisent la technologie VoIP, nouvelle cible des cyber attaques.
- En moyenne, au cours des dernières années, en Belgique, plus de 300 entreprises ont été victimes quotidiennement de cyber-attaque. L'impact d'une perte de données ou d'une cyber-attaque peut être la cause :
  - de pertes financières (budget de l'institution concernée) ;
  - d'actions judiciaires (sanctions internes et condamnation de l'autorité) ;
  - de perte d'image (plaintes, altération grave au niveau national et international) ;
  - de dégâts environnementaux ;
  - de perturbations à l'ordre public ;
  - …

Février 2015

FÉDÉRATION WALLONIE-BRUXELLES
Wallonie

Fiche Info

Sécurité des informations

Pour en savoir plus sur la sécurité des informations
eWBS – Pôle organisationnel de la BCED
info@ensemblesimplifions.be

En Fédération Wallonie-Bruxelles
Boulevard Léopold II, 44
B-1080 Bruxelles
Tél. : +32 (0)2 413 25 10
Fax : +32 (0)2 413 35 10

En Wallonie
Chaussée de Charleroi,
83 B • 4e étage
B-5000 Namur
Tél. : +32 (0)81 40 98 00
Fax : +32 (0)81 40 98 01

1 - Promouvoir la sécurité en se posant les bonnes questions

En tant qu'utilisateur d'informations, notre activité est au cœur des enjeux liés à la sécurité. Pour l'optimiser, un bon point de départ est de se poser des questions comme :

- Le mot de passe de mon poste de travail est-il « robuste » et récent ?
- Le coffre de ma voiture est-il un lieu sûr pour ma tablette, mon pc portable ?
- Dois-je vraiment emporter ces données sensibles sur ma tablette ?
- Comment réagir quand une personne inconnue et non accompagnée erre dans les couloirs de mon service ?
- Est-ce normal de trouver des feuilles abandonnées près de l'imprimante ou la photocopieuse ?
- Dois-je prêter mon badge d'accès à un collègue qui a oublié le sien ?
- Le réseau WiFi public que je viens de détecter sur cette aire d'autoroute est-il fiable ?
- Est-ce normal de recevoir un mail d'un de mes collègues m'invitant à accéder à un site inconnu ?
- Puis-je consulter directement une clé USB trouvée dans le train ?
- …

2 - Promouvoir la sécurité en collaboration avec votre conseiller en sécurité

Véritable « omnipraticien de la sécurité », le Conseiller en sécurité conseille sa Direction au sujet de tous les aspects de la sécurité de l'information. Il a pour rôle de promouvoir les règles de sécurité liées à l'activité de son organisme, de contrôler les mesures de sécurité mises en place et d'émettre des avis de manière objective et autonome. Il exerce sa fonction en toute indépendance et ne peut exercer d'activités incompatibles avec sa mission.

Votre conseiller en sécurité doit être la première personne sollicitée pour améliorer la sécurité au sens large, signaler un incident ou obtenir de l'information. C'est votre point de contact interne pour la sécurité de l'information. Pour les seuls aspects liés à la sécurisation des échanges de données ou la mise en place de sources authentiques, l'équipe de la BCED constitue un support complémentaire.

3 - Promouvoir la sécurité des données partagées avec la collaboration de la BCED

La sécurité de l'information s'applique à tous les aspects de la sûreté, de la garantie, et de la protection d'une donnée ou d'une information, quelle que soit sa forme. La Banque Carrefour d'Echanges de Données (BCED) est ou outil qui y contribue.

La BCED assure le transport fiable et la distribution des données par des services d'accès hautement sécurisés dans le respect des prescrits de la loi sur la vie privée et des bonnes pratiques de la sécurité des systèmes d'information. La BCED se préoccupe tout particulièrement de la responsabilisation de chaque acteur (organisations, agents, sous-traitants,…) dans le cadre du partage de données à caractère personnel.

L'offre de services de la BCED dans le cadre du partage de données

- Avis de sécurité, analyses de risques dans le cadre de projets de partage de données.
- Sensibilisation des agents à la sécurité de l'information dans le cadre du partage de données.
- Aide ponctuelle et support aux conseillers en sécurité pour la rédaction et la mise en œuvre des mesures concernant le partage et le stockage de données au sein d'une politique de sécurité.

Février 2015

FÉDÉRATION WALLONIE-BRUXELLES

Wallonie