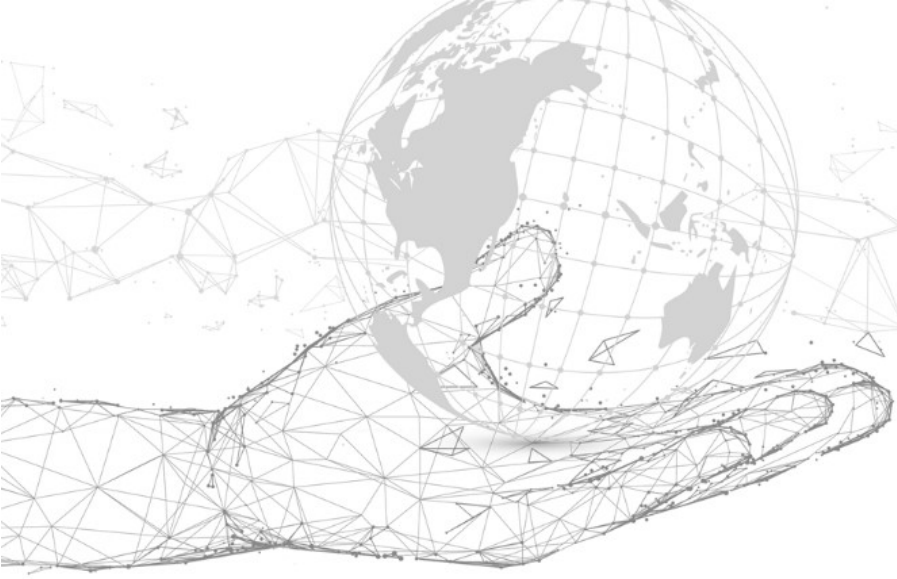


efcse.eu

VADE MECUM DE LA CYBERSECURITE

Guide d'hygiène digitale de protection du patrimoine informationnel de l'entreprise

Auteur : Olivier de MAISON ROUGE

Octobre 2017

PREAMBULE

Parce que la transformation numérique accroît de manière exponentielle le volume de données,

Parce que dans le digital la menace n'est pas virtuelle mais bien réelle,

Parce que 35% des incidents de sécurité informatique sont d'origine humaine,

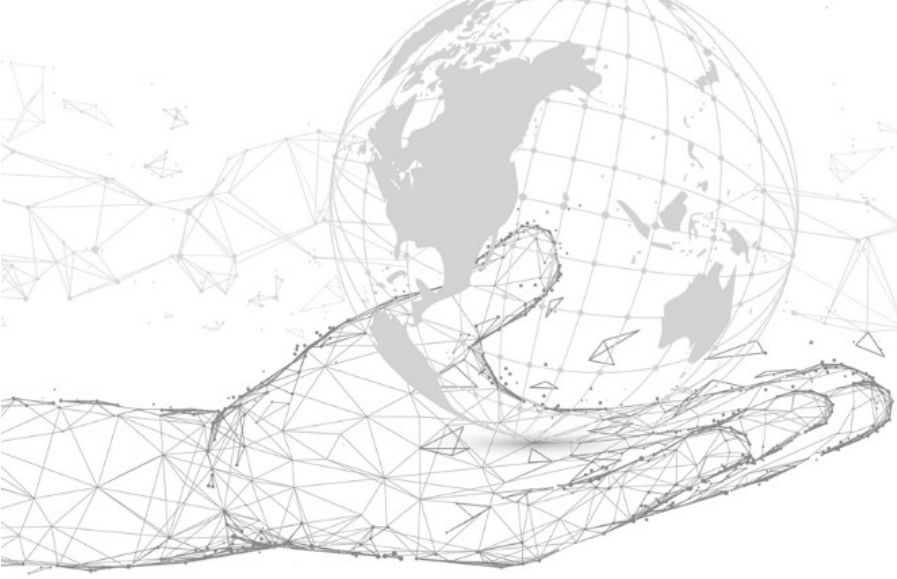
Parce que chaque atteinte critique aux systèmes d'information coûte en moyenne 700.000 € à l'entreprise,

Parce que dès lors la protection des données doit être une préoccupation quotidienne,

Et parce les informations sensibles constituent un outil de travail garant de la protection des emplois,

La cybersécurité est une exigence majeure pour la pérennité des acteurs et des activités économiques.

En réponse, l'European Federation of CyberSecurity Experts a élaboré ce vade mecum.



Vade mecum des 10 bonnes pratiques à implémenter au sein de chaque structure économique et humaine

1. DEFINIR une politique de sécurité globale, efficiente et transverse.

   Insérer dans le règlement intérieur de l'entité la dimension numérique et associer tous les acteurs supports de l'entreprise pour élaborer une politique cohérente et nécessaire à la permanence des informations sensibles de l'entreprise.

2. SENSIBILISER : sécuriser, c'est d'abord irriguer et diffuser les bonnes pratiques de précaution à l'attention de toutes les forces vives de l'entreprise.

   Une formation adaptée et continue doit être réalisée en interne pour assurer à tous les collaborateurs une sensibilisation avec le souci d'agir au quotidien conformément aux règles de sécurité en usage et leur permettre d'avoir conscience des menaces pour les activités et l'entreprise mais aussi l'usage des données personnelles.

3. SE CONFORMER à la règlementation en vigueur : l'effort de conformité doit s'appliquer de manière à être toujours au niveau requis minimum de protection numérique érigé par les textes et les institutions, eu égard au domaine d'activité de l'entreprise.

   Une veille règlementaire et un dialogue permanent avec les institutions doivent permettre d'informer et de conserver un niveau élevé de conformité.

4. ORGANISER la protection physique des installations et des infrastructures : la sécurité des réseaux et des informations n'exclue pas la prise en compte des sinistres.

   Une politique de sûreté-sécurité robuste des supports physiques et logiques doit être intégrée dans le cadre général de la protection des données de l'entreprise, par l'établissement d'une cartographie des lieux tant de stockage que de traitement des données.

5. PRATIQUER un examen régulier des risques et des vulnérabilités : un audit de sécurité numérique sera régulièrement effectué de manière à mettre en œuvre une adaptation nécessaire et évolutive en intégrant des mises à jour nécessaires pour pallier les failles de sécurité recensées.

   L'entreprise doit procéder à une mise à jour de la cartographie et une révision constante des outils de sécurité dédiés. Une telle recension conduira à assurer une mise à niveau de l'ensemble des politiques de sécurité des données, et notamment des données personnelles.

6. VEILLER à intégrer une politique de sécurité adaptée aux besoins de l'entreprise. Cela nécessite une connaissance profonde des données traitées afin de pouvoir opérer une classification des moyens de protection dédiés selon leur nature

   Toute politique de sûreté-sécurité des données « sensibles » et « personnelles » doit être élaborée spécifiquement en tenant compte de l'activité de l'entreprise selon le territoire considéré, et ne pas s'en tenir à apposer un cadre réalisé pour d'autres acteurs.

7. CLOISONNER les informations en fonction du profil de métiers destinés à y accéder. Tous les collaborateurs n'ont pas besoin de connaître toutes les données de l'entreprise.

   Selon la nature des fonctions et en considération du niveau de poste et/ou de qualification, chaque salarié devra posséder un code d'accès distinct, donnant lieu à un accès identifié et séparé des données, tout en assurant leur traçabilité. Organiser et régir les restrictions d'accès, via des paramètres de sécurité opérationnels et traçables.

8. INTEGRER une politique proactive de résilience : savoir gérer et répondre aux crises rencontrées. Anticiper les urgences et les indisponibilités. Intégrer un dispositif interne d'alerte.

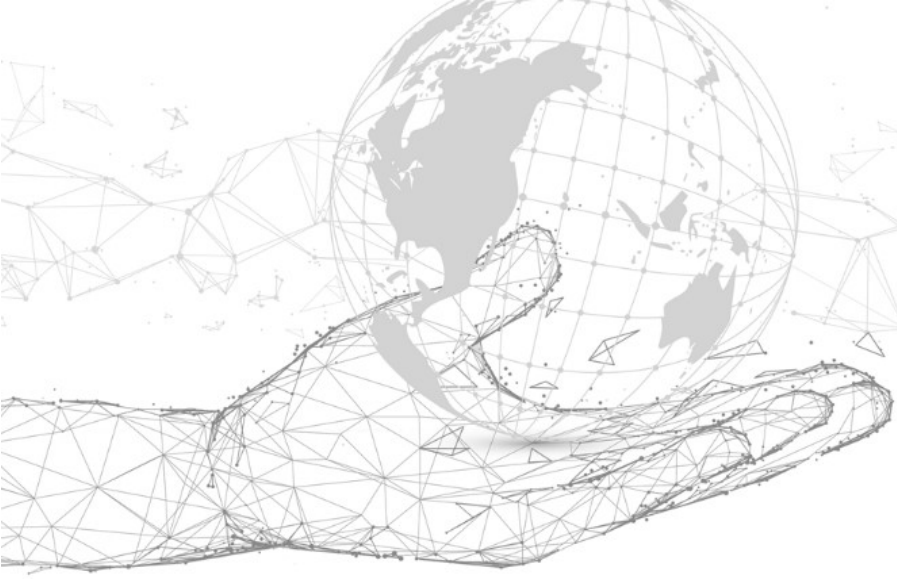
   La politique de sûreté-sécurité doit intégrer un exercice de gestion de crise pour savoir réagir aux cyberattaques de toute nature, et être en mesure de restituer dans un temps donné selon les priorités toutes les données présentes antérieurement au sein de l'entreprise.

9. RAPPELER les règles essentielles de travail et connexion à distance et/ou en déplacement : éviter l'usage des plateformes de partage et les moyens de connexion publics. Ne transférer que les fichiers utiles.

   Faire œuvre de pédagogie quant à l'usage des outils numériques mobiles hybrides contre le vol des supports, la captation technique des données, … notamment lors des déplacements en France ou à l'étranger.

10. INTEGRER des systèmes d'authentification forte : recourir au chiffrement des données stratégiques ou sensibles.

    Assurer une mise à niveau suffisante des codes d'accès et mots de passe. Définir et mettre en œuvre une politique d'identité numérique avec les collaborateurs clefs, et en assurer le suivi.



Extrait du manifeste de l'EFCSE :

> « *La cyber sécurité n'est certes pas une préoccupation nouvelle. En revanche, la prise en considération des risques numériques appelle à un devoir constant de vigilance et de remise en cause. Elle met en exergue le besoin d'innovation permanente pour les organismes, les institutions et les entreprises concernées par les atteintes à leurs informations essentielles. Il leur appartient de parer chaque jour de nouvelles attaques et de nouveaux modes d'ingénierie, lesquels sont désormais multidimensionnels.*
>
> *Le cyber espace, ouvert au grand public depuis plus de vingt ans désormais, est un monde d'échanges de données – constituant le support originel de ces flux constants – un lieu de communication à l'échelle planétaire et un vaste champ dématérialisé.*
>
> *Mais indépendamment de ces immenses territoires largement ouverts, les menaces sont proportionnelles et affectent toute forteresse, dont aucune n'est imprenable.* »