matière d'incendie et de vol, notamment le vol ou la malversation des données numériques. Et techniquement parlant, la cyberprévention touche aussi directement les systèmes actuels de prévention des incendies et des vols : il ne faudrait quand même pas qu'un système de détection incendie connecté devienne la porte d'entrée du réseau IT !

Amis lecteurs, suivez attentivement cette rubrique et vous mettrez toutes les chances de votre côté pour préserver vos activités !

Que pensez-vous des étapes entamées par l'Union européenne en matière de réglementation de la cybersécurité ?
AV : L'approche de l'Europe est à mon sens très intelligente : elle impose des lignes d'actions efficaces tout en préservant les idéaux démocratiques et la liberté de ses citoyens. Aborder la cybersécurité sous l'angle autocratique et dictatorial serait tellement plus facile, mais ce serait mettre en péril la stabilité interne de l'Europe. La Directive NIS, le Règlement eIDAS, le RGPD, le Cyber Act, la création de ENISA, pour ne citer qu'eux, sont autant d'outils pour assurer la meilleure résilience face aux cyberattaques.

En fait, l'Europe utilise subtilement le concept de la 'Nouvelle Approche' adoptée en 1985 qui impose des lignes directrices aux États membres, tout en n'imposant pas les modalités d'exécution précises pour ne pas s'ingérer dans la souveraineté de chaque État. C'est déjà un fait pour les produits via le futur Règlement européen concernant les exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques[3].

LES « FUNDAMENTALS » EN MATIÈRE DE CYBERSÉCURITÉ

Les Cyberfundamentals, promotionnés par le CCB, sont des mesures concrètes permettant aux entreprises et aux organisations :

- de mieux protéger leurs données,
- de réduire de manière significative le risque des cyberattaques les plus courantes,
- d'accroître leur cyber-résilience en général.

Ils sont structurés selon quatre niveaux, contenant chacun un peu plus de mesures que le précédent. Le premier niveau est SMALL, suivi de BASIC, IMPORTANT et ESSENTIAL. L'objectif est qu'à terme, chaque PME et chaque organisation de notre pays atteigne le niveau BASIC.

Le *Cyberfundamentals Framework* s'articule autour de cinq fonctions essentielles : *identifier, protéger, détecter, répondre et récupérer* (Fig. 1). Ces fonctions favorisent la communication autour de la cybersécurité entre les experts du domaine et les parties prenantes, afin que les risques liés à la cybersécurité puissent être intégrés dans la stratégie globale de gestion des risques des organisations. Il permet également d'accroître la résilience des entreprises face aux cyberattaques.

Pour plus d'informations : https://ccb.belgium.be/fr/cyber-fundamentals-framework

© N. Hanacek / NIST

Fig. 1 : Aux cinq principaux piliers d'un programme de cybersécurité réussi (identifier, protéger, détecter, répondre et récupérer), le NIST vient d'en ajouter un sixième, la fonction «gouverner», qui souligne que la cybersécurité est une source majeure de risque pour l'entreprise et qu'elle doit être prise en compte par la haute direction.

3 *Voir article « Appareils connectés et cybersécurité : l'UE passe à l'Act ! », dans Fire & Security Magazine n° 31 - juin 2023, pp. 29-32.*