king tot brand en diefstal, in het bijzonder diefstal of verduistering van digitale gegevens. En technisch gezien is cyberpreventie ook rechtstreeks van invloed op de huidige brand- en diefstalpreventiesystemen: we zouden niet willen dat een aangesloten branddetectiesysteem de toegangspoort wordt tot het IT-netwerk!

Beste lezers, volg deze rubriek zorgvuldig en u zult er alles aan doen om uw bedrijf te beschermen!

Wat vindt u van de stappen die de Europese Unie heeft ondernomen om cyberbeveiliging te reguleren?
AV: Naar mijn mening is de aanpak van Europa zeer intelligent: het legt effectieve actielijnen op en behoudt tegelijkertijd de democratische idealen en vrijheid van zijn burgers. Het zou veel gemakkelijker zijn om cyberveiligheid vanuit een autocratische en dictatoriale hoek te benaderen, maar dat zou de interne stabiliteit van Europa in gevaar brengen. De NIS-richtlijn, de eIDAS-verordening, de AVG (GPDR), de Cyberwet en de oprichting van ENISA, om er maar een paar te noemen, zijn allemaal instrumenten om ervoor te zorgen dat cyberaanvallen zo goed mogelijk worden opgevangen.

In feite maakt Europa subtiel gebruik van het concept van de 'Nieuwe Aanpak' uit 1985, die de lidstaten richtlijnen oplegt zonder expliciete uitvoeringsprocedures op te leggen om niet in te grijpen in de soevereiniteit van elke staat. Dit is al gedaan voor producten via de toekomstige Europese verordening over horizontale cyberveiligheidseisen voor producten met digitale componenten[3].

En hoe verloopt het in België?
AV: Volgens de DESI 2022-index[4] (een jaarlijkse ranglijst opgesteld door de Europese Commissie) staat België op de 16e plaats, iets onder het Europese gemid-

CYBERFUNDAMENTALS FRAMEWORK

De Cyberfundamentals, gepromoot door het CCB, zijn concrete maatregelen waarmee bedrijven en organisaties:

- hun gegevens beter te beschermen,
- het risico op de meest voorkomende cyberaanvallen aanzienlijk te verkleinen,
- hun algehele cyberweerbaarheid te vergroten.

Ze zijn gestructureerd volgens vier niveaus, die elk iets meer maatregelen bevatten dan het vorige. Het eerste niveau is SMALL, gevolgd door BASIS, BELANGRIJK en ESSENTIËEL. De bedoeling is dat uiteindelijk elk kmo-bedrijf en elke organisatie in ons land het BASIS-niveau bereikt.

Het Cyberfundamentals Framework is opgebouwd rond vijf belangrijke functies: identificeren, beschermen, detecteren, reageren en herstellen (fig. 1). Deze functies bevorderen de communicatie rond cyberbeveiliging tussen experts op dit gebied en belanghebbenden, zodat cyberbeveiligingsrisico's kunnen worden geïntegreerd in de algehele risicomanagementstrategie van een organisatie. Het helpt ook om bedrijven weerbaarder te maken tegen cyberaanvallen.

Meer informatie: https://ccb.belgium.be/fr/cyberfundamentals-framework

© N. Hanacek / NIST

Fig. 1: Aan de vijf hoofdpijlers van een succesvol cyberbeveiligingsprogramma (identificeren, beschermen, detecteren, reageren en herstellen) heeft NIST recent een zesde toegevoegd, de functie "besturen", die benadrukt dat cyberbeveiliging een belangrijke risicobron voor het bedrijf is en dat het senior management er rekening mee moet houden.

3 *Zie artikel "Verbonden apparaten en cyberbeveiliging: de EU onderneemt actie!", in Fire & Security Alert Magazine nr. 31 - juni 2023, pp. 29-32.*
4 *Meer informatie over de DESI-index 2022: https://economie.fgov.be/nl/themas/online/ict-belgie/barometer-van-de/desi-index-2022*