FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

Cybersécurité pour PME en Belgique

Guide PME

Votre PME fait tourner l'économie belge. Mais elle est trop grande pour passer inaperçue et trop petite pour avoir un CISO à temps plein. Ce guide n'est pas un catalogue de peur. C'est un plan d'action écrit par des gens qui connaissent votre réalité.

Scannez pour acceder a la version en ligne

contact@flashmodz.be | +32 471 87 87 07

https://flashmodz.be

SYNTHÈSE EXÉCUTIVE

FlashModz

L'essentiel en 5 minutes

Trop grande pour passer inaperçue, trop petite pour avoir un CISO. Voici votre plan d'action.

1

Vous êtes ciblé·e en permanence, pas par hasard mais par algorithmes

Les attaquants ne choisissent pas leurs victimes : ils scannent en continu et exploitent toutes les failles ouvertes. Exchange non patché, VPN sans 2FA, NAS exposé sur Internet. Une PME touchée perd des semaines de production, des clients, et parfois la confiance du marché.

2

NIS2 vous concerne, et la responsabilité du dirigeant est personnelle

Si vous avez plus de 50 employés OU plus de 10M€ de CA dans un secteur visé (santé, énergie, transport, fabrication, numérique, alimentaire), NIS2 s'applique à vous. Amendes jusqu'à 10M€ ou 2% du CA mondial (essentielles), 7M€ ou 1,4% (importantes). Et l'art. 20 prévoit la responsabilité personnelle des organes de direction.

3

Le vrai problème, c'est le manque de visibilité

Vous ne savez pas ce qui est exposé, ce qui est vulnérable, ce qui est sauvegardé. Personne en interne n'a le temps. Sans supervision, une intrusion peut passer inaperçue pendant des mois : le temps pour les attaquants de tout regarder, clients, plans, finances.

4

Une PME peut atteindre la même rigueur qu'un grand compte

Détection managée (EDR/MDR), vCISO à temps partagé, audit sur base du référentiel CyFun ou NIST CSF, formation anti-phishing pratique. Les outils et compétences existent, à un coût sans commune mesure avec celui d'un seul incident. C'est notre métier de rendre ça accessible.

5

Une feuille de route 90 jours change tout

Les 90 premiers jours posent l'essentiel de la posture cyber : audit, durcissement des accès, segmentation réseau, sauvegardes immuables, plan de réponse aux incidents. C'est balisable, c'est mesurable, c'est livrable.

Et maintenant ?

Les pages qui suivent détaillent chacun de ces points avec exemples, chiffres et actions concrètes.

Document conçu pour PME (10 à 250 employés) · Lecture : ~15-20 min · Édition 2026

Table des matières

Naviguez rapidement vers les sections qui vous concernent.

Le marché belge en chiffres

Chapitre 1

18/10/2024

la loi NIS2 belge est en vigueur ; le CCB mène des contrôles actifs depuis 2026

Sources : textes officiels (NIS2, RGPD, DORA) et publications des éditeurs cités

10 M€

amende NIS2 maximale pour une entité essentielle, ou 2% du CA mondial (7 M€ ou 1,4% pour une entité importante)

24h

délai NIS2 pour l'alerte initiale au CCB après un incident significatif

3 voies

pour démontrer la conformité NIS2 : certification CyFun, ISO 27001 ou inspection du CCB

Contexte & enjeux

Soyons directs : si vous dirigez une PME en Belgique, vous êtes probablement la cible idéale pour un cybercriminel. Pas parce que vous avez des millions en banque, mais parce que vos défenses sont faibles et que personne ne surveille.

"On est trop petits pour être ciblés", c'est la phrase qu'on entend le plus souvent. Et c'est la plus dangereuse. Les attaquants ne choisissent pas leurs victimes à la main. Ils scannent des millions d'adresses IP et exploitent la première faille trouvée. Votre serveur Exchange sans mise à jour, votre VPN sans 2FA, votre NAS accessible depuis Internet : ce sont des portes grandes ouvertes.

Pendant ce temps, le cadre légal s'est durci. La loi NIS2 belge est en vigueur depuis le 18 octobre 2024. Elle concerne bien plus de PME qu'on ne le croit, les amendes montent jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires mondial pour les entités essentielles (7 millions ou 1,4% pour les entités importantes), et l'article 20 rend les dirigeants personnellement responsables. L'échéance du 18 avril 2026 pour les entités essentielles est passée : le CCB est en phase de contrôle actif. Le "on verra plus tard" n'est plus une option.

Mais le vrai problème des PME, ce n'est pas l'argent. C'est le manque de visibilité. Vous ne savez pas ce qui est exposé, ce qui est vulnérable, ce qui est sauvegardé ou non. Et personne en interne n'a le temps (ou les compétences) de s'en occuper.

C'est exactement là que FlashModz Enterprise intervient. On vient du monde des grands comptes : audits, gouvernance cyber, gestion d'incidents à grande échelle. Ces ressources humaines, ces connaissances et ces outils n'étaient accessibles qu'aux grandes entreprises. On les a rendus

> *"La cybersécurité d'une PME ne se mesure pas au nombre d'outils déployés, mais à la rapidité avec laquelle elle peut redémarrer après une attaque."*
>
> — Jérémy Manet, FlashModz Enterprise

Les menaces qui pèsent sur vous

Chapitre 2

Ces risques sont réels, documentés, et touchent des entreprises belges chaque semaine.

Ransomware : des semaines de production perdues

Un seul employé clique sur un faux email de livraison, et toute la chaîne de production s'arrête. Sans segmentation réseau ni sauvegardes hors ligne, le ransomware chiffre tout, y compris les sauvegardes locales. Le CCB traite ce type d'incident en continu via le CERT.be : les PME manufacturières sont des cibles privilégiées.

Vos plans, vos clients, vos offres : copiés

Quelqu'un est peut-être dans votre réseau en ce moment, en train de copier vos fichiers les plus précieux. L'espionnage économique ne fait pas de bruit : sans surveillance des connexions et des flux sortants, une intrusion peut durer des mois. Quand on s'en aperçoit, c'est souvent trop tard.

Le faux email du patron

Un fraudeur usurpe l'adresse email du dirigeant et envoie un ordre de virement "urgent et confidentiel" au comptable. Cette fraude au CEO fait l'objet de mises en garde régulières de Febelfin et de la police fédérale. La parade est simple : toute demande de virement inhabituelle se vérifie par téléphone, sans exception.

Votre prestataire IT se fait pirater, et vous avec

Votre fournisseur de paie, votre logiciel ERP, votre hébergeur : chacun d'entre eux peut devenir le point d'entrée vers votre entreprise. Les attaques par la chaîne d'approvisionnement sont en forte hausse selon l'ENISA. Vous ne contrôlez pas la sécurité de vos tiers, mais vous en subissez les conséquences.

NIS2 vous concerne, et vous ne le savez peut-être pas

La loi NIS2 belge, en vigueur depuis le 18 octobre 2024, touche bien plus de PME qu'on ne le pense : santé, énergie, transport, alimentaire, numérique, fabrication. Alerte au CCB sous 24h, gestion des risques documentée, responsabilité personnelle du dirigeant (art. 20). Amendes jusqu'à 10 M€ ou 2% du CA mondial pour les entités essentielles, 7 M€ ou 1,4% pour les importantes.

Mythes vs Réalité

Chapitre 3

Six idées reçues qui empêchent d'agir — et ce qu'en disent les chiffres.

01

ON ENTEND SOUVENT

Notre PME de 60 personnes n'intéresse pas les hackers. Ils visent les grosses boîtes, pas nous.

EN RÉALITÉ — *CCB · CERT.be*

Les attaquants automatisent leurs scans : ils ne choisissent pas à la main. Le CCB le rappelle régulièrement : les PME belges figurent en bonne place parmi les victimes. Vous n'êtes pas ciblé·e parce que vous êtes spécial·e, vous êtes ciblé·e parce que vous êtes joignable et exposé·e.

02

ON ENTEND SOUVENT

On a une boîte d'infogérance qui gère tout. La cyber, c'est leur problème.

EN RÉALITÉ — *ENISA Threat Landscape*

Votre prestataire gère l'opérationnel, pas la stratégie cyber, pas la conformité NIS2, pas la formation des équipes, pas la réponse aux incidents. Et l'ENISA classe les attaques via la chaîne d'approvisionnement parmi les menaces majeures : votre prestataire peut aussi être le point d'entrée.

03

ON ENTEND SOUVENT

NIS2 ne concerne que les opérateurs essentiels du type Engie ou Belfius.

EN RÉALITÉ — *Loi NIS2 belge · 18/10/2024*

NIS2 cible TOUS les secteurs essentiels ET importants : santé, fabrication, numérique, alimentaire, transport, eau, postaux, dès 50 employés ou 10M€ de CA. Et les sous-traitants par ricochet. Si une grande entreprise vous demande votre conformité NIS2 ou une certification CyFun, c'est que vous êtes concerné·e.

04

ON ENTEND SOUVENT

On a fait un audit ISO il y a 2 ans, on est en règle.

EN RÉALITÉ — *Processus continu*

La menace évolue en permanence. Un audit qui a 2 ans ne vous dit rien sur votre exposition actuelle (nouvelles vulnérabilités, nouveaux services exposés, nouveaux employés, nouveaux fournisseurs). La cybersécurité est un processus continu, pas une certification. Même la certification CyFun se maintient dans le temps, elle ne s'acquiert pas une fois pour toutes.

05

ON ENTEND SOUVENT

En dernier recours, on paiera et on récupérera nos données.

EN RÉALITÉ — *Sophos · CCB*

Payer ne garantit RIEN. Les enquêtes annuelles de Sophos (State of Ransomware) le documentent : une part importante des organisations qui paient ne récupère jamais l'intégralité de ses données, et payer vous signale comme cible solvable. Sans compter le risque juridique lié au financement d'organisations criminelles. Le CCB déconseille formellement de payer.

06

ON ENTEND SOUVENT

On a fait une présentation cyber il y a 6 mois, les équipes sont formées.

EN RÉALITÉ — *Programme, pas événement*

Une sensibilisation one-shot s'oublie en quelques semaines. Sans phishing simulé régulier, sans piqûres de rappel et sans culture de signalement, les réflexes retombent. La formation cyber, c'est un programme continu avec des indicateurs (taux de clic, taux de signalement), pas un événement.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

CAS 1 // Usinage de précision à Charleroi — tout s'arrête

Contexte: Metalux, 80 employés, spécialisée en usinage pour l'aéronautique. Kévin, magasinier, clique sur un lien dans un email imitant DHL. Le ransomware Cl0p se propage sur le réseau (aucune segmentation) et chiffre les serveurs de production, l'ERP et les sauvegardes locales.

Impact: 3 semaines d'arrêt complet. 340.000€ de pertes. 2 clients majeurs redirigent leurs commandes. Rançon de 250.000€ demandée (non payée). 6 mois pour retrouver un fonctionnement normal.

Leçon: Si le réseau avait été segmenté, le ransomware serait resté cantonné à un seul poste. Des sauvegardes hors réseau auraient permis de redémarrer en 48h. Coût de la prévention : environ 15.000€/an, soit 4% des dégâts.

CAS 2 // Cabinet d'avocats à Bruxelles — 4 mois d'espionnage

Contexte: 25 avocats, un serveur de fichiers accessible via VPN. Pas de 2FA. Un attaquant récupère le mot de passe d'un associé (réutilisé depuis LinkedIn, piraté 2 ans plus tôt) et consulte l'ensemble des dossiers clients pendant 4 mois sans que personne ne s'en aperçoive.

Impact: 12.000 dossiers sensibles exfiltrés. Notification obligatoire à l'APD et aux clients. Amende RGPD de 75.000€. 30% de la clientèle perdue en un an. La réputation du cabinet ne s'en est jamais remise.

Leçon: Le 2FA sur le VPN aurait bloqué l'accès. Un outil de détection d'anomalies aurait signalé les connexions inhabituelles en quelques jours. Budget : 8.000€/an.

CAS 3 // E-commerce à Namur — Black Friday raté

Contexte: Un site e-commerce wallon de 45 employés subit une attaque DDoS massive la veille du Black Friday. Aucune protection anti-DDoS, aucun CDN, serveurs hébergés sur un seul datacenter.

Impact: 72h d'indisponibilité au pire moment de l'année. 180.000€ de ventes perdues. Les clients partent chez Amazon. L'image de fiabilité est durablement entamée.

Leçon: Un CDN avec protection DDoS (environ 200€/mois) et une architecture multi-zone auraient absorbé l'attaque sans aucune interruption. Parfois, la protection coûte moins cher qu'un week-end de pub sur les réseaux sociaux.

Avant / Après — la différence concrète

Chapitre 5

Ce qui change quand on passe d'une posture artisanale à une posture maîtrisée.

Sans gouvernance cyber structurée	Avec une posture mature pour PME
01 VISIBILITÉ	
Aucune cartographie des actifs, des accès et des prestataires. Les angles morts sont nombreux et inconnus.	Inventaire à jour des actifs, des accès privilégiés, des données sensibles et des prestataires critiques. Surface d'attaque connue.
02 IDENTITÉS & ACCÈS	
Comptes partagés, mots de passe Excel, pas de MFA généralisé, anciens employés toujours actifs.	MFA obligatoire (Conditional Access), comptes nominatifs, gestion automatisée des départs, PAM pour les comptes admin.
03 RÉSEAU & ENDPOINTS	
Réseau plat (production, bureautique, IoT, invités au même endroit). Antivirus de base.	Segmentation par VLAN, EDR sur tous les postes, micro-segmentation des serveurs critiques. Mises à jour automatisées.
04 SAUVEGARDES	
Sauvegardes sur le même réseau que les serveurs (donc chiffrées en cas de ransomware). Pas de tests réguliers.	Règle 3-2-1 appliquée : sauvegardes immuables hors-site, testées tous les mois. Restauration < 4h validée.
05 DÉTECTION & RÉPONSE	
Aucune surveillance en dehors des heures de bureau. Une intrusion peut rester invisible pendant des mois. Improvisation en cas d'incident.	Détection managée (EDR/MDR) avec alertes qualifiées, plan de réponse aux incidents documenté et testé tous les 6 mois.

06 CONFORMITÉ NIS2 / RGPD

- Pas de gouvernance documentée. En cas de contrôle, rien à présenter. Risque de sanctions personnelles pour le dirigeant.
- Politique cyber approuvée par la direction. Registre de traitements RGPD à jour. Procédure de notification 24h NIS2 testée.

07 SENSIBILISATION ÉQUIPES

- Une présentation par an. Aucun phishing simulé. Pas de culture de signalement.
- Programme continu : phishing simulé mensuel, formation interactive trimestrielle, ambassadeurs cyber dans chaque service.

Auto-évaluation de maturité

Chapitre 6

Faites le point en 5 minutes : où en êtes-vous vraiment ?

Pour chaque question, cochez la case qui correspond le mieux à votre situation actuelle.

SITUATION	NON	PARTIEL	OUI
1. Nous avons un inventaire à jour de nos actifs IT (serveurs, postes, applications, prestataires).	☐	☐	☐
2. Le MFA / 2FA est obligatoire sur TOUS les accès externes (VPN, email, SaaS, ERP).	☐	☐	☐
3. Notre réseau est segmenté (production, bureautique, IoT, invités sur des VLAN séparés).	☐	☐	☐
4. Un EDR ou XDR moderne est déployé sur l'ensemble des postes et serveurs.	☐	☐	☐
5. Nos sauvegardes suivent la règle 3-2-1 et sont testées au moins une fois par mois.	☐	☐	☐
6. Nous disposons d'un plan de réponse aux incidents documenté et testé en exercice.	☐	☐	☐
7. Une politique de gestion des patchs garantit le déploiement sous 48h des correctifs critiques.	☐	☐	☐
8. Les comptes à privilèges sont gérés via une solution PAM (gestion / rotation / traçabilité).	☐	☐	☐
9. Nous menons un programme continu de sensibilisation (phishing simulé, formations, métriques).	☐	☐	☐
10. Nous avons cartographié notre exposition NIS2 / RGPD et documenté la gouvernance cyber.	☐	☐	☐
11. Une supervision continue (EDR/MDR managé ou SOC) détecte et qualifie les incidents, y compris hors heures de bureau.	☐	☐	☐
12. Nous auditons régulièrement la posture cyber de nos prestataires critiques.	☐	☐	☐

SCORING : Non = 0 pt • Partiel = 1 pt • Oui = 2 pts

< 40% : Critique • 40-70% : À renforcer • > 70% : Bonne posture

Ce qu'on fait concrètement pour vous

Chapitre 7

Des ressources de grand compte, enfin accessibles — Humaines, Connaissances & Outils.

On fait le point ensemble (audit 360°)

On passe votre infrastructure au peigne fin : réseau, accès, sauvegardes, postes, cloud, prestataires. On teste les failles (pentest) et on vous rend un rapport que vous pouvez comprendre et présenter à votre direction. Pas de jargon inutile, des priorités claires.

Sprint de 30 jours : on stabilise

Un mois intensif avec notre équipe : on segmente votre réseau, on durcit les accès, on externalise vos sauvegardes, on déploie le 2FA partout, on met à jour ce qui doit l'être. C'est le même type d'intervention qu'un grand groupe commanderait à un grand cabinet, adapté à votre taille et votre budget.

Un directeur technique cyber, à temps partagé

Vous n'avez pas besoin d'un CISO à temps plein. Mais vous avez besoin de quelqu'un qui pilote votre sécurité, qui parle aux prestataires, qui suit la conformité NIS2/RGPD, et qui est là quand ça tourne mal. On met à votre disposition des profils qui ont géré la sécurité de grands comptes.

Détection et réponse : le bon dispositif, bien piloté

Détection d'intrusions, analyse des logs, alertes, réponse aux incidents : ces capacités existent aujourd'hui sous forme de solutions EDR/MDR managées. On vous aide à choisir le dispositif adapté à votre taille, on l'intègre, on définit les alertes qui comptent et on pilote le prestataire. Sans vous vendre un SOC surdimensionné.

Vos employés, votre première ligne de défense

On forme vos équipes avec des cas réels belges, du phishing simulé, des exercices pratiques. Pas un PowerPoint soporifique : une vraie mise en situation. L'objectif est mesurable, campagne après campagne : moins de clics dangereux, plus de signalements.

Notre façon de travailler

Une méthode en 4 étapes, progressive, pensée pour votre réalité. Pas de slides : des livrables concrets à chaque étape.

1

VOIR CLAIR

AUDIT

On commence par comprendre votre contexte : cartographie de l'existant, entretiens avec les équipes, identification des vrais risques. Pas de diagnostic à distance, pas d'hypothèses. On part de ce qui existe chez vous.

2

PRIORISER ENSEMBLE

PLAN

Qu'est-ce qui est urgent, qu'est-ce qui peut attendre ? On construit le plan avec vous, pas à votre place. Chaque action est pondérée par son impact, son effort et votre budget. Vous gardez la main sur les décisions.

3

STABILISER

ACTION

On corrige, on durcit, on protège. Des actions concrètes et mesurables, livrées par jalons. À chaque étape, vous validez avant qu'on avance. Pas de surprise, pas de dérive budgétaire.

4

TRANSMETTRE

AUTONOMIE

On documente tout ce qu'on fait, on forme vos équipes, on vous laisse les clés. Notre succès se mesure à votre capacité à continuer sans nous. Pas de dépendance, du transfert de compétences.

Feuille de route en phases

Chapitre 8

Un chemin balisé, du diagnostic à la maturité — étape par étape.

1 — 30 JOURS — Diagnostic

- Audit NIST CSF
- Pentest externe
- Cartographie SI
- Top 10 risques

2 — MOIS 2 — Quick wins

- MFA généralisé
- EDR déployé
- Patch critiques
- Sensibilisation 1h

3 — MOIS 3-4 — Durcissement

- Segmentation VLAN
- Sauvegardes immuables
- PAM admins
- Politique cyber

4 — MOIS 5-6 — Détection

- EDR/MDR managé
- Plan incidents
- Phishing simulé
- Tests restauration

5 — MOIS 7-12 — Conformité & maturité

- CyFun / NIS2
- Audit fournisseurs
- Exercices crise
- Cyber-assurance

Conseil méthodo

Chaque phase est un livrable autonome. Vous pouvez vous arrêter à n'importe quelle étape ou ralentir le rythme selon votre budget et votre charge interne. L'important n'est pas la vitesse — c'est de ne pas reculer.

Obligations oubliées & bénéfices cachés

Chapitre 9

Des cadres réglementaires sous-estimés qui sont pourtant des leviers de valeur.

NIS2 — Votre PME est probablement concernée

Mal compris

Plus de 50 employés ou 10M€ de CA dans un secteur visé (santé, énergie, transport, numérique, alimentaire, fabrication) ? NIS2 s'applique à vous. Sous-traitant d'une entité essentielle ? Aussi. La conformité se démontre par trois voies : certification CyberFundamentals (CyFun, niveaux Basic/Important/Essential), certification ISO 27001, ou inspection du CCB.

BÉNÉFICE CACHÉ :

La mise en conformité NIS2 force à documenter vos processus IT. Résultat concret : quand un collaborateur clé quitte l'entreprise, son savoir-faire reste. Plus de "il n'y a que Jean-Marc qui sait comment ça marche". C'est aussi un argument commercial : les grands comptes exigent de plus en plus que leurs fournisseurs soient conformes. Le référentiel CyFun est gratuit et pensé pour les PME : c'est un bon point de départ même si vous n'êtes pas dans le périmètre.

RGPD — L'analyse d'impact que personne ne fait

Rarement fait

Si vous traitez des données sensibles à grande échelle, une Analyse d'Impact (AIPD) est obligatoire AVANT de commencer. L'APD belge vérifie de plus en plus. La plupart des PME n'en ont jamais fait.

BÉNÉFICE CACHÉ :

En cartographiant vos flux de données, vous découvrez des processus manuels qui pourraient être automatisés : encodages en double, exports faits à la main, fichiers qui circulent par email. L'AIPD devient alors un levier d'efficacité, pas juste une case à cocher. Moins de tâches répétitives, moins d'erreurs, et des employés qui travaillent sur ce qui a de la valeur.

Code des sociétés — Le dirigeant engage sa responsabilité

Ignoré

Le droit belge (CSA, art. 2:56) prévoit la responsabilité personnelle des administrateurs pour faute de gestion. Ne pas avoir de politique de sécurité IT documentée peut constituer une faute. Des jurisprudences existent.

BÉNÉFICE CACHÉ :

Documenter votre gouvernance IT protège le dirigeant personnellement. Mais au-delà de l'aspect juridique, ça structure votre organisation : les rôles sont clairs, les procédures existent, les nouveaux arrivants sont opérationnels plus vite. C'est un investissement qui réduit le turnover, parce que les équipes travaillent dans un cadre clair plutôt que dans le flou.

NIS2 — Vous avez 24h pour réagir

Très strict

Incident significatif ? Alerte au CCB sous 24h, rapport complet sous 72h, rapport final sous 1 mois. Sans procédure en place, c'est impossible à tenir.

BÉNÉFICE CACHÉ :

Le rapport IBM Cost of a Data Breach le mesure chaque année : les organisations qui disposent d'un plan de réponse testé réduisent nettement le coût et la durée de leurs incidents. Mais le vrai bénéfice, c'est que l'exercice de préparation identifie les personnes clés, leurs compétences et les dépendances. Vous savez exactement qui sait quoi, et vous anticipez avant qu'un départ ne crée un trou dans votre sécurité.

Bien-être numérique — Loi sur le droit à la déconnexion

Sous-estimé

Depuis 2023, les entreprises de plus de 20 salariés doivent formaliser le droit à la déconnexion. Mais la plupart des PME se limitent à une charte papier sans aucun outil pour l'appliquer.

BÉNÉFICE CACHÉ :

Mettre en place de vrais outils (gestion des notifications, plages horaires automatisées, séparation pro/perso sur les appareils) transforme la charte en pratique réelle. Des employés reposés font moins d'erreurs, y compris en cybersécurité : la fatigue et l'urgence sont les deux ingrédients préférés du phishing.

Checklist détachable — vos actions prioritaires

Imprimez cette page, cochez au fur et à mesure. Les colonnes EFFORT et IMPACT vous aident à séquencer.

		EFFORT	IMPACT	DÉLAI
☐	Cartographier l'exposition externe : tout ce qui est joignable depuis Internet (VPN, RDP, NAS, webcams).	2/5	5/5	2 semaines
☐	MFA obligatoire sur tous les accès externes (VPN, email, SaaS, ERP). Sans exception.	2/5	5/5	1 mois
☐	Déployer un EDR pro sur tous les postes et serveurs (CrowdStrike, SentinelOne, Defender for Endpoint).	3/5	5/5	1 mois
☐	Segmenter le réseau : VLAN séparés pour production, bureautique, IoT et invités.	4/5	4/5	2 mois
☐	Mettre en place des sauvegardes immuables hors-site et tester la restauration mensuellement.	3/5	5/5	1 mois
☐	Patch management automatisé : SLA 48h pour les patchs critiques.	3/5	4/5	2 mois
☐	Inventaire des prestataires critiques + revue annuelle de leur posture cyber.	2/5	3/5	2 mois
☐	Programme phishing simulé mensuel + formation interactive trimestrielle.	3/5	4/5	3 mois
☐	Plan de réponse aux incidents documenté et testé en exercice tabletop annuel.	3/5	5/5	3 mois
☐	Politique cybersécurité approuvée par la direction (preuve NIS2 art. 20).	2/5	4/5	2 mois
☐	Solution PAM pour les comptes admin (rotation, traçabilité, validation).	4/5	4/5	4 mois

		EFFORT	IMPACT	DÉLAI
☐	Détection managée (EDR/MDR) via un partenaire qualifié, avec procédure de réponse.	3/5	5/5	4 mois
☐	Gap analysis NIS2 sur base du référentiel CyFun + roadmap conformité 12 mois.	3/5	5/5	3 mois
☐	Cyber-assurance adaptée à votre maturité (et pas l'inverse).	2/5	3/5	6 mois

CONSEIL : Commencez par les actions à fort impact ET faible effort (les "quick wins").

Si vous bloquez sur une action, contactez-nous : on vous oriente gratuitement.

Questions fréquentes

Chapitre 10

Les questions que nos clients posent le plus souvent — et nos réponses sans détour.

Q1. Comment savoir si NIS2 s'applique vraiment à notre PME ?

Deux critères principaux : (1) la taille (au moins 50 employés OU 10M€ de CA), (2) un secteur listé en annexe de la loi (santé, fabrication critique, énergie, transport, banque, infrastructure numérique, alimentaire, eau, postaux). Les entités sont classées essentielles ou importantes, avec des obligations et des sanctions différentes. Si vous êtes sous-traitant d'une entité essentielle, vous êtes aussi concerné·e indirectement via ses exigences. En cas de doute, le CCB publie les critères et un point de contact sur son portail Safeonweb@Work.

Q2. On a un budget IT limité. Par où commencer ?

Trois actions à fort impact / faible coût : (1) MFA généralisé sur tous les accès externes (souvent inclus dans vos licences Microsoft 365). (2) EDR pro à la place de l'antivirus standard (de l'ordre de 80 €/poste/an). (3) Sauvegardes immuables hors-site testées (quelques milliers d'euros par an pour 50 postes). Le total annuel reste sans commune mesure avec les semaines d'arrêt qu'évite chacune de ces mesures. Le niveau CyFun Basic couvre précisément ces fondamentaux : c'est un bon fil conducteur gratuit.

Q3. Faut-il recruter un CISO en interne ?

En dessous de 250 employés, recruter un CISO à temps plein n'est pas rentable. La meilleure approche est un vCISO (CISO fractionnel) à 2-4 jours par mois : il pilote la stratégie cyber, anime le comité de pilotage, suit la conformité, gère les incidents majeurs. Comptez de l'ordre de 1 500 à 4 000 €/mois pour un profil senior, soit une fraction d'un temps plein, avec une expérience grand compte.

Q4. Qu'est-ce qu'une détection managée (EDR/MDR) apporte concrètement ?

Un service EDR/MDR managé surveille vos systèmes en continu et détecte les comportements suspects, y compris les nuits et week-ends, quand les attaques ransomware sont souvent déclenchées précisément parce que personne ne regarde. Il qualifie les alertes, isole les machines compromises et coordonne la réponse. Pour une PME de 50 personnes, comptez de l'ordre de 800 à 2 500 €/mois selon la couverture. Sans supervision, une intrusion peut rester invisible pendant des mois.

Q5. On a déjà une cyber-assurance, est-ce suffisant ?

Non. Une cyber-assurance couvre les conséquences financières d'un incident, mais : (1) les assureurs exigent un niveau de maturité minimum (MFA, EDR, sauvegardes immuables), sinon ils refusent l'indemnisation. (2) L'assurance ne réduit pas le risque, elle le mutualise. (3) Les primes ont fortement augmenté ces dernières années pour les organisations sans posture cyber documentée.

Q6. Combien de temps pour être "compliant" NIS2 ?

Pour une PME partant de zéro : 9 à 12 mois pour atteindre une maturité démontrable (les mesures de l'art. 21 + la gouvernance). Pour une PME ayant déjà des bases (audit récent, MFA déployé, sauvegardes testées) : 4 à 6 mois. La voie de démonstration la plus accessible est la certification CyberFundamentals (CyFun) au niveau correspondant à votre profil de risque ; ISO 27001 et l'inspection CCB sont les deux autres. Et rappel : l'échéance d'avril 2026 pour les entités essentielles est passée, le CCB contrôle activement.

Q7. Le télétravail rend-il notre PME plus vulnérable ?

Oui, significativement, si rien n'est fait. Le télétravail démultiplie la surface d'attaque (réseaux Wi-Fi domestiques, appareils personnels, partage de mots de passe en famille). Les bonnes pratiques : VPN avec MFA obligatoire, EDR sur les laptops fournis, MDM (Intune ou Jamf) pour gérer la flotte, charte télétravail signée. Bien équipé·e, le télétravail n'est pas plus risqué qu'un bureau.

Q8. Que se passe-t-il vraiment si on est attaqué·e ?

Heure 0 : détection. Heure 1-4 : isolation des machines compromises. Heure 4-24 : analyse forensique pour comprendre l'étendue. Sous 24h : alerte au CCB si vous êtes dans le périmètre NIS2, puis rapport intermédiaire sous 72h. Sous 72h : notification APD si des données personnelles sont concernées. Jours 1-30 : reconstruction propre depuis des sauvegardes saines. Mois 1-6 : remédiation, durcissement et, sous NIS2, rapport final au régulateur sous un mois. Sans plan préparé, tous ces délais explosent.

Glossaire

Chapitre 11

Tous les termes techniques de ce guide, expliqués en français clair.

2FA / MFA (Authentification à deux facteurs)

Méthode qui combine deux preuves d'identité pour se connecter : un mot de passe + un code reçu sur le téléphone, ou une empreinte. Selon les mesures publiées par Microsoft, bloque la grande majorité des piratages de compte. C'est gratuit, ça prend 5 minutes à activer, et ça change tout.

APD (Autorité de Protection des Données)

Le régulateur belge du RGPD. C'est l'organisme qui contrôle, conseille et sanctionne en cas de non-respect des règles sur les données personnelles. Site : autoriteprotectiondonnees.be.

APT (Advanced Persistent Threat)

Groupe d'attaquants très organisé (souvent étatique : Russie, Chine, Corée du Nord) qui s'infiltre lentement dans un réseau et y reste des mois pour espionner ou voler. Cible plutôt les grandes entreprises et les administrations.

Backup 3-2-1

Règle d'or des sauvegardes : 3 copies de vos données, sur 2 supports différents (disque + cloud par exemple), dont 1 hors site et déconnectée. Si un ransomware frappe, la copie déconnectée reste intacte.

BitLocker / FileVault

Outils intégrés gratuitement à Windows (BitLocker) et macOS (FileVault) pour chiffrer le disque dur. Si votre laptop est volé, le voleur ne peut rien lire. À activer dès aujourd'hui — c'est en 10 minutes.

CCB (Centre for Cybersecurity Belgium)

L'autorité belge de cybersécurité. Publie des alertes, accompagne les victimes d'incidents, et signale les attaques en cours. C'est aussi à eux qu'on notifie les incidents NIS2 sous 24h.

CISO / RSSI

Chief Information Security Officer / Responsable de la Sécurité des SI. La personne (interne ou externe / fractionnelle) qui pilote la stratégie cybersécurité d'une organisation.

Conditional Access

Mécanisme Microsoft (Entra ID) qui décide si un utilisateur peut se connecter selon le contexte : depuis quel appareil, quelle localisation, à quelle heure. Empêche un attaquant de se connecter même avec votre mot de passe.

DLP (Data Loss Prevention)

Technologie qui empêche la fuite de données sensibles : un employé qui essaie d'envoyer un fichier client par email perso, ou de le mettre sur une clé USB, est bloqué automatiquement.

DORA (Digital Operational Resilience Act)

Règlement européen entré en vigueur en janvier 2025. Impose au secteur financier (banques, assurances, fintechs) des règles strictes sur la résilience IT. Sanctions jusqu'à 1% du CA quotidien.

EDR / XDR

Endpoint Detection & Response : un antivirus "intelligent" qui détecte les comportements suspects sur un poste (un ransomware qui chiffre des fichiers, par exemple) et le bloque en temps réel. XDR = même chose mais étendu au réseau et au cloud.

Entra ID (anciennement Azure AD)

Le service d'identité Microsoft dans le cloud. C'est lui qui gère qui peut se connecter à quoi (Microsoft 365, applications métier, Azure). Le "trousseau de clés" central de votre IT.

Hameçonnage / Phishing

Email frauduleux qui se fait passer pour un fournisseur, un client, votre banque ou votre patron, pour vous voler vos identifiants ou vous faire cliquer sur un lien malveillant. Cause #1 des piratages.

IAM / PAM

Identity Access Management / Privileged Access Management. Outils qui gèrent qui a accès à quoi, et surtout qui contrôlent les comptes "admin" très puissants (avec validation, traces, sessions enregistrées).

ISO 27001

Norme internationale qui définit comment organiser la sécurité de l'information. Une certification ISO 27001 prouve à vos clients et partenaires que vous avez mis en place une vraie démarche structurée.

NIS2

Directive européenne transposée en droit belge en 2024. Oblige certains secteurs (santé, énergie, transport, fabrication, numérique…) à mettre en place une gouvernance cybersécurité, sous peine de 10M€ d'amende. Voir notre guide dédié.

NIST CSF

Framework de cybersécurité publié par le NIST (institut américain). Structure la sécurité en 5 fonctions : Identifier, Protéger, Détecter, Répondre, Récupérer. Référence mondiale, gratuit.

Patch / Patch management

Mise à jour de sécurité d'un logiciel ou système. Les hackers exploitent les failles connues en quelques heures après publication d'un patch. La gestion de patches consiste à appliquer ces correctifs systématiquement et rapidement.

PRA / PCA

Plan de Reprise d'Activité / Plan de Continuité d'Activité. Document qui décrit comment redémarrer l'IT après une catastrophe (incendie, ransomware, panne majeure). Sans plan testé, on improvise — et on perd plus.

Ransomware

Logiciel malveillant qui chiffre tous vos fichiers et exige une rançon en cryptomonnaie pour les déchiffrer. Le CCB traite ce type d'incident en continu en Belgique, PME et indépendants compris.

RGPD / GDPR

Règlement européen sur la protection des données personnelles (Règlement Général sur la Protection des Données). En vigueur depuis 2018. S'applique à toute organisation qui traite des données de citoyens européens. Sanctions jusqu'à 20M€ ou 4% du CA mondial.

SIEM / SOAR

Security Information & Event Management : centralise les logs de tous vos systèmes et détecte les anomalies. SOAR ajoute l'automatisation des réponses aux incidents.

SOC (Security Operations Center)

Équipe (interne ou externe) qui surveille en continu les systèmes IT pour détecter et répondre aux attaques. Un SOC externalisé permet à une PME d'avoir une protection 24/7 sans recruter.

VPN

Virtual Private Network : tunnel chiffré entre votre poste et un réseau d'entreprise. Indispensable en télétravail, MAIS doit absolument être protégé par 2FA, sinon un mot de passe volé ouvre tout votre SI.

Zero Trust

Philosophie de sécurité moderne : "ne jamais faire confiance, toujours vérifier". Chaque accès est validé en continu, même quand l'utilisateur est à l'intérieur du réseau. Remplace le modèle "château fort" obsolète.

Ressources externes

Chapitre 12

Sites officiels, outils gratuits et lectures recommandées pour aller plus loin.

CCB — Centre for Cybersecurity Belgium

ccb.belgium.be

L'autorité belge officielle de la cybersécurité. Alertes en temps réel, fiches pratiques en français, signalement d'incidents, accompagnement gratuit pour les victimes (Safeonweb).

APD — Autorité de Protection des Données

autoriteprotectiondonnees.be

Le régulateur belge RGPD. Modèles de registre, guides sectoriels, formulaire de notification des fuites de données sous 72h.

Safeonweb (CCB)

safeonweb.be

Plateforme grand public du CCB. Alertes phishing en cours en Belgique, conseils simples, formation gratuite "Citizen Cybersafe".

Have I Been Pwned

haveibeenpwned.com

Service gratuit pour vérifier si votre adresse email ou un mot de passe a fuité dans une cyberattaque connue. À consulter au moins une fois par trimestre.

ENISA — European Cybersecurity Agency

enisa.europa.eu

Agence européenne de la cybersécurité. Publications de référence sur NIS2, DORA, supply chain, gestion d'incidents — gratuites.

NIST Cybersecurity Framework

nist.gov/cyberframework

Le référentiel mondial de gouvernance cyber. Gratuit, structurant, utilisé pour cadrer les audits internes et les feuilles de route.

CIS Controls v8

cisecurity.org/controls

18 contrôles de sécurité priorisés et concrets, conçus par la communauté. Idéal pour les PME qui veulent une checklist actionnable plutôt qu'un référentiel théorique.

Bitwarden (gestionnaire de mots de passe)

bitwarden.com

Outil open-source, gratuit pour usage personnel et abordable pour les équipes. Élimine la réutilisation des mots de passe — la première cause de piratage.

KeePassXC (alternative locale)

keepassxc.org

Gestionnaire de mots de passe 100% local, gratuit, open-source. Pour ceux qui ne veulent rien stocker dans le cloud.

FlashModz Enterprise — Documents & guides

flashmodz.be/documents

Notre bibliothèque complète de guides cybersécurité, conformité, infrastructure et automatisation pour les PME et indépendants belges. Gratuit.

À propos de FlashModz Enterprise

FlashModz Enterprise est un cabinet d'expertise IT opérationnelle, fondé par Jérémy Manet et basé à Farciennes, dans la région de Charleroi. Conseil et mise en œuvre concrète : sécurité, audit et pentest, automatisation Linux/DevOps et formations — pour les particuliers comme pour les entreprises, en Belgique et à l'international. Notre conviction : les ressources, les connaissances pointues et les outils des grandes entreprises doivent être accessibles aux PME et aux indépendants. À leur échelle. À leur budget. Avec la même rigueur.

CE QUE NOUS FAISONS

- Audit sécurité
- Pentest & rapport
- Sprint de stabilisation
- Team Lead fractionnel
- Formations Linux / DevOps

CERTIFICATIONS & RÉFÉRENTIELS

- CWNA · Ruckus
- Cisco Meraki
- Fortinet NSE
- Veeam
- Jamf · Apple
- OWASP / PTES
- NIS2
- ISO 27001
- RGPD

Jérémy Manet

Fondateur · Ingénieur & architecte système/réseau

Plus de 15 ans en architecture et ingénierie système/réseau : infrastructure, Wi-Fi d'entreprise, sécurité et virtualisation. Également management (people & technique) et gouvernance IT en tant que Process Owner COBIT, DORA et NIS2. Certifié CWNA, Cisco Meraki, Fortinet, Veeam, Jamf, Apple. Technologies : Aruba, HPE, Cisco, FortiGate, Nutanix.

Spécialités : Architecture · Réseau · Wi-Fi · Sécurité · Virtualisation · Gouvernance · NIS2 · DORA

De l’expertise IT pour ce qui compte vraiment.

contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

LinkedIn Facebook TikTok Avis Google

IDENTITÉ LÉGALE

FlashModz Enterprise

DÉNOMINATION	FlashModz Enterprise
FONDATEUR	Jérémy Manet
SIÈGE SOCIAL	Rue du Wainage 18, 6240 Farciennes (Belgique)
BCE / TVA	1035.510.038 · BE 1035.510.038
EU VAT	2.386.268.987
ZONES DESSERVIES	Charleroi et alentours (B2C) · Belgique & international (B2B)
CONTACT	contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

FlashModz

Sécurisez votre PME avant qu'il ne soit trop tard

Chaque entreprise est unique. Chaque idée a ses contraintes, son contexte et ses priorités.

C'est pourquoi nous ne proposons pas de grille tarifaire figée. Nous préférons échanger avec vous, comprendre votre situation et construire une réponse adaptée à vos vrais besoins.

Parlons de votre situation

EMAIL

contact@flashmodz.be

TELEPHONE

+32 471 87 87 07

WEB

flashmodz.be

RETROUVEZ-NOUS

LinkedIn · Facebook · TikTok · Avis Google

Scannez pour accéder à ce document

BCE 1035.510.038 | Charleroi · Belgique & international