FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

Cybersécurité pour Indépendants en Belgique

Guide IPP / Indépendants

Vous êtes seul aux commandes. Votre laptop, c'est votre bureau, votre coffre-fort et votre gagne-pain. Si demain tout s'arrête (ransomware, vol, arnaque), qui prend le relais ? Ce guide est fait pour vous, sans jargon, avec des solutions concrètes.

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

Vous êtes seul aux commandes. Si demain tout s'arrête, qui prend le relais ?

1

Vous êtes une cible, précisément parce que vous êtes accessible

Les attaques ne sont pas ciblées à la main : des bots scannent en continu des millions d'adresses IP et de boîtes mail, et exploitent la première faille trouvée. Un indépendant sans 2FA ni sauvegarde est une porte ouverte, quelle que soit la taille de son activité.

2

Un incident, ce sont des semaines de travail et des clients perdus

Ransomware, boîte mail piratée, laptop volé : dans chaque scénario, vous perdez du temps facturable, des dossiers, et parfois la confiance de clients. Ajoutez l'obligation de notifier l'APD sous 72h si des données personnelles sont concernées, avec une amende possible à la clé.

3

Le RGPD vous concerne aussi, et l'APD sanctionne déjà

Un fichier Excel avec des emails clients non protégé suffit à déclencher une procédure en cas de fuite. L'APD a déjà sanctionné de très petites structures, et le plafond légal monte à 20 M€ ou 4% du chiffre d'affaires. Le registre des traitements (art. 30) est obligatoire dès le premier client.

4

L'essentiel du risque est couvert par 4 réflexes simples

2FA partout (gratuit, 10 min) · Gestionnaire de mots de passe (gratuit, 30 min) · Sauvegarde cloud automatique (quelques euros par mois) · Chiffrement du disque (gratuit, 10 min). Moins d'une demi-journée de mise en place pour fermer les portes les plus utilisées par les attaquants.

5

Vous n'êtes pas seul·e : il existe des solutions à votre taille

Un Check-up gratuit de 30 minutes suffit à identifier vos points faibles. Des kits clé-en-main couvrent l'essentiel pour quelques centaines d'euros. Et un suivi régulier coûte beaucoup moins cher qu'un seul sinistre.

Et maintenant ?

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

Document conçu pour Indépendants & Professions Libérales · Lecture : ~15-20 min · Édition 2026

Table des matières

Naviguez rapidement vers les sections qui vous concernent.

Le marché belge en chiffres

Chapitre 1

72h

délai légal pour notifier une fuite de données personnelles à l'APD (RGPD art. 33)

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

20 M€

plafond des amendes RGPD, ou 4% du chiffre d'affaires annuel mondial

10 min

suffisent pour activer le chiffrement de disque intégré à Windows ou macOS

7 ans

durée minimale de conservation de vos pièces comptables imposée par la loi belge

Contexte & enjeux

On va être honnête avec vous. En tant qu'indépendant, vous n'avez probablement pas le temps de penser à la cybersécurité. Vous avez des clients à servir, des factures à envoyer, un business à faire tourner.

Le problème, c'est que les attaquants le savent aussi. Vous n'avez pas de service IT, pas de firewall d'entreprise, pas de plan B. Et c'est exactement pour ça qu'ils vous ciblent. Pas parce que vous êtes riche : parce que vous êtes accessible. Les attaques sont automatisées, elles frappent la première porte mal fermée, quelle que soit la taille de la structure derrière.

Imaginez un comptable qui perd trois semaines de travail et ses dossiers clients à cause d'un seul clic sur un faux email. Un médecin qui se fait voler son laptop dans sa voiture, avec des milliers de dossiers patients non chiffrés dedans. Ce sont les scénarios types que le CCB (Centre pour la Cybersécurité Belgique) et sa plateforme Safeonweb décrivent toute l'année.

Et puis il y a le cadre légal. Le RGPD vous concerne, même en tant qu'indépendant. Dès que vous traitez des données de clients ou de patients, vous devez tenir un registre des traitements (art. 30), sécuriser vos supports (art. 32) et notifier toute fuite à l'APD sous 72 heures (art. 33). L'Autorité de Protection des Données a déjà sanctionné de très petites structures. Ce n'est pas pour faire peur, c'est le cadre en vigueur.

Chez FlashModz Enterprise, on vient du monde des grands comptes. Les outils, les méthodes, les réflexes qu'on utilise pour protéger des entreprises de 500 personnes, on les a adaptés pour vous. Parce qu'un indépendant mérite la même qualité de protection qu'une multinationale, simplement à son échelle

> *"On ne paie pas un consultant cyber pour qu'il vous fasse peur. On le paie pour qu'il vous fasse dormir tranquille."*
>
> — 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 : tout s'arrête en quelques minutes

Un faux email de votre fournisseur, un clic, et c'est fini. Vos fichiers sont chiffrés, votre PC est bloqué, et on vous réclame une rançon pour récupérer votre propre travail. Les indépendants sont des cibles courantes : ils paient plus souvent, parce qu'ils n'ont pas de plan B.

On se fait passer pour vous

Un pirate accède à votre boîte mail et envoie une fausse facture à vos clients avec son IBAN. Le client paie, vous devez gérer les dégâts. La fraude à la facture fait l'objet de mises en garde régulières de la police et de Febelfin : elle vise en priorité les petites structures, où une seule boîte mail fait tout.

Votre disque dur lâche. Pas de backup.

Pas besoin d'un pirate pour tout perdre. Un café renversé, un vol, un incendie. Sans sauvegarde externalisée et automatique, des années de travail disparaissent. Un disque externe branché en permanence ne compte pas : un ransomware le chiffre en même temps que le reste.

Le RGPD vous concerne aussi

L'APD a déjà sanctionné des indépendants et de très petites structures. Un simple fichier Excel avec des noms et des emails, stocké sans protection, suffit à déclencher une procédure en cas de fuite. Et les amendes RGPD peuvent monter jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires.

Mythes vs Réalité

Chapitre 3

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

01

ON ENTEND SOUVENT

Beaucoup d'indépendants pensent qu'un cybercriminel ne perdrait pas son temps avec eux. La réalité est radicalement différente.

EN RÉALITÉ — *CCB · Safeonweb*

Les attaques ne sont pas ciblées à la main. Des bots scannent en continu des millions d'IP et frappent la première faille venue, peu importe la taille de la structure. Le CCB et Safeonweb le répètent : les indépendants et TPE font partie des victimes les plus fréquentes en Belgique, justement parce que leurs défenses sont minimales.

02

ON ENTEND SOUVENT

L'antivirus gratuit Windows Defender, c'est largement assez pour un indépendant.

EN RÉALITÉ — *Défense en couches*

Un antivirus ne protège ni contre le phishing qui vous fait donner votre mot de passe, ni contre la réutilisation de mots de passe fuités sur des sites tiers, ni contre le vol physique du laptop. Un trio "antivirus + 2FA + chiffrement disque" est non négociable.

03

ON ENTEND SOUVENT

J'ai un disque dur USB que je branche de temps en temps, mes données sont à l'abri.

EN RÉALITÉ — *Règle 3-2-1*

Un disque branché en permanence est chiffré en même temps que votre PC en cas de ransomware. Un café renversé, un vol, un incendie, et tout disparaît. Une sauvegarde digne de ce nom est automatique, externalisée, et testée.

04

ON ENTEND SOUVENT

Je suis indépendant, je n'ai pas de DPO, le RGPD ne s'applique pas vraiment à moi.

EN RÉALITÉ — *RGPD art. 30*

Le RGPD s'applique à TOUTE structure qui traite des données personnelles, y compris un fichier Excel de clients. L'APD a déjà sanctionné des indépendants et de très petites structures. Le registre des traitements est obligatoire dès le premier client.

05

ON ENTEND SOUVENT

Les emails de phishing, ça se voit, je suis vigilant·e.

EN RÉALITÉ — *Verizon DBIR*

Les phishing modernes copient parfaitement vos vrais fournisseurs (DHL, bpost, votre banque). Le facteur humain est impliqué dans la majorité des violations de données analysées chaque année par le Verizon DBIR. Une formation pratique sur de vrais cas change durablement les réflexes.

06

ON ENTEND SOUVENT

La cybersécurité, c'est sur ma to-do, je m'en occuperai au prochain trimestre creux.

EN RÉALITÉ — *Prévention vs incident*

Un ransomware ou une boîte mail piratée, ce sont des semaines d'arrêt et des clients perdus, parfois une procédure APD en plus. La prévention de base coûte quelques centaines d'euros et une demi-journée. Le rapport entre les deux est sans appel.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

CAS 1 // Comptable à Namur — un clic, 3 semaines d'arrêt

Contexte: Marc est comptable indépendant depuis 12 ans. Un mardi matin, il ouvre une pièce jointe qui ressemble à une facture de son fournisseur habituel. En 12 minutes, le ransomware LockBit chiffre tous ses fichiers clients.

Impact: 3 semaines sans pouvoir travailler. 47 dossiers clients perdus. Rançon de 8.000€ demandée. Au total : 32.000€ de dégâts (chiffre d'affaires perdu, récupération, clients partis chez un concurrent).

Leçon: Un antivirus professionnel, une sauvegarde cloud automatique et 2h de formation anti-phishing auraient évité tout ça. Coût : environ 300€/an. Marc a investi depuis.

CAS 2 // Médecin à Liège — laptop volé, 2.300 patients exposés

Contexte: Sophie est médecin généraliste. Son laptop est volé dans sa voiture un vendredi soir. Pas de chiffrement, pas de mot de passe BIOS. 2.300 dossiers patients sont accessibles en quelques secondes.

Impact: Obligation légale de prévenir l'APD et chaque patient individuellement. Amende de 15.000€. En 6 mois, 40% de ses patients changent de médecin. La confiance est brisée.

Leçon: Activer BitLocker (Windows) ou FileVault (Mac) prend 10 minutes. C'est gratuit et intégré. Si le disque avait été chiffré, le voleur n'aurait rien pu lire. Aucune notification nécessaire.

CAS 3 // Architecte à Mons — 12.500€ volés à son client

Contexte: Thomas utilise le même mot de passe partout. Un site qu'il fréquentait est piraté, et ses identifiants fuitent. Un hacker se connecte à sa boîte mail pro et envoie une fausse facture à un de ses clients, avec un IBAN modifié.

Impact: Le client paie 12.500€ sur le compte du hacker. Thomas doit rembourser de sa poche. La relation professionnelle est terminée.

Leçon: L'authentification à deux facteurs (2FA) sur sa boîte mail aurait bloqué l'accès du hacker. Temps de mise en place : 10 minutes.

Avant / Après — la différence concrète

Chapitre 5

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

Sans démarche cybersécurité	Avec une posture saine
01 AUTHENTIFICATION	
Mots de passe réutilisés, parfois notés sur un post-it. Pas de 2FA. Un site piraté = tous vos comptes compromis.	2FA partout (email, banque, cloud, réseaux sociaux). Gestionnaire de mots de passe avec un mot de passe maître unique. La grande majorité des compromissions de comptes est bloquée à la source.
02 SAUVEGARDES	
Disque externe branché en permanence (ou rien du tout). Aucun test de restauration. Un ransomware = tout est perdu.	Sauvegarde cloud automatique quotidienne, chiffrée. Une copie hors-site déconnectée. Testée 1 fois par mois. Restauration en moins de 4h.
03 VOL DE MATÉRIEL	
Laptop non chiffré. En cas de vol, tous les fichiers clients sont accessibles. Notification APD obligatoire, amende possible.	BitLocker / FileVault activé. Mot de passe BIOS. En cas de vol, l'attaquant ne peut rien lire. Aucune notification, aucune fuite.
04 PHISHING & ARNAQUES	
Aucune formation. Un faux email DHL ou de votre fournisseur passe. Risque de virement frauduleux ou de ransomware.	Formation pratique de 2h sur de vrais cas belges. Réflexe automatique : vérification par téléphone avant tout virement ou clic suspect.
05 CONFORMITÉ RGPD	
Aucun registre, aucune politique. En cas de contrôle APD ou de fuite, on improvise. Amende et procédure possibles, même pour un indépendant.	Registre des traitements à jour. Modèles de consentement et de mentions légales prêts. En cas d'incident, procédure claire de notification 72h.

06 CONTINUITÉ D'ACTIVITÉ

- Si le PC tombe en panne demain, c'est l'arrêt complet. Plusieurs jours pour récupérer un accès aux fichiers et aux outils.
- Tout est dans le cloud sécurisé, accessible depuis n'importe quel appareil. Reprise d'activité en moins de 2h, même en cas de sinistre majeur.

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. J'utilise un gestionnaire de mots de passe et chaque compte a un mot de passe unique.	☐	☐	☐
2. Le 2FA est activé sur ma boîte mail principale, ma banque en ligne et mon cloud.	☐	☐	☐
3. Mon disque dur est chiffré (BitLocker, FileVault ou équivalent).	☐	☐	☐
4. Mes données sont sauvegardées automatiquement chaque jour sur un cloud sécurisé.	☐	☐	☐
5. J'ai testé une restauration de sauvegarde au moins une fois cette année.	☐	☐	☐
6. Je tiens à jour un registre RGPD basique des données clients que je traite.	☐	☐	☐
7. Mon antivirus est à jour et actif (pas seulement Windows Defender de base).	☐	☐	☐
8. Mon système d'exploitation et mes logiciels métier sont à jour (patches récents).	☐	☐	☐
9. En cas d'email suspect, j'ai un réflexe clair de vérification (appel téléphonique).	☐	☐	☐
10. Je sais qui appeler en cas d'incident cyber et j'ai une procédure claire en tête.	☐	☐	☐

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.

Check-up Sécurité (30 min, on fait le point ensemble)

On s'installe avec vous, on regarde vos mots de passe, vos sauvegardes, vos mails, votre antivirus. En 30 minutes, vous savez exactement où vous en êtes et ce qu'il faut faire en priorité. C'est le même diagnostic qu'on ferait pour une PME de 50 personnes, adapté à votre réalité.

Kit Protection Clé en Main

On vous installe tout en une demi-journée : gestionnaire de mots de passe, 2FA sur tous vos comptes, sauvegarde automatisée dans le cloud, chiffrement de vos appareils, antivirus pro. Vous n'avez rien à faire. On s'occupe de tout et on vous explique le minimum à savoir.

Quelqu'un qui veille sur vous

On met en place des outils qui vous alertent si un de vos identifiants apparaît dans une fuite de données. On gère les mises à jour de sécurité. Et si un jour il y a un problème, vous savez qui appeler. C'est le confort qu'ont les employés des grandes boîtes. Maintenant, c'est aussi le vôtre.

Formation Anti-Phishing (1h, en face à face)

Pas de slides ennuyeux. On vous montre de vrais emails frauduleux, de vraies arnaques belges, et on vous apprend à les repérer en 2 secondes. Après cette session, vous ne cliquerez plus jamais sans réfléchir.

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	2	3	4	5
J0 — 30 MIN	SEMAINE 1	MOIS 1	MOIS 2-3	CONTINU
Diagnostic	**Quick wins**	**Stabilisation**	**Conformité**	**Suivi**
• Check-up gratuit • Cartographie données • Top 5 risques	• Activer 2FA • Bitwarden installé • Chiffrement disque	• Sauvegarde cloud auto • Antivirus pro • Formation phishing 2h	• Registre RGPD • Mentions légales • Procédure incidents	• Veille mensuelle • Test sauvegardes • Audit annuel léger

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.

RGPD — Le registre des traitements (art. 30)

Souvent ignoré

Si vous gérez des données de clients, de patients ou de fournisseurs, vous devez tenir un registre de ce que vous faites avec ces données. Quasi personne ne le fait. Mais l'APD peut le demander à tout moment.

BÉNÉFICE CACHÉ :

En cartographiant vos données, vous identifiez ce qui est inutile et ce qui manque de protection. C'est aussi l'occasion de mettre en place des outils qui automatisent la gestion de vos fichiers (classement, archivage, suppression). Moins de bazar, moins de risques, et du temps gagné chaque semaine. Un modèle de registre tient sur un tableur : la barrière est plus psychologique que technique.

RGPD — La règle des 72h (art. 33)

Délai 72h

Si des données personnelles fuitent (même un laptop volé), vous avez 72 heures pour le signaler à l'APD. Un laptop non chiffré qui disparaît déclenche cette obligation.

BÉNÉFICE CACHÉ :

En chiffrant vos appareils, un vol de matériel ne constitue plus une fuite de données : pas de notification, pas de procédure. Mais surtout, vous sécurisez tout votre savoir-faire (vos modèles de contrats, vos processus, vos contacts). C'est votre capital intellectuel qui est protégé, celui qui fait que vos clients restent chez vous.

Conservation comptable — 7 ans minimum

Sous-estimé

La loi belge exige de conserver vos pièces comptables pendant au moins 7 ans. Un ransomware sans backup, c'est donc une infraction fiscale en plus de la perte.

BÉNÉFICE CACHÉ :

Une sauvegarde cloud automatisée ne vous protège pas que du piratage. Elle vous permet de retrouver n'importe quel document en 30 secondes, même un dimanche soir pour préparer un contrôle fiscal. C'est de l'automatisation pure : ça tourne tout seul, ça ne demande aucun effort, et ça vous économise des heures de stress et de recherche.

Facturation électronique — obligatoire dès 2026

Nouveau

La Belgique rend la facturation électronique structurée (e-invoicing via le réseau Peppol) obligatoire pour les transactions entre assujettis TVA à partir du 1er janvier 2026. Beaucoup d'indépendants ne sont pas encore prêts.

BÉNÉFICE CACHÉ :

Se mettre en conformité maintenant, c'est l'occasion d'automatiser toute votre chaîne de facturation : envoi, suivi, relances, archivage. Fini l'encodage manuel et les factures PDF perdues dans les boîtes mail. Et vous vous faites payer plus vite, parce que le processus est fluide côté client aussi.

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
☐	Activer le 2FA sur email, banque, cloud : la mesure qui bloque le plus d'intrusions.	●○○○○	●●●●●	Aujourd'hui
☐	Installer Bitwarden (gratuit) et arrêter de réutiliser les mots de passe.	●●○○○	●●●●●	Cette semaine
☐	Activer BitLocker (Windows) ou FileVault (Mac), le chiffrement intégré.	●○○○○	●●●●○	Aujourd'hui
☐	Configurer une sauvegarde cloud automatique quotidienne et chiffrée.	●●○○○	●●●●●	Cette semaine
☐	Vérifier sur haveibeenpwned.com si vos emails ont déjà fuité.	●○○○○	●●○○○	Aujourd'hui
☐	Mettre à jour Windows/macOS et tous les logiciels métier dans les 48h.	●○○○○	●●●●○	Cette semaine
☐	Créer un registre simple des données clients que vous traitez (RGPD art. 30).	●●●○○	●●●○○	15 jours
☐	Suivre une formation anti-phishing pratique (2h, sur cas belges).	●●○○○	●●●●○	1 mois
☐	Tester votre sauvegarde : restaurer un fichier au hasard pour vérifier.	●○○○○	●●●○○	1 mois
☐	Souscrire une cyber-assurance pro adaptée à votre activité.	●●○○○	●●●○○	2 mois
☐	Documenter qui contacter en cas d'incident (CCB, assureur, expert IT).	●○○○○	●●●○○	15 jours

- [ ] Faire auditer votre setup par un tiers une fois par an.

EFFORT	IMPACT	DÉLAI
🟢🟢🟠⚪⚪	🟢🟢🟠🔴⚪	1× par an

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. Je n'ai pas le temps. Comment commencer ?

Commencez par 30 minutes : activez le 2FA sur votre email principal et votre banque en ligne. C'est l'action qui protège le plus, pour le moins d'effort. Vous pouvez le faire ce soir, en regardant les actualités. Le reste viendra ensuite, étape par étape.

Q2. Combien ça coûte de "se mettre en règle" cyber + RGPD ?

Pour un indépendant, le minimum vital coûte entre 150 et 500 € en outils par an (gestionnaire de mots de passe, antivirus pro, cloud sécurisé, sauvegarde) + une demi-journée de mise en place. Si vous voulez un accompagnement clé-en-main, comptez 800 à 1 500 € en one-shot. À comparer aux semaines d'arrêt d'activité et aux clients perdus que coûte un seul incident.

Q3. Si je suis attaqué·e, qui appeler en premier ?

Dans cet ordre : (1) Déconnectez immédiatement votre PC du réseau (Wi-Fi off, câble débranché). (2) Signalez l'incident au CERT.be (cert.be), le service opérationnel du CCB. (3) Si des données personnelles sont concernées : notifiez l'APD sous 72h. (4) Votre assureur si vous avez une cyber-assurance. (5) Un expert IT pour la remédiation. Déposez aussi plainte à la police : c'est utile pour l'assurance.

Q4. Faut-il une cyber-assurance ?

Pour un indépendant traitant des données clients sensibles (santé, juridique, comptabilité), oui. Ça coûte de l'ordre de 200 à 500 €/an et couvre les frais de notification, l'expertise technique, la perte d'exploitation. Mais l'assurance ne dispense JAMAIS des mesures techniques de base, qu'elle exige même comme préalable.

Q5. Le cloud, c'est risqué pour mes données clients ?

Un cloud professionnel européen (OneDrive Pro, Dropbox Business, Tresorit, pCloud Suisse) avec chiffrement et 2FA est bien plus sûr que votre disque local. Les datacenters ont une protection physique et logique inaccessible à un indépendant. Le risque réel, c'est la mauvaise configuration, pas le cloud lui-même.

Q6. Et si je mélange déjà pro et perso sur mon ordi ?

C'est très courant et ça augmente le risque. La bonne pratique : créer un compte utilisateur Windows/Mac dédié au pro, ou mieux, utiliser un navigateur séparé (par exemple Firefox pour le pro, Chrome pour le perso) avec des sessions différentes. Pas besoin de racheter un PC.

Q7. On me parle de "MFA" et de "2FA", c'est pareil ?

Oui. 2FA = "Two-Factor Authentication" et MFA = "Multi-Factor Authentication". En pratique on les utilise comme synonymes. L'idée est la même : ajouter une seconde preuve d'identité (un code SMS, une app comme Google Authenticator, une empreinte digitale) en plus du mot de passe. Préférez une app d'authentification au SMS quand le service le permet.

Q8. Pourquoi vous, et pas mon neveu qui s'y connaît en informatique ?

Votre neveu peut probablement installer un antivirus. Mais peut-il auditer votre conformité RGPD ? Vous accompagner en cas de fuite de données ? Vous former contre les arnaques ciblant votre métier ? Notre métier, c'est de venir des grands comptes et d'apporter ce niveau de rigueur à votre échelle. Sans jargon, sans surfacturation.

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

Protégez votre activité dès aujourd'hui

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