LE GUIDE

B4CYBER

UNE ORGANISATION
DE **BUSINESS FOR CHARLEROI**

PRÉFACE

Diriger une entreprise aujourd'hui, c'est naviguer dans un monde où le numérique est devenu incontournable. Outils en ligne, facturation électronique (via Peppol !), cloud, e-mails, télétravail, applications métiers… tout cela vous aide à développer votre activité, à servir vos clients, à structurer votre organisation.

Mais ce même numérique expose aussi votre entreprise à de nouveaux risques.

La **cybersécurité** n'est plus un sujet réservé aux grandes entreprises ou aux experts techniques. Les PME et les indépendants sont aujourd'hui parmi les cibles préférées des cybercriminels, parce qu'ils savent que vous avez beaucoup à perdre… et souvent peu de temps à consacrer à ce sujet.

Et pourtant, la **cybersécurité** n'est pas qu'une affaire de technologie.

C'est avant tout une question de bon sens, d'organisation, de discipline et de vigilance. Ce guide a été conçu pour vous, dirigeants, entrepreneurs, responsables, femmes et hommes de terrain. Il ne cherche pas à vous transformer en expert.

Son rôle est simple :

- ➔ Vous aider à comprendre les risques réels ;
- ➔ Vous donner des réflexes concrets et applicables ;
- ➔ Vous permettre d'évaluer votre niveau de maturité ;
- ➔ Vous inspirer à passer à l'action, progressivement mais sûrement.

Chaque page contient un conseil clair, résumé en une phrase volontairement marquante, suivie d'une explication simple et de quelques questions à vous poser. Car la bonne question amène souvent la bonne décision.

La **cybersécurité** parfaite n'existe pas.
Mais une **cybersécurité** suffisante, pragmatique, adaptée à votre entreprise : oui, cela existe. Et vous pouvez la mettre en place.

Je vous invite donc à lire ce guide, à le partager avec vos équipes, et surtout… à l'utiliser comme un outil de réflexion. Certes, il n'est pas exhaustif mais chaque petit pas compte. Chaque amélioration renforce votre résilience. Chaque bonne pratique protège votre activité, vos collaborateurs,
et la confiance de vos clients.

La cybersécurité n'est pas un coût.
C'est une assurance vie pour votre entreprise.

Bonne lecture et surtout, bonne protection.

Benjamin Blampain (Ankaroo)
Consultant en cybersécurité

CONSEILS CYBER

PRÉVENIR LES INCIDENTS

Mots de passe forts et uniques, utiliser tu devras.

Des mots de passe simples sont la porte d'entrée idéale pour les cybercriminels. Utilisez des mots de passe longs (au moins 16 caractères), uniques pour chaque service, et stockez-les dans un gestionnaire sécurisé. Ajoutez l'authentification à deux facteurs dès que possible.

Questions à se poser :

- ➔ Mes employés utilisent-ils des mots de passe uniques ?
- ➔ Utilisons-nous un gestionnaire de mots de passe comme KeePass ou 1Password ?
- ➔ L'authentification à double facteur est-elle activée ?

« Former tes équipes régulièrement, tu devras. »

La plupart des attaques commencent par une erreur humaine. Sensibiliser vos équipes au phishing, aux pièces jointes suspectes et aux bonnes pratiques réduit fortement les risques.

Questions à se poser :

- ➔ Une formation cybersécurité annuelle existe-t-elle ?
- ➔ Mes équipes savent-elles reconnaître un e-mail frauduleux ?
- ➔ Faisons-nous des tests ou rappels régulièrement en interne ?

« Sauvegardes fiables et hors ligne, mettre en place tu feras. »

En cas d'attaque, une bonne sauvegarde peut sauver votre entreprise. Sauvegardez vos données automatiquement, testez la restauration, et conservez une copie déconnectée.

Questions à se poser :

- ➔ Mes sauvegardes sont-elles automatiques ?
- ➔ Une copie hors ligne existe-t-elle ?
- ➔ Ai-je déjà testé une restauration ?

Toujours à jour tes systèmes seront.

Les mises à jour corrigent des failles connues exploitées par les cybercriminels. Assurez-vous que vos logiciels, ordinateurs et serveurs sont mis à jour régulièrement.

Questions à se poser :

- ➔ Les mises à jour sont-elles automatiques ?
- ➔ Qui est responsable du suivi des mises à jour ?
- ➔ Quel pourcentage de systèmes obsolètes avons-nous ?

Limiter les accès, tu devras.

Tout le monde n'a pas besoin d'accéder à tout. Réduire les droits limite les dégâts possibles en cas de piratage ou d'erreur.

Questions à se poser :

- ➔ Qui a accès à quoi ?
- ➔ Les droits sont-ils revus régulièrement ?
- ➔ Des comptes inutiles existent-ils ?

Sécuriser tes e-mails, important cela est.

L'e-mail est la principale porte d'entrée des fraudes. Activez des filtres, sensibilisez vos équipes, et vérifiez toujours les demandes inhabituelles (factures, RIB, urgences...).

Questions à se poser :

- ➔ Avons-nous un filtre anti-spam avancé en place ?
- ➔ Une procédure de vérification existe-t-elle ?

BYCYBER

CONSEILS CYBER

ORGANISER SA CYBERSÉCURITÉ

Responsable cybersécurité, nommer tu feras.

Même dans une PME, quelqu'un doit piloter le sujet : suivi des risques, formations, procédures, prestataires. Sans pilote, la cybersécurité reste théorique. Et votre informaticien ne sait pas tout faire...

Questions à se poser :

- ➔ Avons-nous une personne référente concernant la cybersécurité ?
- ➔ Ses missions sont-elles définies ?
- ➔ Dispose-t-elle de temps et de moyens pour les thématiques liées à la cybersécurité ?

Politique simple et claire, définir tu devras.

Des règles écrites évitent les improvisations : usages IT, mots de passe, gestion des données, comportements attendus.

Questions à se poser :

- ➔ Avons-nous des règles écrites quelque part (politiques et procédures) ?
- ➔ Tous les employés les ont-ils reçues ?
- ➔ Sont-elles réalistes et appliquées ?

Cartographier tes actifs, essentiel cela est.

Savoir quels sont les actifs à protéger et où ils se trouvent est la base de la cybersécurité. Vous vous devez de savoir ce que vous devez sécuriser et leur niveau de criticité afin de mieux les protéger.

Questions à se poser :

- ➔ Quels sont les actifs importants à sécuriser pour mon activité ?
- ➔ Où se trouvent ces actifs ?
- ➔ Qui y accède ?

Vérifier tes prestataires, tu devras.

Si vos prestataires gèrent vos systèmes, leurs failles deviennent vos failles. Évaluez leur sérieux et leurs garanties.

Questions à se poser :

- ➔ Mes prestataires mettent-ils en place des contrôles de sécurité pour la gestion de mes actifs ?
- ➔ Un contrat précise-t-il leurs obligations ?
- ➔ En cas d'incident, leur rôle est-il clair ?

B4CYBER

CONSEILS CYBER

PROTÉGER SON ENTREPRISE

CONSEILS CYBER

Séparer usages pro et perso, tu devras.

Mélanger données privées et professionnelles augmente le risque de fuite et de contamination.

Questions à se poser :

- ➔ Les employés utilisent-ils leurs appareils personnels ?
- ➔ Une règle existe-t-elle ?
- ➔ Est-ce que les mesures de sécurité sont appliquées ?

Antivirus et filtrage, en place tu mettras.

Un bon antivirus et un filtrage du web réduisent les risques de contamination. Assurez-vous qu'ils sont bien configurés et surveillés.

Questions à se poser :

- ➔ Un antivirus est-il installé partout ?
- ➔ Est-il à jour ?

Sécuriser ton Wi-Fi, indispensable cela est.

Un Wi-Fi ouvert ou mal protégé expose votre réseau. Utilisez un mot de passe fort, un chiffrement moderne, et un réseau invité pour les visiteurs.

Questions à se poser :

- ➔ Qui peut se connecter à mon Wi-Fi ?
- ➔ Est-ce que mon réseau Wi-Fi est séparé des autres réseaux internes ?
- ➔ Le mot de passe est-il changé régulièrement ?

Protéger les appareils mobiles, tu devras.

Smartphones et tablettes contiennent souvent des données critiques. Activez le verrouillage, la géolocalisation et l'effacement à distance.

Questions à se poser :

- ➔ Les appareils sont-ils protégés via un système MDM (Mobile Device Management) ?
- ➔ Puis-je effacer les données à distance ?
- ➔ Une sauvegarde existe-t-elle ?

B4CYBER

CONSEILS CYBER

EN CAS D'INCIDENT

Plan de gestion d'incident, préparer tu devras.

Le jour où cela arrive, improviser coûte cher. Définissez qui fait quoi : isoler, analyser, communiquer, restaurer.

Questions à se poser :

- ➔ Un plan existe-t-il ?
- ➔ Est-ce que tout le monde sait quoi faire en cas d'incident ?
- ➔ Les contacts d'urgence sont-ils disponibles ?

En cas d'incident ou de doute, appel à des experts tu feras.

Perdre du temps peut aggraver la situation. Contactez rapidement un professionnel pour éviter les erreurs.

Questions à se poser :

- ➔ Qui appeler en cas de cyberattaque ?
- ➔ Le numéro est-il connu ?
- ➔ Avons-nous un contrat d'assistance ?

Communiquer calmement et clairement, tu devras.

La panique et les rumeurs aggravent la situation. Informez simplement les personnes clés : ce que l'on sait, ce que l'on fait, ce qui change.

Questions à se poser :

- ➔ Qui doit être informé ?
- ➔ Quel message transmettre ?
- ➔ Avons-nous un modèle de communication ?

Réinitialiser tes systèmes, surtout tu ne feras pas. Du réseau, les déconnecter tu devras.

Lorsqu'un incident survient (ransomware, piratage, comportement suspect...), la première réaction naturelle est souvent de tout réinstaller pour remettre le système en marche.

Mauvaise idée ! Cela détruit les preuves techniques qui permettent de comprendre comment l'attaque a eu lieu et si l'attaquant est toujours présent.

La bonne réaction est de déconnecter immédiatement les systèmes du réseau (Wi-Fi, câble, VPN) tout en les laissant allumés si possible. Cela limite la propagation tout en préservant les traces nécessaires aux enquêteurs et aux experts en cybersécurité (forensic).

Une fois isolés, seuls des professionnels doivent intervenir.

Questions à se poser :

- ➔ Mes équipes savent-elles qu'il ne faut pas réinitialiser ou formater en cas d'incident ?
- ➔ Savons-nous comment déconnecter rapidement une machine du réseau ?
- ➔ Avons-nous identifié un expert forensic en cas de besoin ?
- ➔ Une procédure écrite existe-t-elle pour encadrer ces actions ?

Après un incident, apprendre tu devras.

Chaque incident révèle des faiblesses. Analysez ce qui s'est passé et améliorez vos protections.

Questions à se poser :

- ➔ Pourquoi cela est-il arrivé ?
- ➔ Comment éviter que cela se reproduise ?
- ➔ Ai-je corrigé les failles ?

Cybersécurité, un chemin et non une destination cela est.

La cybersécurité n'est pas un projet ponctuel. C'est une démarche continue : améliorer, vérifier, sensibiliser.

Questions à se poser :

- ➔ Mes actions sont-elles suivies dans le temps ?
- ➔ Ai-je défini des priorités ?
- ➔ La cybersécurité fait-elle partie de ma stratégie ?

BYCYBER

UNE ORGANISATION
DE **BUSINESS FOR CHARLEROI**