Sécurité numérique : ensemble fermons la porte aux cybercriminels

1. Pourquoi ce dossier sur la cybersécurité et pour qui ?

1.1. Pourquoi les courtiers sont aujourd'hui exposés

La Belgique connaît une hausse notable des cyber incidents. Selon un article publié en février 2026 par Computable, plus de la moitié des entreprises belges ont été touchées par un incident cyber au cours des douze derniers mois. Cela inclut aussi bien de grandes organisations que des PME et des bureaux de services professionnels.

Plusieurs cas récents illustrent l'ampleur du phénomène. Fin 2025, différents piratages ont conduit à la mise en circulation de plus d'un million et demi de données de citoyens belges. En janvier 2026, l'hôpital AZ Monica à Anvers a dû fonctionner pendant près d'un mois sans son système informatique après une cyberattaque, démontrant combien un incident peut paralyser des services essentiels.

Les courtiers d'assurance travaillent au centre d'une chaîne numérique complexe comportant compagnies, plateformes sectorielles, Portima, prestataires IT et clients. Une faille dans un seul service peut perturber cette chaîne et entraîner des conséquences opérationnelles, financières ou réputationnelles importantes.

La cybersécurité n'est donc plus une préoccupation technique réservée aux spécialistes. Elle est devenue un enjeu de continuité de service et de confiance pour les courtiers et leurs clients.

1.2. Ce que vous trouverez dans ce dossier

Ce dossier a été conçu pour offrir aux courtiers une vision claire et pratique de leur exposition aux risques cyber. Il permet de comprendre les risques concrets auxquels un bureau de courtage est confronté, même lorsqu'il est de petite taille.

Le dossier explique de manière simple et structurée ce que Portima sécurise dans son rôle de fournisseur de solutions, et ce qui relève de la responsabilité

du courtier dans son propre environnement informatique : postes de travail, réseau, messagerie, gestion des utilisateurs et pratiques internes.

Il propose également un ensemble de recommandations accessibles et réalistes, qui permettent à un bureau d'évaluer ses priorités et d'avancer pas à pas dans l'amélioration de sa sécurité. Une checklist est fournie en complément pour faciliter cette démarche. Ce document n'a pas vocation à transformer un courtier en expert IT. Il vise au contraire à donner un cadre clair, compréhensible et actionnable, en s'appuyant sur des exemples concrets et des recommandations adaptées au secteur.

1.3. Comment utiliser ce dossier

Ce dossier peut vous servir de guide pour structurer votre démarche de cybersécurité. Il est conseillé de le lire une première fois pour avoir une vue d'ensemble de vos points forts et de vos faiblesses.

Discutez ensuite de vos priorités avec votre partenaire informatique : certaines actions peuvent être mises en place immédiatement, d'autres nécessitent un accompagnement.

La checklist vous permet d'évaluer concrètement votre situation et d'identifier les actions à entreprendre.

2. Ce que Portima met en place pour assurer une sécurité robuste

2.1. Portima comme « coffre-fort » du courtier

Portima assure la sécurité des données qui transitent via Portima Connect et de celles stockées dans les bases BRIO. Les échanges sont protégés, surveillés et traités sur une infrastructure conforme aux exigences du secteur. Les données restent sécurisées à chaque étape du processus, de l'envoi à la réception. Portima a obtenu la certification ISO 27001 (Système de Management de la Sécurité de l'Information).

2.2. Sécurité technique de l'infrastructure

Portima s'appuie sur une architecture technique conçue pour offrir un haut niveau de protection. L'hébergement repose sur des partenaires fiables dont Microsoft Azure, qui permet de bénéficier d'infrastructures modernes et robustes. Le réseau est protégé par des mécanismes de défense multicouches afin de réduire les tentatives d'intrusion et de garantir la continuité des services.

Les données sont chiffrées aussi bien lorsqu'elles transitent que lorsqu'elles sont stockées. Les logiciels sont développés selon une approche security-by-design, intégrant des contrôles et validations à chaque étape pour limiter les risques.

Ces éléments assurent une base technique solide, conforme aux bonnes pratiques du secteur.

2.3. Authentification et sécurité renforcée

L'accès aux applications Portima repose sur un système d'authentification sécurisé qui évolue en continu. Portima renforce régulièrement ses mécanismes de connexion afin de garantir un haut niveau de protection, en s'appuyant sur des standards reconnus et des évaluations régulières de la sécurité.

Dans ce cadre, Portima prépare l'introduction d'une authentification à double facteur, qui viendra renforcer l'identification de l'utilisateur par une validation supplémentaire. Cette évolution permettra d'augmenter encore la protection contre les accès non autorisés, notamment en cas de vol ou de compromission d'un mot de passe. Portima adapte ses mécanismes de manière progressive pour offrir une expérience sécurisée et conforme aux exigences du secteur, tout en limitant l'impact pour les utilisateurs.

2.4. Procédures administratives et identification des utilisateurs

Lors de l'affiliation, Portima vérifie toujours l'identité du responsable de bureau, soit par une visite, soit par un échange vidéo. Cette étape garantit que les accès sont fournis exclusivement aux personnes habilitées.

Les accès des utilisateurs au sein du bureau sont définis par le responsable de bureau qui dispose des outils nécessaires pour créer et gérer les droits d'accès de ses collaborateurs. Cela permet de s'assurer que seuls les collaborateurs autorisés disposent des autorisations nécessaires.

2.5. Suivi et amélioration continue

La sécurité n'est pas un état figé. Portima réalise régulièrement des audits internes et, lorsque nécessaire, des tests d'intrusion pour vérifier la solidité de ses systèmes. La certification ISO 27001 rend obligatoire un test d'intrusion une fois par an pour tous les éléments critiques. Les infrastructures sont surveillées en continu afin de détecter rapidement toute activité suspecte et d'y répondre efficacement.

Les collaborateurs internes suivent une formation régulière en cybersécurité pour maintenir un niveau de vigilance élevé et appliquer les bonnes pratiques au quotidien.

2.6. Conclusion

Portima met en place une sécurité complète et structurée, couvrant l'infrastructure, les accès, les échanges de données et les procédures internes. Cette protection constitue une base solide pour le secteur. Elle ne remplace toutefois pas le rôle du courtier, qui reste responsable de son propre environnement informatique et des pratiques appliquées dans son bureau ; si les plateformes Brio et Portima Connect sont sécurisées avec un haut niveau, c'est bien le courtier qui donne accès à ces plateformes, et qui va échanger les données qui y sont stockées avec ses clients et partenaires dans le monde de l'assurance Le courtier doit donc être vigilant par rapport aux accès qu'il donne à ses partenaires, à la nature des données échangées, et à la manière de procéder à ces échanges.

3. Comprendre les risques et faiblesses pour mieux prévenir les cyberincidents

3.1. Quels sont les risques pour un bureau de courtage ?

Un incident cyber peut prendre différentes formes et toucher tous les aspects du fonctionnement d'un bureau. Les conséquences vont bien au-delà d'un simple souci technique. Une faille peut entraîner des coûts de restauration, des pertes d'exploitation, des sanctions RGPD ou des obligations de notification. La confiance est essentielle dans la relation entre un courtier et ses clients. Un incident de sécurité réduit immédiatement cette confiance et peut avoir des effets durables.

Vol ou perte de données clients	Les données détenues par un courtier sont sensibles et très recherchées. Leur perte ou divulgation peut entraîner des conséquences importantes pour les clients comme pour le bureau.
Vol d'identité du courtier ou de ses collaborateurs	L'usurpation d'identité permet aux fraudeurs d'envoyer de faux messages, de demander des paiements ou d'obtenir des informations auprès d'assureurs ou de clients.
Compromission de la messagerie professionnelle	Une boîte mail piratée peut être utilisée pour envoyer des messages malveillants aux clients, aux compagnies ou aux partenaires, provoquant une perte de confiance immédiate.
Prise de contrôle de l'environnement informatique	Certaines attaques chiffrent les données sur le PC du courtier ou sur les serveurs de ses partenaires informatiques, bloquent les outils et demandent une rançon. Ce type d'incident peut arrêter les activités du bureau du jour au lendemain.

Interruption temporaire de travail	Un système indisponible, même quelques heures, peut empêcher le traitement des dossiers, retarder les demandes des clients et perturber les échanges avec les compagnies.

3.2. Quelles faiblesses ouvrent la porte à ces risques ?

La plupart des incidents ne résultent pas d'un piratage sophistiqué mais de faiblesses simples dans le bureau. Les points suivants sont parmi les plus fréquents.

Mots de passe réutilisés, partagés ou trop simples	L'utilisation d'un même mot de passe par plusieurs personnes ou sur plusieurs outils facilite les intrusions. Lors de l'utilisation d'un mot de passe unique pour tout le bureau, une seule compromission suffit pour accéder à l'ensemble des applications et des données. Un utilisateur qui réutilise le même mot de passe pour ses activités privées et professionnelles s'expose à un risque sur l'ensemble de ses comptes si l'un d'entre eux est compromis. Une fuite de donnée sur un site anodin peut du coup mettre en danger les comptes les plus sensibles et confidentiels.
Dispositifs non sécurisés	Des PC, portables ou smartphones sans protection adéquate constituent une porte d'entrée facile pour les attaquants.

Logiciels et systèmes non mis à jour	Des mises à jour repoussées peuvent laisser ouvertes des failles connues et exploitées activement.
Réseau Wi-Fi non sécurisé ou réseau invité mal isolé	Un Wi-Fi mal protégé ou partagé peut permettre l'accès au réseau interne du bureau.
Mauvaise gestion des arrivées et départs	Un ancien collaborateur dont le compte n'est pas désactivé représente un risque direct. Un nouveau collaborateur qui récupère les identifiants d'un autre rend toute activité non traçable.
Manque de sensibilisation du personnel	Les menaces passent souvent par Outlook, les pièces jointes, les liens cliqués ou les dossiers partagés. Sans rappel régulier, les gestes de base ne deviennent pas des réflexes, ce qui favorise les erreurs et les incidents.

3.3. Comment ces faiblesses mènent-elles aux risques ?

Chaque faiblesse augmente la probabilité qu'un incident survienne. Deux exemples illustrent ce lien.

• Exemple 1 : boîte mail compromise

Un collaborateur clique sur un lien de phishing, son mot de passe Outlook est volé et l'attaquant prend le contrôle de la messagerie.

Conséquences possibles : envoi d'e-mails frauduleux aux clients, demandes de paiement falsifiées, perte de confiance, fuite de données.

• Exemple 2 : ordinateur non mis à jour

Un PC qui n'a pas reçu une mise à jour de sécurité peut être infecté par un logiciel malveillant.
Conséquences possibles : chiffrement de dossiers, blocage du système, interruption de travail, restauration coûteuse.

Ces scénarios montrent que de petites erreurs ou négligences peuvent avoir de grands impacts. La bonne nouvelle est que la majorité de ces faiblesses peuvent être corrigées avec des mesures simples.

4. Les bonnes pratiques à adopter pour sécuriser votre activité

Ce chapitre propose un ensemble d'actions simples et réalistes pour renforcer la sécurité d'un bureau de courtage. Une checklist détaillée est également mise à disposition pour guider votre bureau dans l'évaluation de son niveau de sécurité et l'identification des actions prioritaires.

4.1. Une politique de cybersécurité adaptée à votre bureau

Chaque bureau, même de petite taille, gagne à définir quelques règles internes qui structurent son approche de la cybersécurité. Cela commence par clarifier les rôles : qui fait quoi, qui gère les accès, qui doit être averti en cas d'incident. La gestion des droits est un élément essentiel : seuls les collaborateurs qui en ont besoin doivent avoir accès à certaines données ou applications.

Une politique simple doit encadrer l'utilisation des systèmes, des mots de passe et du travail à distance. Elle doit également prévoir des procédures minimales pour accueillir les nouveaux collaborateurs et supprimer rapidement les accès lors d'un départ. Ces gestes simples évitent de nombreuses failles.

Cette politique ne doit pas être théorique, mais doit être discutée sans tabou avec les collaborateurs. En particulier, il faut instaurer un climat de confiance et de transparence : en cas d'erreur humaine – et les cyber-attaques sont majoritairement basées sur ce facteur – il est préférable que le collaborateur

ne cache pas le problème sous le tapis ; au contraire, au plus tôt le problème est détecté et discuté, au plus il est possible de limiter les dégâts.

4.2. Utilisateurs et mots de passe : la rigueur avant tout

La plupart des incidents trouvent leur origine dans de mauvaises pratiques en matière d'accès. L'utilisation d'un même mot de passe par plusieurs personnes ou pour plusieurs outils représente un risque majeur. Chaque utilisateur doit disposer de ses propres identifiants, suffisamment forts pour être difficiles à deviner et jamais réutilisés.

Pour simplifier cette gestion, l'usage d'un gestionnaire de mots de passe est recommandé. Lorsque les outils le permettent, l'activation de l'authentification multifacteur (MFA) ajoute une couche de protection bienvenue.

4.3. Hygiène numérique de base

La protection du bureau dépend largement de la manière dont sont entretenus les systèmes et les appareils. Les mises à jour automatiques doivent être activées et appliquées sans retard, car elles corrigent des failles que les cybercriminels exploitent activement.

Les appareils utilisés dans le cadre professionnel doivent être protégés par un antivirus fiable et, idéalement, par le chiffrement du disque. Une stratégie de sauvegarde régulière est indispensable : une copie en local ne suffit pas, il faut au moins une sauvegarde hors ligne ou située dans un autre lieu.

4.4. Former et sensibiliser le personnel

Même avec de bons outils, la sécurité reste fragile si les collaborateurs ne sont pas conscients des risques. Il existe de nombreuses formations accessibles aux courtiers, proposées par les fédérations, les organismes spécialisés ou d'autres acteurs du secteur.

Il est important que les messages liés à la cybersécurité viennent du management et soient incarnés par lui. Lorsque le responsable du bureau applique et rappelle les bonnes pratiques, les collaborateurs les adoptent plus facilement.

De courts moments de sensibilisation peuvent être intégrés aux réunions d'équipe pour rappeler les réflexes essentiels. Les formations existantes constituent un bon point de départ, surtout pour les petites structures. Chacun, quel que soit son rôle, contribue à la sécurité du bureau en restant attentif aux e-mails suspects, aux demandes inhabituelles et aux comportements à risque.

4.5. Se concentrer sur l'essentiel

Les outils avancés comme les simulations de phishing, les audits complexes ou les exercices de crise peuvent être utiles pour les grandes structures.

Pour les petits bureaux, il est suffisant de se concentrer sur les bases et de s'appuyer sur les formations externes structurées déjà disponibles. Une approche simple, bien appliquée, permet de renforcer efficacement la sécurité sans complexité inutile.

5. En cas d'hacking : ce que Portima fait et ce que vous devez faire

Ce chapitre vous explique comment Portima intervient lorsqu'un incident survient dans un bureau, et quelles actions vous devez mener en parallèle pour rétablir une situation de travail sécurisée.

5.1. Ce que Portima fait si votre bureau est victime d'un hacking

Dès que vous soupçonnez un incident, il est essentiel d'en avertir immédiatement Portima. Cela déclenche une procédure standard qui vise à sécuriser votre environnement le plus rapidement possible.

À partir du moment où vous signalez l'incident, Portima vous déconnecte temporairement du réseau afin d'éviter toute propagation. Les certificats locaux installés sur vos appareils ainsi que les mots de passe liés à vos accès Portima sont révoqués. De nouveaux certificats et de nouveaux accès sont ensuite générés, de manière à garantir que seule une configuration saine et contrôlée puisse à nouveau se connecter.

Si nécessaire, certains éléments de votre installation sont réinstallés ou reconfigurés pour assurer une reprise en toute sécurité. Portima veille ainsi à ce que la restauration de vos accès se fasse dans les meilleures conditions possibles.

L'objectif de ce plan est double : limiter l'impact de l'incident sur votre activité et rétablir un environnement de travail sécurisé le plus rapidement possible. L'intervention coordonnée de Portima et les bonnes pratiques mises en place dans votre bureau permettent de reprendre vos activités dans des conditions maîtrisées.

5.2. Ce que vous devez faire en parallèle

Pendant que Portima sécurise les accès liés à ses systèmes, vous devez prendre plusieurs mesures complémentaires. Suivez en priorité les recommandations que Portima vous transmet pour la partie applicative, afin d'éviter toute nouvelle tentative d'accès.

Une communication interne claire est également importante.
Vos collaborateurs doivent comprendre ce qui se passe et savoir ce qu'ils doivent éviter de faire tant que la situation n'est pas stabilisée. Dans certains cas, un message transparent à certains clients peut être utile pour préserver la confiance.

6. Ressources et formations disponibles

6.1. Instances officielles et sites d'information

Plusieurs organisations belges publient des recommandations claires et régulièrement mises à jour sur la cybersécurité. Elles constituent une première source d'information pour comprendre les risques et adopter les bons réflexes.

- Centre pour la Cybersécurité Belgique (CCB)
- Safeonweb
- SPF Économie

Ces sites proposent des conseils pratiques, des alertes en cas de menace active et des outils faciles à consulter.

6.2. Secteur financier et fédérations

Le secteur financier communique régulièrement sur les menaces les plus courantes et sur les bons comportements à adopter. Les fédérations offrent également des formations adaptées aux petits bureaux.

- Febelfin – dossier fraude et sécurité
- Feprabel Magazine Risk
- FvF

Ces organismes peuvent vous aider à mieux comprendre les risques que vous rencontrez dans votre activité quotidienne et à former vos collaborateurs à reconnaître les menaces.

7. Checklist : évaluer votre niveau de sécurité

7.1. Présentation de la checklist

La checklist est composée d'une série de points à vérifier, chacun pouvant être évalué simplement à l'aide de réponses comme Oui, Partiellement ou Non.

Elle peut être imprimée et utilisée comme outil de travail, seul ou en collaboration avec votre partenaire informatique. Elle a pour objectif de vous aider à structurer vos actions et à suivre votre progression dans le temps.

Checklist-FR (1).xlsx

7.2. Grandes rubriques de la checklist

Les points abordés dans la checklist sont regroupés en plusieurs thèmes essentiels :

Gestion des accès et des mots de passe	Vérifier comment sont attribués les accès, comment les mots de passe sont gérés et si les bonnes pratiques sont appliquées.
Mises à jour et sauvegardes	Confirmer que les appareils, logiciels et systèmes sont régulièrement mis à jour, et que les données du bureau sont correctement sauvegardées.
Procédures internes	S'assurer que les arrivées et départs de collaborateurs sont encadrés par des procédures claires, et que les droits d'accès sont ajustés en conséquence.

Sensibilisation de l'équipe	Évaluer la fréquence et la qualité des actions de sensibilisation à la cybersécurité au sein du bureau.
Réaction en cas d'incident	Vérifier si le bureau sait quoi faire en cas d'hacking et si les rôles et étapes sont clairement définis.

8. Conclusion : la cybersécurité, un effort collectif

La cybersécurité repose sur la contribution de chacun. Portima joue pleinement son rôle en sécurisant les données qui transitent par ses solutions et en en faisant de celles-ci un véritable coffre-fort numérique. Les investissements continus dans l'infrastructure, les procédures et la formation garantissent un haut niveau de protection pour l'ensemble du secteur.

Votre bureau reste toutefois responsable de son propre environnement informatique et des pratiques adoptées au quotidien. Les accès, les appareils, la messagerie, les mots de passe et la sensibilisation du personnel sont autant d'éléments qui dépendent directement de votre organisation.

En combinant les efforts de Portima, des courtiers, des fédérations et des organismes spécialisés, le secteur devient plus résilient face aux cybermenaces. Chacun joue un rôle complémentaire dans cette chaîne de sécurité.

Nous vous invitons à consulter régulièrement ce dossier sur www.portima.com et MyPortima. Il sera mis à jour pour intégrer de nouveaux conseils, ressources et bonnes pratiques qui pourront vous aider à renforcer encore votre niveau de sécurité.