CENTRE FOR
CYBER SECURITY
BELGIUM

CYBER SECURITY
COALITION.be

CYBERSÉCURITÉ
GUIDE POUR LES PME

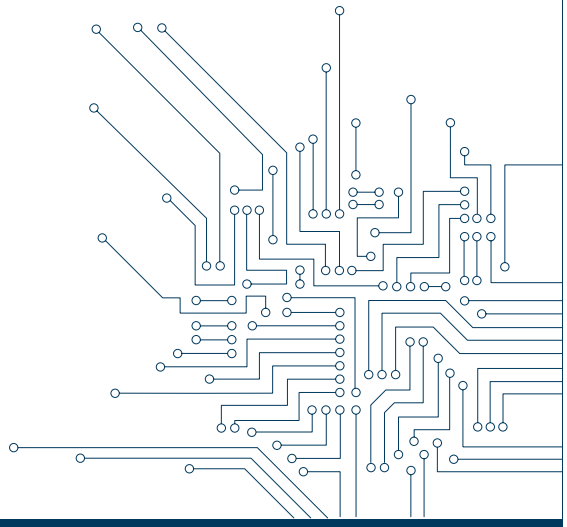
/ BELGIQUE

PRÉSENTATION

CE GUIDE DE CYBERSÉCURITÉ A ÉTÉ DÉVELOPPÉ PAR LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE (CCB), EN PARTENARIAT AVEC LA CYBER SECURITY COALITION BELGIUM, À L'INTENTION DES PETITES ET MOYENNES ENTREPRISES. IL REPOSE SUR DES CONTRIBUTIONS ET DES MEILLEURES PRATIQUES DES ENTITÉS PRIVÉES ET PUBLIQUES.

L'objectif est de fournir aux PME un aperçu des mesures de base et des mesures plus avancées sur le plan de la cybersécurité. Toutes les PME étant tenues de mettre en place une politique de cybersécurité en fonction des résultats de leur propre évaluation des risques, le présent guide fournit un bref aperçu des contrôles de sécurité qui pourraient ou devraient être exercés.

Ce guide entend permettre aux entreprises d'améliorer leur niveau de cybersécurité, de réduire les risques liés à la cybersécurité, d'atténuer les vulnérabilités et d'améliorer leur résilience. Il offre un cadre simple, permettant aux petites et moyennes entreprises d'intégrer leur activité dans un marché mondial qui fonctionne vingt-quatre heures sur vingt-quatre et ce, en toute sécurité.



LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE

CENTRE FOR CYBER SECURITY BELGIUM

LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE (CCB) EST L'AUTORITÉ CENTRALE POUR LA CYBERSÉCURITÉ EN BELGIQUE.

Le CCB a été fondé par l'arrêté royal du 10 octobre 2014. Il est chargé de dessiner les contours d'une politique nationale en matière de cybersécurité et d'encourager tous les départements pertinents du Gouvernement belge à apporter une contribution adéquate et intégrée. Le CCB opère sous l'autorité du Premier Ministre et peut compter sur le soutien administratif et logistique du Service public fédéral Chancellerie du Premier Ministre dans l'exécution de ses missions.
Veuillez consulter le site **www.ccb.belgium.be** pour un aperçu global des missions du Centre.

LA CYBER SECURITY COALITION

CYBER SECURITY COALITION.be

LA CYBER SECURITY COALITION OFFRE UN PARTENARIAT UNIQUE ENTRE DES ACTEURS ISSUS DU MONDE UNIVERSITAIRE, DES AUTORITÉS PUBLIQUES ET DU SECTEUR PRIVÉ ET LES INVITE À UNIR LEURS FORCES DANS LA LUTTE CONTRE LA CYBERCRIMINALITÉ.

Actuellement, plus de 50 acteurs clés issus de ces 3 secteurs sont des membres actifs et contribuent à la mission et aux objectifs de la coalition. La coalition répond au besoin urgent d'une collaboration intersectorielle afin de partager des connaissances et des expériences, d'initier, d'organiser et de coordonner des initiatives intersectorielles concrètes, de sensibiliser les citoyens et les organisations, de promouvoir le développement de l'expertise, ainsi que de formuler des recommandations pour des politiques et des réglementations plus efficaces.

AVANT-PROPOS

LES PETITES ET MOYENNES ENTREPRISES (PME) CONSTITUENT UN MOTEUR IMPORTANT POUR L'INNOVATION ET LA CROISSANCE EN BELGIQUE.

La cybercriminalité est une préoccupation croissante dans l'environnement des PME. Contrairement aux grandes organisations, la plupart des PME ne disposent pas de leurs propres équipes de cybersécurité. Les cybercriminels qui cherchent à tirer des avantages financiers ou à nuire aux entreprises, ont tendance à viser les cibles les plus vulnérables. Par ailleurs, vu leur dépendance aux technologies de l'information et Internet, les PME sont devenues vulnérables à la cybercriminalité. Ces faiblesses font de la sécurité de l'information une question essentielle pour toutes les PME.

Le présent guide contient des mesures de cybersécurité destinées aux petites et moyennes entreprises et a été créé par le Centre pour la Cybersécurité Belgique (CCB), en étroite collaboration avec la Cyber Security Coalition. Nous avons dressé une liste de 12 thèmes de cybersécurité, accompagnés de recommandations de base et avancées en la matière qui permettront aux PME de réduire faiblesses et vulnérabilités exploitables et de se protéger contre les violations de données et les cyberattaques.
Les principales recommandations contenues dans ce guide aideront les PME à avoir une longueur d'avance en termes de sécurité. Elles contribueront aussi à éviter les pièges les plus courants et à protéger leurs données les plus précieuses. Les bonnes pratiques et astuces permettent d'adopter des techniques de protection encore plus efficaces.

MIGUEL DE BRUYCKER
Directeur général du Centre pour la Cybersécurité Belgique (CCB)

CHRISTINE DARVILLE
Présidente de la Cyber Security Coalition

CONTENU

01 IMPLIQUEZ LE TOP MANAGEMENT

PROTECTION DE BASE

- **Désignez** un responsable de la sécurité de l'information
- **Identifiez** votre risque en matière d'ICT et protégez votre entreprise pour l'avenir
- **Respectez** les exigences légales et réglementaires concernant la vie privée, le traitement des données et la sécurité
- **Soyez** conscient des cybermenaces et des vulnérabilités sur vos réseaux

PROTECTION AVANCÉE

- **Assurez-vous** que le responsable de la sécurité de l'information soit un agent indépendant qui ne fait pas partie des services informatiques
- **Définissez** clairement les objectifs du monitoring du système et du réseau
- **Identifiez** les conséquences juridiques pour l'entreprise d'une fuite de données, d'une défaillance du réseau, ...
- **Procédez** périodiquement à un audit des risques et de la sécurité ; les résultats et le plan d'action sont communiqués au management

02 ÉLABOREZ UNE POLITIQUE DE SÉCURITÉ ET UN CODE DE CONDUITE

PROTECTION DE BASE

- **Créez** et appliquez des procédures pour l'arrivée et le départ d'utilisateurs (personnel, stagiaires, etc.)
- **Décrivez** les rôles et les responsabilités en matière de sécurité (physique, du personnel et des ICT)
- **Développez** et diffusez un code de conduite pour l'utilisation des ressources informatiques
- **Planifiez** et exécutez des audits de sécurité

PROTECTION AVANCÉE

- **Créez** un schéma de classement et de traçabilité des informations sensibles
- **Introduisez** les notions «need to know», «least privilege» et «segregation of duties» dans vos politiques et processus d'entreprise
- **Publiez** une politique de divulgation responsable
- **Stockez** les documents sensibles dans des armoires fermées à clé
- **Détruisez** les documents sensibles à l'aide d'une déchiqueteuse
- **À la fin** de la journée de travail, **détruisez** les documents laissés sur l'imprimante
- **Appliquez** le Locked Print si disponible
- **Développez** un concept et un plan de formation à la cybersécurité

03 SENSIBILISEZ VOS TRAVAILLEURS AUX RISQUES CYBER

PROTECTION DE BASE

- **Ralliez** vos utilisateurs à votre code de conduite
- **Rappelez** régulièrement aux utilisateurs l'importance d'un comportement sûr
- **Rappelez** régulièrement aux utilisateurs que les informations doivent être considérées comme sensibles et traitées dans le respect des règles de protection de la vie privée
- **Informez** les utilisateurs sur la façon de reconnaître le phishing (fraude par e-mail) et la réaction à adopter. Le test suivant est un bon outil: https://www.safeonweb.be/fr/testphishing
- **Informez** les collaborateurs du service comptabilité au sujet du phénomène de «fraude au CEO» et prévoyez des procédures de contrôle dans le cadre de l'exécution des payements

PROTECTION AVANCÉE

- **Intégrez** les notions de connaissance et de respect du code de conduite dans l'évaluation du personnel
- **Évaluez** périodiquement la sensibilisation et la réactivité des utilisateurs

04 GÉREZ VOS RESSOURCES INFORMATIQUES IMPORTANTES

PROTECTION DE BASE

- **Tenez** un inventaire de l'ensemble des équipements ICT et des licences de logiciels
- **Maintenez** une carte détaillée et actualisée de tous vos réseaux et interconnexions

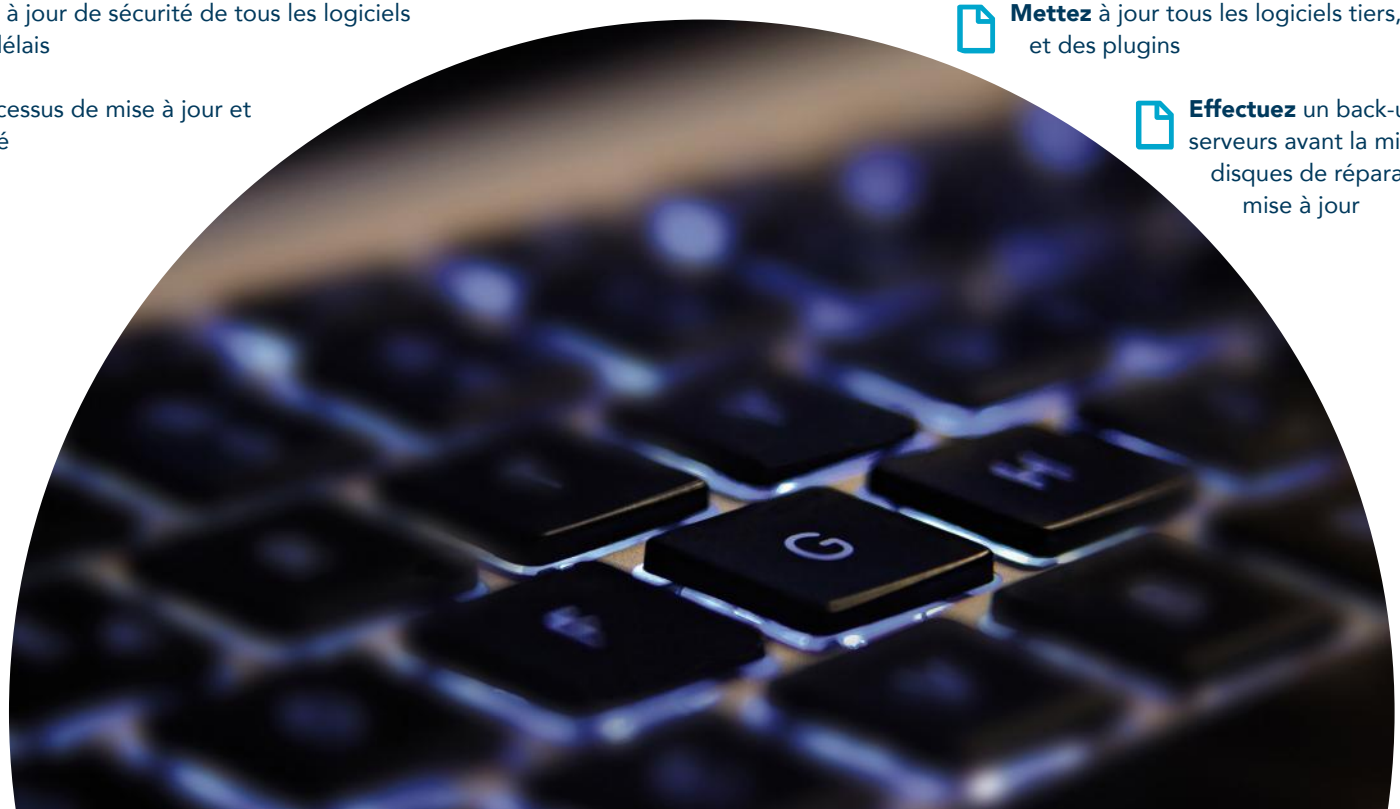
PROTECTION AVANCÉE

- **Utilisez** un instrument de gestion de configuration (ou au moins un outil tel que Microsoft MMC, ...)
- **Définissez** une configuration de sécurité de base
- **Assurez-vous** que les contrats et les accords de niveau de service (Service Level Agreements) disposent d'une clause de sécurité
- **Implémentez** un processus de contrôle du changement
- **Implémentez** un niveau uniforme de sécurité pour tous vos réseaux
- **Auditez** régulièrement toutes les configurations (y compris les serveurs, les pare-feux et les composants de réseau)

05 METTEZ À JOUR TOUS LES PROGRAMMES

PROTECTION DE BASE

- **Introduisez** une culture interne du «patch» (postes de travail, appareils mobiles, serveurs, composants de réseau, …)
- **Procédez** aux mises à jour de sécurité de tous les logiciels dans les plus brefs délais
- **Automatisez** le processus de mise à jour et auditez son efficacité



PROTECTION AVANCÉE

- **Mettez** en place un environnement d'essai et de référence pour les nouveaux patches
- **Mettez** à jour tous les logiciels tiers, comme des navigateurs et des plugins
- **Effectuez** un back-up complet pour les serveurs avant la mise à jour et créez des disques de réparation d'urgence après la mise à jour

06 INSTALLEZ UNE PROTECTION ANTIVIRUS

PROTECTION DE BASE

- **Un logiciel antivirus** est installé sur tous les postes de travail et serveurs
- **Les mises à jour** des antivirus se font automatiquement
- **Les utilisateurs savent** comment le logiciel antivirus alerte d'une infection virale

PROTECTION AVANCÉE

- **Toutes les** alertes de virus sont **analysées** par un expert ICT
- **Un logiciel** antivirus est **installé** sur tous les appareils mobiles
- **L'antivirus** est **testé** régulièrement à l'aide du test EICAR

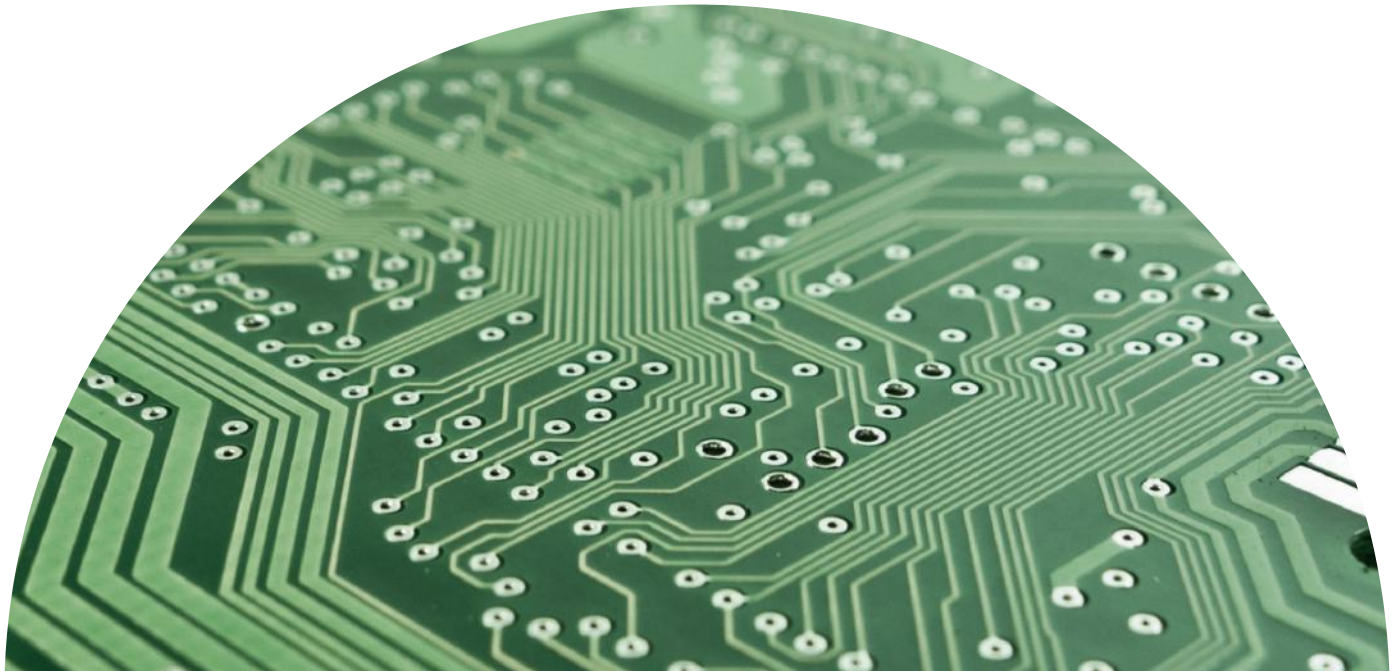
07 SAUVEGARDEZ TOUTES LES INFORMATIONS

PROTECTION DE BASE

- **Sauvegardez** vos données importantes quotidiennement
- **Hébergez** vos solutions de sauvegarde sur vos propres serveurs ou dans le cloud
- **Sauvegardez** les sauvegardes hors ligne et à un endroit séparé (si possible, éloignées de leur source)

PROTECTION AVANCÉE

- **Les sauvegardes** sont stockées dans un coffre-fort ou dans un centre de données sécurisé
- **Des tests** de restauration périodiques sont **effectués** pour évaluer la qualité des sauvegardes
- **Cryptez** les données stockées dans le cloud



08 GÉREZ L'ACCÈS À VOS ORDINATEURS ET RÉSEAUX

PROTECTION DE BASE

- **Changez** tous les mots de passe par défaut
- **Personne** ne dispose de privilèges d'administrateur pour les tâches quotidiennes
- **Maintenez** une liste limitée et actualisée des comptes d'administrateur du système
- **Les mots de passe** doivent comporter au minimum 10 caractères (une combinaison de types de caractères) et doivent être modifiés périodiquement ou dès qu'il y a un soupçon de compromission
- **Utilisez** uniquement des comptes individuels et ne partagez jamais vos mots de passe
- **Désactivez** immédiatement les comptes non utilisés
- **Rendez** l'authentification et les règles de mot de passe obligatoires
- **Les droits** et les privilèges sont gérés par groupes d'utilisateurs

PROTECTION AVANCÉE

- **Les utilisateurs ne sont autorisés** à accéder qu'aux informations dont ils ont besoin pour effectuer leurs missions
- **Détectez** et bloquez les comptes non utilisés
- **Utilisez** l'authentification multi-facteurs
- **Bloquez** l'accès à Internet à partir de comptes détenant des droits d'administrateur
- **Détectez** les accès irréguliers aux informations et aux systèmes (délais, applications, données, ...)
- **Auditez** fréquemment le répertoire central (Active Directory ou LDAP directory)
- **Limitez** l'accès des travailleurs avec un système de badges et créez plusieurs zones de sécurité
- **Enregistrez** toutes les visites
- **Organisez** le nettoyage de bureaux pendant les heures de travail ou sous surveillance permanente

09 SÉCURISEZ LES POSTES DE TRAVAIL ET LES APPAREILS MOBILES

PROTECTION DE BASE

- Les **postes** de travail et les appareils mobiles non utilisés sont **verrouillés** automatiquement
- **Les ordinateurs** portables, les smartphones et les tablettes **ne sont jamais laissés** sans surveillance
- **Désactivez** la fonction « Autorun » de médias externes
- **Stockez** ou copiez toutes les données sur un serveur ou un NAS (Network Area Storage)

PROTECTION AVANCÉE

- **Les disques durs**, les médias et les imprimantes déclassés contenant des données **sont physiquement détruits**
- **Interdisez** la connexion des appareils personnels au système d'information de l'organisation
- **Cryptez** les disques durs des ordinateurs portables
- **Les données sensibles ou confidentielles** ne sont transmises que sous forme cryptée
- **Empêchez** techniquement la connexion des supports portables non enregistrés
- **Les données** stockées dans le cloud **sont cryptées** (par exemple BoxCryptor)
- **Les garanties** offertes par le fournisseur du cloud **correspondent** au niveau de criticité des informations stockées
- **Les lecteurs de médias externes** comme les clés USB **sont contrôlés** au niveau des virus éventuels avant d'être connectés à un ordinateur

10 SÉCURISEZ LES SERVEURS ET LES COMPOSANTS DE RÉSEAU

PROTECTION DE BASE

- **Changez** tous les mots de passe par défaut et désactivez les comptes non utilisés
- **Protégez Le Wi-Fi** par un cryptage WPA2
- **Fermez** les ports et services non utilisés
- **Évitez** la connexion à distance aux serveurs
- **Utilisez** des applications et des protocoles sécurisés
- **Les journaux** de sécurité sur les serveurs et les pare-feux **sont conservés** pendant une période d'au moins 1 mois
- **Le réseau** Wi-Fi public **est séparé** du réseau d'entreprise

PROTECTION AVANCÉE

- **Les journaux** de sécurité **sont conservés** pendant une période d'au moins 6 mois
- **Protégez le Wifi** d'entreprise par WPA2 Enterprise avec un système d'enregistrement des appareils
- **Renforcez** tous les systèmes conformément aux recommandations du fournisseur
- **Utilisez** un réseau (logiquement) distinct du réseau de l'utilisateur pour l'administration des serveurs
- **Évaluez** tous les évènements et alertes des serveurs, pare-feux et composants de réseau
- **Un système d'analyse et d'alerte** se base sur les journaux afin de détecter tout comportement malveillant (SIEM)
- **Un système IDS/IPS** (Intrusion Detection/Prevention System) assure le monitoring de toutes les communications
- **L'accès** physique aux serveurs et aux composants de réseau **est limité** à un nombre minimum de personnes
- **Tout accès** physique aux serveurs et aux composants de réseau **est enregistré**
- **Exécutez** des tests d'intrusion et des scans de vulnérabilité

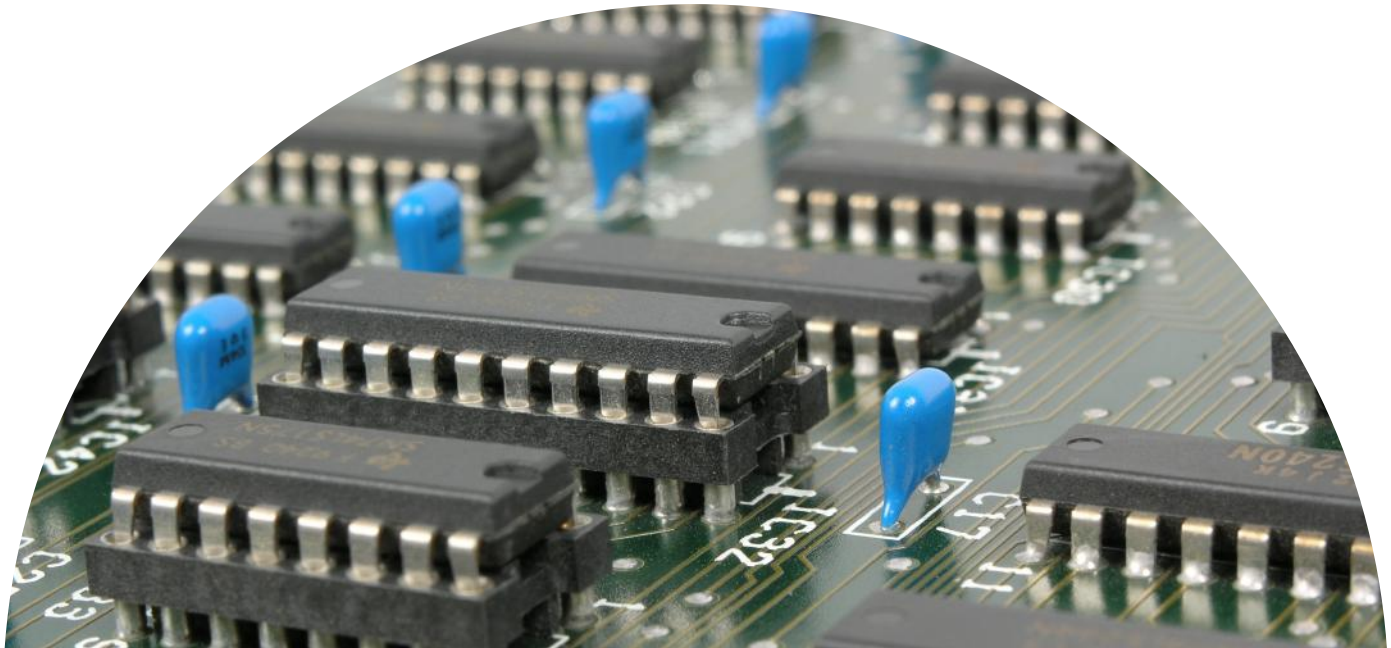
11 SÉCURISEZ LES ACCÈS À DISTANCE

PROTECTION DE BASE

- **L'accès** à distance **doit être fermé** automatiquement en cas d'inactivité pendant un certain temps
- **Limitez** l'accès à distance à ce qui est strictement nécessaire
- **Toutes les** connexions au réseau d'entreprise **sont sécurisées** et cryptées

PROTECTION AVANCÉE

- **N'autorisez** que des connexions de Virtual Private Network (VPN) à partir de points finaux
- **Une authentification** forte **est utilisée** lors d'une connexion à partir de réseaux publics extérieurs
- **L'accès** à distance **est limité** aux adresses IP des fournisseurs et des régions nécessaires



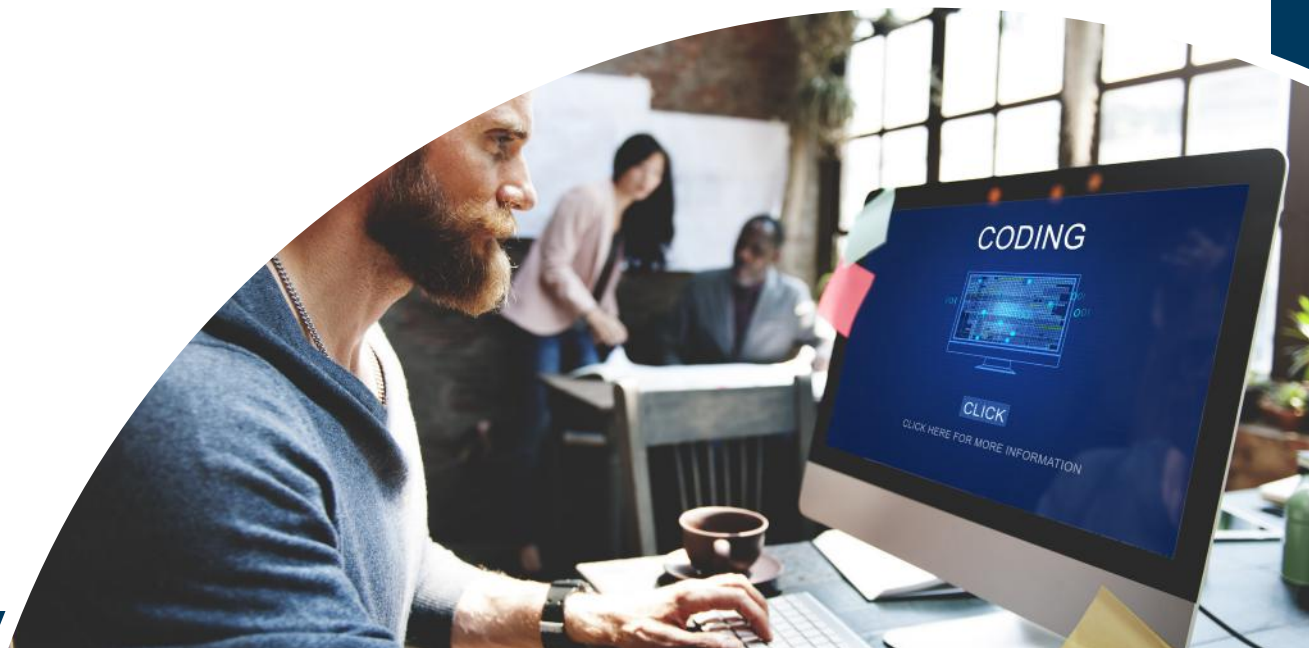
12 DISPOSEZ D'UN PLAN DE LA CONTINUITÉ DES ACTIVITES & D'UN PLAN DE GESTION DES INCIDENTS

PROTECTION DE BASE

- **Disposez** d'un plan de gestion des incidents afin de répondre à un incident
- **Disposez** d'un plan de continuité des activités afin de préserver l'entreprise
- **Tous les** travailleurs doivent connaître le point de contact pour signaler un incident
- **Diffusez** et actualisez les informations sur le point de contact (contacts internes et externes, direction et contacts techniques, ...)
- **Signalez** tous les incidents au management

PROTECTION AVANCÉE

- **Évaluez** et testez ces plans annuellement
- **Évaluez** l'opportunité d'une assurance contre les incidents de cybersécurité
- **Installez** des dispositifs d'urgence pour les services d'utilité (électricité, téléphone, Internet, ...)



DISCLAIMER

CE GUIDE ET SES ANNEXES ONT ÉTÉ ÉLABORÉS PAR LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE.
TOUS LES TEXTES, LES MISES EN PAGE, LES CONCEPTIONS ET AUTRES ÉLÉMENTS DE TOUTE NATURE DANS CE GUIDE SONT PROTÉGÉS PAR LE DROIT D'AUTEUR. LA REPRODUCTION D'EXTRAITS DU TEXTE DE CE GUIDE EST AUTORISÉE À DES FINS NON COMMERCIALES EXCLUSIVEMENT ET MOYENNANT MENTION DE LA SOURCE. LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE DÉCLINE TOUTE RESPONSABILITÉ QUANT AU CONTENU DE CE GUIDE.

Les informations fournies :

- sont exclusivement à caractère général et n'entendent pas prendre en considération la situation particulière de toute personne physique ou morale ;
- ne sont pas nécessairement exhaustives, précises ou actualisées ;
- ne constituent ni des conseils professionnels ni des conseils juridiques ;
- ne sauraient se substituer aux conseils d'un expert ;
- n'offrent aucune garantie quant à la sûreté de la protection.

SPONSORS

KBC

BNP PARIBAS FORTIS

VBO Verbond van Belgische Ondernemingen | FEB Fédération des Entreprises de Belgique

Deloitte.

Solvay Brussels School Economics & Management

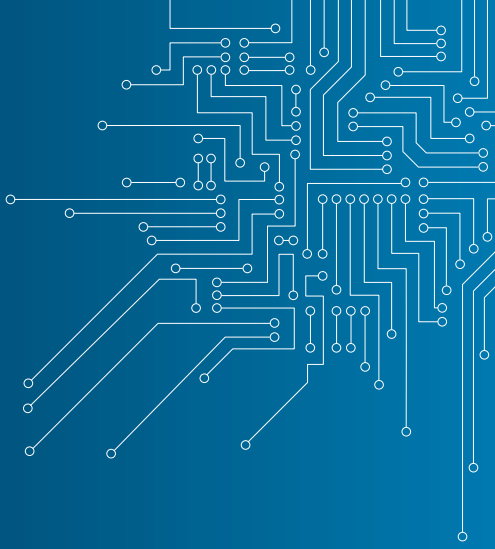
proximus

ICT CONTROL
Your Trusted Advisor

CYBER SECURITY COALITION.be

CENTRE FOR
CYBER SECURITY
BELGIUM

CYBER SECURITY
COALITION.be



LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE
Rue de la Loi, 16 - 1000 Bruxelles

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

.be