PME ANALYSE DES RISQUES **CYBERSÉCURITÉ**

QUESTIONNAIRE

STREAMSCAN

www.streamscan.ai

1-877-208-9040

POUR COMMENCER

Suivez cette analyse de risques de cybersécurité étape par étape afin de comprendre où se situent vos risques. Vous serez ainsi en mesure de donner la priorité aux bons investissements en matière de sécurité.
Si vous n'avez pas d'expert en cybersécurité dans votre équipe, assurez-vous d'en engager un pour cet exercice.

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Cadre de gouvernance de la sécurité		
Disposez-vous d'un cadre de gouvernance de la cybersécurité approuvé et communiqué ? Si oui, pouvez-vous fournir la liste des politiques de sécurité?		
Si oui, révisez-vous ce cadre de manière périodique (au moins 1 fois par an)?		
Si oui, votre politique de sécurité de l'information est-elle communiquée au sein de votre organisation?		
Organisation de la sécurité de l'information		
Les rôles et responsabilités liés à la sécurité de l'information sont-ils formellement définis, documentés et communiqués dans votre organisation?		
Disposez-vous d'un département ou service dédié à la cybersécurité? • Non • Oui, département/service dédié • Oui, mais intégré à un autre département/service		

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Politique de gestion des risques de sécurité		
Avez-vous un processus documenté d'évaluation des risques de sécurité, incluant les critères d'acceptation des risques et les critères d'évaluation des risques?		
Avez-vous un processus ou une procédure documentée de traitement des risques, incluant les options de traitement des risques (mise en place des mesures correctives, transfert du risque, acceptation du risque, etc.)?		
Contrôle d'accès au réseau		
Avez-vous une politique de gestion des identités et des accès à votre environnement TI?		
Avez-vous une politique de mot de passe documentée et communiquée? Si oui, pouvez-vous fournir les règles de cette politique?		
Avez-vous un processus qui couvre tout le cycle de vie de la gestion des accès des utilisateurs de votre réseau (création, modification, suppression, désactivation des accès, gestion des départs d'employés, etc.)?		
Appliquez-vous le principe des moindres privilèges (« Least privilege ») lors de l'octroi des accès aux utilisateurs de votre réseau? Ce principe stipule que l'on doit donner aux utilisateurs uniquement les droits minimums stricts nécessaires pour faire leur travail.		
Appliquez-vous le principe du besoin de savoir (« Need to know ») lorsque vous donnez accès à votre réseau? Ce principe stipule que seules les personnes qui ont besoin d'avoir accès aux informations dans le cadre de leur travail y ont effectivement accès.		

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Contrôle d'accès au réseau		
Les mots de passe initiaux et autres authentifications secrètes sont-ils fournis par un moyen sûr?		
Vos utilisateurs ont-ils uniquement accès aux réseaux et services pour lesquels ils sont spécifiquement autorisés?		
Les propriétaires désignés de vos actifs informationnels vérifient-ils périodiquement tous les droits d'accès privilégiés aux actifs?		
Révisez-vous de manière périodique les accès à votre réseau?		
Il y a-t-il des règles claires pour les utilisateurs sur comment protéger les mots de passe et autres informations d'authentification?		
Les droits d'accès de tous les employés et sous-traitants sont-ils supprimés immédiatement lors de la résiliation de leurs contrats?		
Sécurité des accès à distance et limitation de la surface d'attaque		
Quel type de solution d'accès à distance utilisez-vous (RDP, VPN, etc.)?		
Une authentification multifacteurs (MFA) est-elle requise pour l'accès à distance à votre réseau?		
Lors des tentatives de connexion à distance, les comptes se verrouillent-ils après un certain nombre de tentatives de connexion avec échec?		

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Sécurité des accès à distance et limitation de la surface d'attaque		
Si applicable, après combien de tentatives d'accès à distance échouées les comptes se verrouillent-ils?		
Disposez-vous actuellement d'une technologie qui vous alerte en cas de tentative d'accès non autorisés (ex: outil de gestion des logs - SIEM, système de détection d'intrusions - IDS, etc.)? Si oui, le(s)quelle(s)?		
Sécurité des courriels		
Avez-vous une politique de sécurité qui encadre l'utilisation de la messagerie électronique?		
Votre solution de courriels est-elle hébergée en interne ou à l'externe (ex: O365 dans le Cloud)?		
Une authentification multifacteurs (MFA) est-elle requise pour l'accès à vos boîtes de courriels?		
Lors d'une connexion à distance aux courriels, les comptes se verrouillent-ils après un certain nombre de tentatives de connexion échouées?		
Si applicable, après combien de tentatives d'accès à distance échouées les comptes se verrouillent-ils?		
Votre solution de courriels dispose-t-elle de fonctionnalités permettant de bloquer ou mettre en quarantaine les courriels malicieux entrants?		
Votre solution de courriels dispose-t-elle de fonctionnalités qui détectent les tentatives d'accès échouées (ex. : utilisateurs à risque, utilisateurs connectés dans les lieux improbables, etc.)?		
Protection contre l'hameçonnage		
Vos employés sont-ils sensibilisés régulièrement aux risques d'hameçonnage?		

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Protection contre l'hameçonnage		
Si oui, à quelle fréquence sensibilisez-vous vos employés?		
Vous avez sensibilisé vos employés au moins 1 fois depuis mars 2020?		
Sauvegarde des données		
Vos données sont-elles sauvegardées régulièrement?		
Si oui, à quelle fréquence faites-vous les sauvegardes?		
Avez-vous toujours une copie de sauvegarde récente en ligne et une autre copie hors-ligne?		
Conservez-vous une copie de vos sauvegardes hors de vos locaux?		
Votre solution de sauvegarde est-elle directement connectée aux serveurs où vous sauvegardez les données?		
Faites-vous régulièrement des tests de récupération de données?		
Si oui, à quelle fréquence faites-vous les tests de restauration de données?		
Gestion des vulnérabilités de sécurité		
Avez-vous une politique formelle de gestion des vulnérabilités de sécurité?		
Avez-vous une personne ou une équipe formellement désignée pour prendre en charge la collecte des informations sur les vulnérabilités (vigie sur les vulnérabilités de sécurité)?		

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Gestion des vulnérabilités de sécurité		
Par quels moyens identifiez-vous actuellement les vulnérabilités de sécurité de votre réseau? • Tests d'intrusions périodiques • Balayage de vulnérabilités régulier • Processus de gestion des patchs et correctifs de sécurité • Autres, préciser.		
Les vulnérabilités identifiées sont-elles prises en charge et promptement résolues selon leur niveau de sévérité?		
Restrictez-vous l'installation de logiciels par les utilisateurs de votre réseau informatique?		
Faites-vous auditer régulièrement la sécurité de votre réseau?		
Si applicable, à quelle fréquence le faites-vous?		
Faites-vous des tests d'intrusions réguliers dans votre réseau ou sur vos applications?		
Si oui, à quelle fréquence le faites-vous?		
Sécurité de la navigation Internet		
Utilisez-vous une solution de filtrage de la navigation Internet pour vous assurer que les employés ne naviguent pas sur des sites web non autorisés ou malicieux?		
Vos employés sont-ils régulièrement sensibilisés aux risques liés à la navigation Internet? Si oui, à quelle fréquence?		

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Sécurité du télétravail (COVID-19)		
En télétravail, vos employés sont-ils obligés de se connecter à votre réseau pour utiliser Internet (ex: via VPN)?		
Vos employés utilisent-ils leurs propres ordinateurs pour se connecter à distance à votre réseau?		
Si oui, prenez-vous des mesures pour vous assurer qu'ils ont un antivirus fonctionnel?		
Fournissez-vous un antivirus corporatif aux employés qui accèdent à votre réseau via leur ordinateur personnel?		
Avez-vous fait une sensibilisation spéciale sur les risques de sécurité liés au télétravail?		
Plan de réponse aux incidents de sécurité		
Avez-vous une politique ou un plan de réponse aux incidents et aux cyberattaques?		
Les rôles et responsabilités de la gestion des incidents de sécurité sont-ils clairement définis et communiqués?		
Avez-vous une procédure formelle de signalement des événements et des incidents de sécurité?		
Tous les évènements de sécurité de l'information sont-ils rapportés en temps opportun?		
Vos employés ont-ils l'obligation de signaler les failles de sécurité qu'ils constatent ou identifient?		
Les évènements de sécurité qui vous sont signalés sont-ils tous évalués et classifiés?		

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Plan de réponse aux incidents de sécurité		
Les incidents de sécurité sont-ils analysés de façon à acquérir de la connaissance sur le mode opératoire qui a permis leur réalisation (root cause analysis)?		
Faites-vous des tests réguliers de réponse aux incidents? Si oui, à quelle fréquence?		
Connaissance de vos risques de sécurité		
Qu'est-ce qui, selon vous, constitue les plus gros risques de sécurité pour votre organisation? • Attaques internes • Tentatives de piratage • Virus transmis via des courriers électroniques • Malware • Phishing /hameçonnage • Configuration incorrecte • Dispositifs mobiles personnels (BOYD) incontrôlés • Extorsion en ligne • Autres, préciser.		
Connaissance des incidents de sécurité		
Votre organisation a-t-elle connu un ou des incidents de sécurité au cours des 24 derniers mois?		
Si oui, lister les cas concernés ainsi que le nombre d'incidents vécus : • Vol ou accès non autorisé à des renseignements personnels • Attaques de virus • Attaques de pirates • Outils malicieux (ransomwares, etc.) • Pertes d'actifs (vol ou perte d'ordinateurs, de supports de stockage externes) • Fuite ou divulgation non autorisée d'informations sensibles • Autres, préciser.		

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Gestion de la continuité des activités		
Avez-vous un plan de continuité des activités et de recouvrement des désastres et sinistres informatiques?		
Avez-vous un environnement de recouvrement des désastres pour vos infrastructures informatiques critiques?		
À quelle fréquence faites-vous des tests de la continuité et des recouvrements de désastres?		
Gestion de la vie privée et de la conformité		
Avez-vous une politique de protection de la vie privée ou de protection des données à caractère personnel?		
Vérifiez-vous périodiquement votre niveau de conformité avec les politiques et les normes de sécurité que vous appliquez?		
La sécurité de vos systèmes d'information est-elle régulièrement révisée de façon à vérifier sa conformité avec vos politiques de sécurité de l'information?		
Défense du périmètre réseau		
Quelle(s) mesure(s) de sécurité avez-vous en place pour vous protéger contre les cyberattaques? • Antivirus sur les postes de travail et les serveurs • Technologie de protection endpoints (EDR) installées sur tous les serveurs et postes de travail • Pare-feux • Anti-spam/Spyware/Solutions anti-phishing • Systèmes de détection d'intrusions/prévention d'intrusion/brèches de sécurité (IPS/IDS /NDR) • Solution de gestion d'événements de sécurité (SIEM) • Systèmes de prévention de pertes de données (DLP) • Chiffrement de fichiers et données • Autres, préciser.		

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Défense du périmètre réseau		
Avez-vous déjà effectué des tests de pénétration (test d'intrusions) ? • Oui, par une équipe externe ou interne • Non		
Protection des données confidentielles		
Détenez-vous des informations confidentielles? Si oui, quelles sont les natures de ces données? • Renseignements personnels • Données de carte de crédit • Secrets commerciaux et propriété intellectuelle (PI) • Autres, préciser.		
Si vous avez des données confidentielles, tenez-vous un inventaire précis de ces données?		
Partagez-vous avec des tierces parties (ex : sous-traitants) des données confidentielles?		
Si applicable, faites-vous toujours signer un accord de confidentialité (NDA) avec vos partenaires, avant de leur communiquer des informations confidentielles?		
Avez-vous une procédure qui assure le respect des droits de propriété intellectuelle, en particulier, l'utilisation des logiciels sous licence?		
Avez-vous actuellement une politique de rétention des données qui indique clairement la durée de conservation des données?		
Comment protégez-vous actuellement les données confidentielles que vous détenez? • Chiffrement des données • Contrôle d'accès (limitation du nombre de personnes qui ont accès à ces données) • Authentification forte ou multifacteurs (MFA) • Autres, préciser.		

OBJECTIF DE SÉCURITÉ	STATUT Oui/Non	COMMENTAIRES
Protection des données confidentielles		
Connaissez-vous la liste de toutes les personnes au sein de votre organisation qui ont accès à vos données confidentielles (renseignements personnels, etc.)?		
Les informations personnelles que vous detenez sont-elles protégées comme exigées par les lois et les règlements?		
Disposez-vous d'un outil technologique vous permettant de détecter et empêcher les tentatives d'exfiltration de données (ou fuite d'informations)?		

PRENEZ EN MAIN VOTRE CYBERSÉCURITÉ

Comment peut-on aider?

Si votre organisation a besoin d'aide pour effectuer une analyse des risques, un audit de sécurité, développer un plan de sécurité ou mettre en œuvre une solution de surveillance externalisée de la cybersécurité (MDR), ou si vous avez simplement des questions sur la cybersécurité, contactez-nous à l'adresse suivante : info@streamscan.ai

À propos de StreamScan

La cybersécurité est tout aussi importante pour les moyennes entreprises que pour les multinationales. La réalité est que chaque année, une entreprise canadienne sur quatre, quelle que soit sa taille, voit son réseau être compromis. Avant StreamScan, il n'existait pas de solutions de sécurité conçues et tarifées spécifiquement pour les moyennes entreprises.

Le service de Détection et Réponse Gérées de StreamScan s'appuie sur la technologie CDS, un outil de surveillance de réseaux basée par l'IA pour fournir une protection optimale, à un prix qui vous conviendra. Pour en savoir plus, visitez notre site web : www.streamscan.ai.