Dossier de présentation

Association suisse pour le label de cybersécurité :
Sécurisez vos activités et faites le savoir !

Association suisse pour le Label de Cybersécurité
Chemin des Piécettes 2
1052 Le Mont-sur-Lausanne
info@cyber-safe.ch

www.cyber-safe.ch

L'ASSOCIATION SUISSE POUR LE LABEL DE CYBERSÉCURITÉ A ÉTÉ CRÉÉE EN 2018 AVEC POUR OBJECTIF DE FAVORISER UNE GESTION RESPONSABLE DE LA CYBERSÉCURITÉ DANS LES PETITES ET MOYENNES ORGANISATIONS EN SUISSE.

Pour ce faire, elle développe un Label qui permettra à ces organisations d'atteindre un niveau de sécurité informatique défini comme acceptable par un ensemble de partenaires publics et privés. En reposant sur une méthode d'évaluation originale alliant outil en ligne, questionnaires, tests d'hameçonnage et interventions humaines, le label offrira un outil d'aide à la décision et de connaissance fine des cyberrisques en matière d'infrastructure, d'organisation et de compétences humaines. Il permettra ainsi aux organisations candidates d'implémenter les mesures préventives à plus forte valeur ajoutée pour sécuriser leurs activités – et le faire savoir !

Ces dernières années, la prolifération de cyberattaques et d'incidents inédits, leur forte médiatisation à l'échelle mondiale et l'évolution des législations suisse et européenne, ont suscité une prise de conscience nouvelle des cyberrisques dans la plupart des organisations. Si les plus grandes d'entre elles disposent en général des moyens et compétences nécessaires pour un traitement judicieux des cyberrisques, les petites et moyennes organisations sont souvent plus démunies face à ces nouveaux risques. Ce constat est à l'origine de la création de l'Association suisse pour le Label de cybersécurité.

LE SAVIEZ-VOUS ?

- 1 PME sur 3 a déjà été victime de cyberattaques[1].
- 15% des sociétés forment leurs collaborateurs aux bonnes pratiques de cybersécurité, or 100% des organisations font l'objet de tentatives d'hameçonage (phishing)[1].
- Pour plus d'1/4 des victimes de cyberattaques, les coûts de réparation ont été importants ; dans un quart des cas, la facture est supérieure à 10 000 CHF[2].

[1] Mändli Lerch, K. (2017). Cyberrisiken in Schweizer KMUs. Zürich : gfs-zürich.
Consulté à l'adresse https://gfs-zh.ch/wp-content/uploads/2017/12/Schlussbericht_CyberriskKMU_12122017.pdf

[2] Krähenbühl, J.-F. (2018). Les entreprises vaudoises face aux enjeux de la cybersécurité. Lausanne : Chambre vaudoise du commerce et de l'industrie.
Consulté à l'adresse : https://www.cvci.ch/fileadmin/documents/cvci.ch/pdf/Medias/publications/divers/12315_ENQUETE_CYBERSECURITE_PROD_PP.pdf

UN LABEL, POURQUOI ?

De nombreuses barrières existent à l'entrée des PMEs et autres petites structures dans le monde de la sécurité informatique. Le Label Cyber Safe vise à abaisser ces barrières en offrant une incitation forte et en mettant à disposition des organisations les instruments nécessaires à une gestion responsable de la cybersécurité. Et ce à un prix abordable !

En effet, malgré une médiatisation croissante des risques liés au numérique (vol de données, perte d'exploitation, etc.) et une prise de conscience grandissante, le passage à l'action reste souvent difficile pour les petites et moyennes organisations. Outre l'importance des coûts de conseil et d'audit en sécurité informatique, ces organisations sont confrontées à des questions auxquelles elles ne parviennent que difficilement à répondre sans l'aide de spécialistes. Quel est le niveau actuel de cybersécurité de mon organisation ? Est-ce satisfaisant ? Quelles sont les mesures à prendre pour l'améliorer, à quel prix et avec quels effets ? En l'absence de compétences spécialisées, dresser un état des lieux ou savoir quelles mesures mettre en œuvre est difficile, voire impossible.

S'il existe de nombreux référentiels de gestion des risques informatiques (type ISO), ces derniers ne sont souvent pas adaptés aux besoins des petites structures en raison de leur complexité, du jargon utilisé et de l'approche sectorielle des cyberrisques qu'ils proposent (ainsi un référentiel portera exclusivement sur la dimension organisationnelle, un autre sur la sécurité des logiciels et/ou du matériel, un autre se focalisera sur les compétences humaines). Or, la mise en conformité à de multiples référentiels (potentiellement contradictoires) n'est pas chose aisée pour les organisations, sans parler des multiples coûts associés.

UN LABEL À FORTE VALEUR AJOUTÉE

- Connaissance fine du niveau de cybersécurité.
- Aide à la décision accessible et quantifiée.
- Plan de réduction de la vulnérabilité aux cyberattaques.
- Optimisation des coûts de cybersécurité.
- Réduction des primes d'assurances.
- Respect des bonnes pratiques
  (élément d'appréciation de la responsabilité).
- Confiance accrue des partenaires et clients, gains réputationnels.

CYBER SAFE RÉPOND À CES DÉFIS.

Le Label Cyber Safe offre tout d'abord un outil d'aide à la décision essentiel permettant aux petites et moyennes organisations de dresser un état des lieux, de connaître les coûts probables engendrés par une cyberattaque, et, partant, la valeur ajoutée de différentes actions de remédiations possibles.

Il permet ainsi aux organisations de réduire leur vulnérabilité aux futures cyber-attaques. Il répond ensuite aux besoins de ces organisations en déployant une approche holistique et non sectorielle des cyberrisques. Il permet enfin aux organisations labellisées d'engranger de la confiance et de tirer ainsi pleinement profit de leur gestion responsable de la cybersécurité.

L'ASSOCIATION : UNE DÉFINITION PARTICIPATIVE DU NIVEAU ACCEPTABLE DE CYBERSECURITÉ

Le risque zéro n'existe pas en matière de sécurité informatique comme ailleurs. La notion de risque acceptable s'impose donc pour définir le niveau d'exigences auquel une organisation doit satisfaire pour être labellisée.

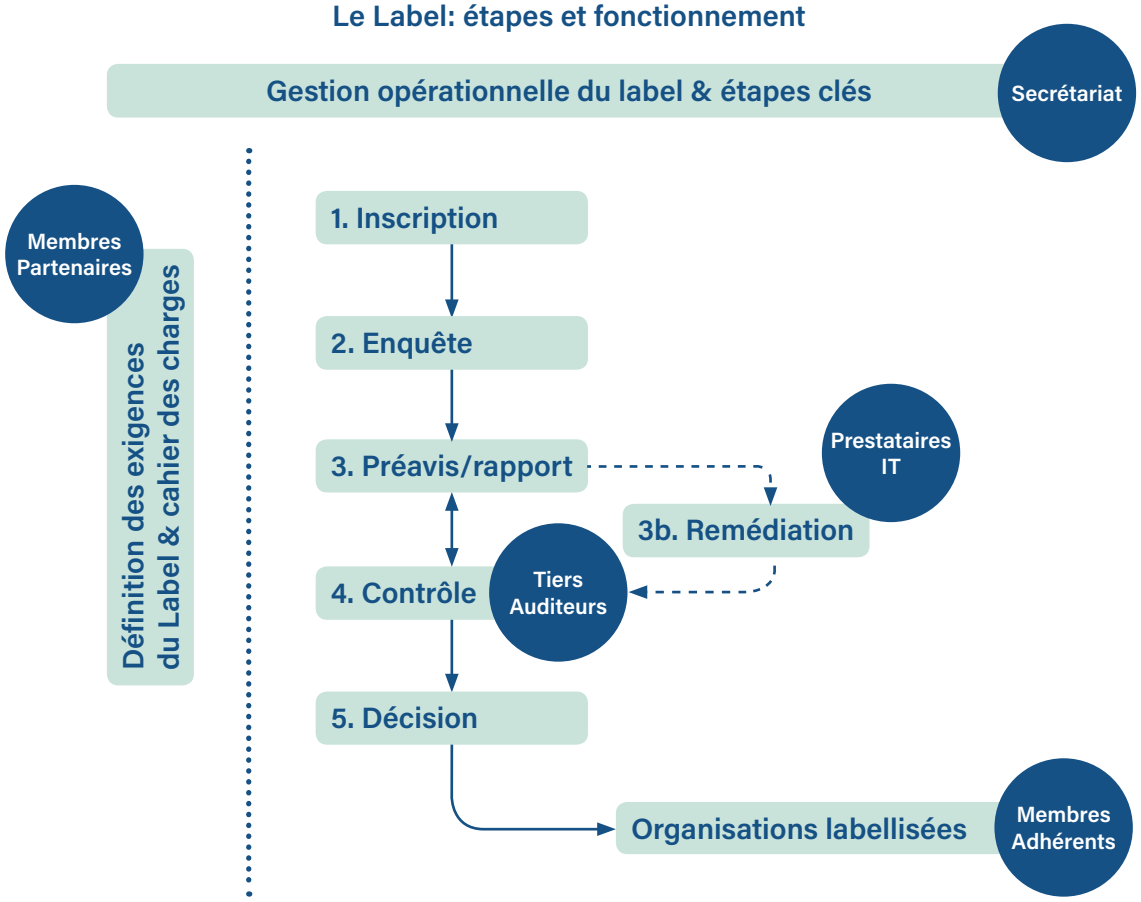
Afin de définir un niveau acceptable de cybersécurité, l'Association mobilise les connaissances et expériences de l'ensemble des parties prenantes concernées. Des spécialistes de la sécurité informatique, des représentants des milieux économiques et politiques ainsi que du monde académique et associatif se réunissent sous l'égide de l'Association. Ils définissent sur une base délibérative et consensuelle le niveau acceptable de cybersécurité donnant droit au Label. Cette activité dite de « normalisation » intervient néanmoins dans un périmètre donné ; la limite inférieure du niveau d'exigence est fournie par le seuil de faillite d'une organisation (par ex. faillite en raison des conséquences financières et opérationnelles d'un piratage de données). La limite supérieure est quant à elle atteinte lorsque le coût de l'investissement est plus important que le coût qu'entraînerait la réalisation du cyberrisque.

LE LABEL, UNE APPROCHE GLOBALE DE LA CYBERSECURITÉ

Afin de déterminer le niveau de cybersécurité d'une organisation, le Label repose sur une technologie innovante développée par une entreprise suisse. Cette technologie permet d'appréhender les cyberrisques de façon globale.

Elle évalue aussi bien l'infrastructure informatique, que la sécurité des données (y compris plan de sauvegarde et de récupération) et des sites web (les failles connues des systèmes de gestion de contenu WordPress et Joomla) ou encore les pratiques humaines et organisationnelles affectant la cybersécurité (par exemple test d'hameçonnage). Elle permet ainsi d'évaluer les dimensions techniques, humaines et organisationnelles nécessaires à la définition d'une stratégie cohérente et proactive des cyberrisques.

Le Label: étapes et fonctionnement



1. Inscription : L'organisation dépose sa demande auprès du secrétariat qui l'accepte ou non sur la base de critères formels (nombre d'employés, siège en Suisse, activités hors FINMA). La phase d'inscription prend fin suite à l'acceptation de la demande et du règlement des frais d'inscription.

2. Enquête : Démarre alors la phase d'enquête au cours de laquelle une première appréciation du niveau de cybersécurité de l'organisation candidate est réalisée à l'aide d'outils spécialisés (scans externes et internes de l'infrastructure IT et site web), de questionnaires (politique de sauvegarde des données et plan de récupération, attribution des responsabilités au sein de l'organisation, etc.) et de tentatives d'hameçonnage (évaluation des compétences humaines).

3. Préavis/rapport : L'organisation candidate reçoit alors un rapport détaillé de son niveau de cybersécurité, de ses failles et de leurs coûts potentiels ; un préavis de labélisation est simultanément transmis. Disponible sous format pdf ainsi que dans un tableau de bord interactif, ce rapport présente en outre les mesures de remédiations possibles et leurs effets sur le niveau général de cybersécurité (ratio coût/effet). Le tableau de bord permet à l'organisation de simuler les différentes mesures et leurs effets sur les différents volets (infrastructure, organisation, compétences humaines) pris en compte dans l'évaluation du niveau de cybersécurité

3b. Remédiation: En fonction du niveau de cybersécurité de l'organisation candidate, cette dernière met en oeuvre le cas échéant la ou les mesure(s) de remédiation nécessaire(s) pour atteindre le niveau d'exigence défini pour l'obtention du Label. Selon les cas, les mesures de remédiation peuvent être mises en œuvre soit directement par l'organisation, soit par son prestataire IT. Pour chacune des mesures possibles, des prestataires potentiels sont communiqués à l'organisation candidate.

4. Contrôle : Lorsque l'organisation candidate estime satisfaire aux exigences du Label, elle en informe le secrétariat de l'Association qui mandate alors un tiers auditeur indépendant (i.e. non impliqué dans les mesures de remédiations) pour vérifier avec l'organisation candidate l'exactitude des données collectées et, le cas échéant, leur actualisation suite à la mise en œuvre de(s) mesure(s) de remédiation. Le tiers auditeur dresse ensuite un rapport d'évaluation qu'il transmet au secrétariat de l'Association.

5. Décision : Sur la base du rapport d'évaluation transmis par le tiers auditeur, le secrétariat de l'Association prend décision formelle d'attribution ou d'ajournement. Une décision d'ajournement peut être prise au maximum une fois afin de permettre à l'organisation ne répondant pas aux exigences du Label de répéter les étapes 2 à 5 sans frais additionnels. Si l'organisation ne répond toujours pas aux exigences au terme de l'ajournement, l'Association refuse l'attribution du Label.

ASSOCIATION SUISSE POUR
LE LABEL DE CYBERSÉCURITÉ

Association suisse pour
le Label de Cybersécurité
Chemin des Piécettes 2
1052 Le Mont-sur-Lausanne
info@cyber-safe.ch

www.cyber-safe.ch