

Lausanne, le 5 novembre 2019



Communiqué de presse

Cybersécurité et PME: parlons francs!

Le 6 novembre à Lausanne, PME, communes, associations professionnelles et hautes écoles participaient à la définition du Label cyber-safe.ch. Objectif? Disposer d'un outil pour évaluer le coût potentiel des cyberattaques et identifier les mesures de protection les plus efficaces.

Pourquoi un Label ?

Le projet, né sous l'égide de l'Association Suisse pour le Label de Cybersécurité (ASLaC), part d'un constat simple : même si plus d'un tiers des petites et moyennes organisations ont déjà fait l'objet de cyberattaques, la plupart restent démunies face à ces nouveaux risques, principalement par manque de ressources et de compétences. L'objectif du Label ? Permettre à ces organisations d'identifier les données de valeur à protéger, de connaître leur niveau de protection et de mettre en place des mesures ciblées pour atteindre un niveau acceptable de cybersécurité. Et c'est en réunissant des experts d'horizons divers, représentant au total plus de 8'500 PME et quelques centaines de communes, que le Label définit des exigences en phase avec les réalités du terrain. Ces experts étaient réunis hier à Lausanne pour l'une des dernières séances de définition des exigences du Label.

Votre cyberrisque en CHF

L'ASLaC a été fondée en septembre 2018 pour accompagner les PME qui sont aujourd'hui la cible de hackers malveillants. Pour la plupart des organisations, déterminer les actions efficaces parmi les multiples recommandations et bonnes pratiques tient de l'impossible en l'absence de compétences spécialisées. En adoptant une approche pragmatique fondée sur la valeur des données des organisations et l'évaluation du coût, en francs suisses, des cyberrisques encourus, le label offre aux dirigeants un outil d'aide à la décision essentiel pour prioriser la mise en place de mesures correctives en fonction de leur situation spécifique.

Une démarche participative

Afin de définir les exigences du Label, l'Association mobilise les connaissances et expériences des parties prenantes concernées. Des spécialistes de la sécurité informatique, des représentants des milieux économiques et politiques ainsi que du monde académique et de milieux associatifs se réunissent sous l'égide de l'Association, afin de définir le niveau acceptable de cybersécurité donnant droit au Label. Un tel dialogue entre spécialistes et non-spécialistes de la sécurité informatique est essentiel pour deux raisons : garantir la définition d'exigences en phase avec les réalités des PME et démocratiser les enjeux de cybersécurité qui nous concernent tous. C'est d'ailleurs la raison qui a poussé l'ASLaC à

participer à l'élaboration de la Stratégie Nationale de Protection de la Suisse contre les Cyberrisques (SNPC), dont elle est partenaire pour la mise en oeuvre.

[\[https://www.isb.admin.ch/dam/isb/fr/dokumente/themen/NCS/Umsetzungsplan_NCS_2018-2022_FR.pdf.download.pdf/Umsetzungsplan_NCS_2018-2022_FR.pdf\]](https://www.isb.admin.ch/dam/isb/fr/dokumente/themen/NCS/Umsetzungsplan_NCS_2018-2022_FR.pdf.download.pdf/Umsetzungsplan_NCS_2018-2022_FR.pdf)

Des exigences évolutives

Les exigences définies dans le cadre du Label sont particulièrement innovantes car elles dépendent de la valeur des données nécessaires au bon fonctionnement d'une organisation (notamment les données de tiers, relatives aux clients, aux fournisseurs, etc.). Ainsi une PME qui a plus à perdre en cas de violation des données sous sa responsabilité (perte, fuite, etc.) devra répondre à des exigences de protection plus élevées. Ces exigences portent à la fois sur la sécurité des infrastructures, sur les compétences des collaborateurs (p.ex. identification de courriels malveillants) et sur les questions organisationnelles (p.ex. politique de protection des données).

Une solution abordable et indépendante

Questionnaires en ligne, analyse technique de l'infrastructure informatique ou encore tests d'hameçonnage (phishing) font partie de l'évaluation. C'est sur cette base que l'organisation candidate obtient un rapport contenant notamment le préjudice potentiel lié aux risques encourus en l'état et, le cas échéant, une liste de mesures correctives à mettre en oeuvre pour l'obtention du Label. Une fois les mesures mises en oeuvre avec le prestataire de son choix, l'organisation reçoit la visite d'un auditeur qui effectue un contrôle puis transmet sa recommandation à l'Association en vue de l'octroi du Label. Afin de garantir l'indépendance et la crédibilité du Label, l'Association et les auditeurs s'engagent à ne vendre aucune mesure corrective aux organisations candidates, conservant ainsi strictement son rôle de conseil impartial et indépendant.

Le Label reste valable deux ans, durant lesquels l'organisation labellisée a accès à des services continus, comme des tests de vulnérabilité et de phishing pour s'assurer que le niveau de sécurité reste au moins stable, sinon en amélioration. Les tarifs débutent à 3'000CHF pour une petite PME. Lancement officiel prévu en décembre 2019 sur www.cyber-safe.ch !

Pour toutes questions, merci de vous adresser à :

Association Suisse pour le Label de Cybersécurité (ASLaC)
Christophe Hauert, secrétaire général
Ch. des Picettes 2,
CH-1052 Le Mont-sur-Lausanne

e-mail : chauert@cyber-safe.ch

mobile : 079 628 95 24

Twitter : [@CybersafeLabel](https://twitter.com/CybersafeLabel)

Linkedin : <https://www.linkedin.com/company/cyber-safe-ch>

Annexes:

- Dossier
- Liste fondateurs
- Liste COPIL
- Liste CN
- Logo (attention : uniquement pour utilisation dans le cadre de l'article !!!)