Cahier des charges exigences

V2.0– 25 NOVEMBRE 2019

Table des matières

1 Introduction

1.1 Objectifs du document

Ce document décrit les exigences requises pour l'obtention du Label "cyber-safe". Subsidiairement, il décrit les méthodes de calcul utilisées tout au long du processus de labellisation.

1.2 Principes du Label cyber-safe

Alors que les attaques des systèmes informatiques et autres cyberincidents concernent indistinctement toutes les organisations, quel que soit leur secteur d'activité ou leur taille, la criticité de tels événements est propre à chaque organisation. Par exemple, une menuiserie dont la production est entièrement assistée par ordinateur subira des pertes plus importantes en cas de cyberincident qu'une menuiserie n'utilisant les systèmes informatiques qu'à des fins administratives, comme par exemple un ERP comptable. C'est pourquoi le Label cyber-safe fixe des exigences qui varient selon la place occupée par les systèmes informatiques dans votre organisation.

Pour déterminer la criticité des systèmes informatiques d'une organisation, le Label cyber-safe s'appuie sur une approche pragmatique qui consiste à évaluer la valeur des actifs numériques et des données à protéger et le niveau de cybersécurité requis. Ainsi la première étape de tout processus de labellisation consiste à identifier les types de données que l'organisation candidate a en sa possession. Dans une deuxième étape, une décomposition des impacts en cas de cyberincident sera effectuée sur trois axes pour lesquels il convient d'estimer le montant du dommage économique:

1. **Confidentialité (C)**: quels dommages économiques l'organisation candidate peut-elle subir en cas de divulgation de ses données?
2. **Intégrité (I)**: quels est le montant des dommages pour l'organisation candidate si ses données sont altérées ou modifiées (p. ex. en termes de contenu, de format, d'exactitude, etc)?
3. **Absence de disponibilité** temporaire (AT) et l'indisponibilité définitive (AD): quels sont les coûts engendrés si mes données sont inaccessibles durant une journée, respectivement si elles sont définitivement perdues?

La réponse à ces questions dépend non seulement du type d'activité de l'organisation candidate, qui affecte le type de données en sa possession (par ex. en terme de

confidentialité, la divulgation de données médicales aura des répercussions économiques plus importantes que la divulgation de relevés du temps de travail), mais aussi du nombre de collaborateurs dont l'activité dépend des systèmes informatiques (par ex. en cas d'indisponibilité temporaire des données, le coût variera en fonction du nombre de collaborateurs dont l'activité n'est plus possible en l'absence de données informatiques). Enfin, le Label cyber-safe définit une série d'exigences de base qui relèvent de bonnes pratiques en matière de cybersécurité et à ce titre valable pour toutes les organisations. (p. ex. utilisation et mise à jour d'un anti-virus , existence d'une sauvegarde des données, etc.). Ces exigences génériques sont affinées en fonction de la valeur des données et du nombre de collaborateurs utilisant l'informatique.

1.3 Terminologie

Logiciel métier : Le ou les logiciels qui permettent de gérer les processus de l'entreprise, notamment les progiciels de gestion (*ERP*), les gestionnaires de la relation clients (*CRM*) et les les planificateurs des besoins en composants (*MRP*).

CVSS : *Common Vulnerability Scoring System*, évaluation de la criticité d'une vulnérabilité. (voir https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System)

Équipement réseau : Tous les éléments permettant l'interconnexion d'un réseau informatique, notamment les points d'accès WiFi, les routeurs, les switch, les passerelles, etc...

Périphérique : Tout appareil connecté au réseau et présentant une interface de travail pour l'utilisateur (PC, iMAC, SmartPhone, tablette, etc.)

Réseau de travail : Réseau informatique (physique ou VLAN) sur lequel des collaborateurs travaillent.

Support de données : Le support de donnée est un élément physique qui peut recevoir, conserver et restituer l'information de manière durable.**Valeur d'impact de confidentialité** : Valeur estimée, en francs suisses, du coût de la divulgation des données gérées par l'organisation candidate.

Valeur d'impact d'intégrité: Valeur estimée, en francs suisses, du coût de la modification par un tiers non autorisé de tout ou partie des données gérées par l'organisation candidate.**Valeur d'impact d'absence temporaire de disponibilité** : Valeur estimée, en francs suisses, du coût de l'indisponibilité temporaire des données pour une période donnée.

Valeur d'impact d'absence définitive de disponibilité : Valeur estimée, en francs suisses, du coût de reconstitution des données nécessaires au bon fonctionnement de l'entreprise.

Valeur des données : représente le cumul des valeurs d'impact pour la confidentialité, l'intégrité, la disponibilité temporaire pour une période de 10 jours et l'absence définitive de disponibilité.

2 Conditions d'obtention du Label

2.1 Générales

Les exigences sont valables pour les organisations comprenant un maximum de 250 employés et réparties sur 3 sites géographiques différents. Les organisations ne répondant pas à ces critères restent néanmoins éligibles à l'obtention du Label. Les exigences auxquelles elles doivent répondre sont alors définies sur mesure et au respect des principes du Label par la commission de labellisation de l'Association.

2.2 Valeur des données

La valeur des données est calculée au cas par cas avec l'organisation candidate et en tenant compte de chaque axe C/I/AT/AD.
La valeur total des données, *Vtd*, est calculée en additionnant les valeurs sur les différents axes.

2.3 Catégories d'exposition

L'organisation candidate se voit attribuer une catégorie en fonction de la valeur relative des données *Vrd*, définie par la valeur totale de ses données, *Vtd*, divisée par le nombre de collaborateurs, *Ntc*, exprimé en équivalent plein temps.

$$Vrd = Vtd \,/\, Ntc$$

***Vrd*<=10k**	**10k< *Vrd*<=20k**	**20k< *Vrd*<=50k**	**50k< *Vrd*<=100k**	**100k< *Vrd***
non critique	peu critique	moyennement critique	critique	très critique
cat 1	cat 2	cat 3	cat 4	cat 5

3 Exigences pour l'obtention du Label

Pour que l'organisation candidate soit éligible à l'attribution du Label elle doit satisfaire toutes les exigences requises pour :

- sa catégorie selon le point 2.3

  OU

- le nombre de périphériques utilisés dans l'organisation candidate, à l'exception de l'équipement réseau.

Il suffit qu'une des deux conditions soit remplie pour que l'exigence s'applique à l'organisation candidate.

L'expert peut, exceptionnellement et sur la base d'une justification écrite, recommander l'attribution du Label alors qu'au maximum 2 critères ne sont pas satisfaits.

3.1 Compétences et responsabilités

3.1.1 Ressources humaines

Exigence	Cat.	Nb périph.
a) L'organisation candidate doit avoir désigné une personne de contact interne en charge des questions de l'IT.	2	20
b) L'organisation candidate doit disposer d'une personne de contact formée en informatique (*CFC au minimum*) et avoir, au minimum, suivi une formation de sensibilisation à la cybersécurité.	3	50
c) L'organisation candidate doit disposer dans son comité de direction d'une personne responsable de la cybersécurité.	4	150

3.1.2 Test de phishing

L'évaluation des performances se base sur l'envoi de courriels contenant des contenus différents et envoyés à chaque adresse courriel fournie, selon les règles suivantes:

- Chaque courriel envoyé contient au minimum un élément permettant au collaborateur de constater qu'il s'agit d'un courriel frauduleux.
- Les courriels envoyés sont génériques et facilement détectables comme étant frauduleux.
- Au minimum 5 courriels sont envoyés à chaque adresse.
- La période de test dure entre 2 et 6 semaines, selon le nombre d'adresses.
- Chaque courriel contient une image qui, une fois affichée, est comptabilisée dans les statistiques d'hameçonnage.
- Chaque courriel contient un lien qui, une fois cliqué, est comptabilisée dans les statistiques d'hameçonnage

Exigence	Cat.	Nb périph.
a) Le taux de clics moyen calculé pour l'ensemble des courriels envoyés doit être inférieur à 25 %		
b) Le taux de clics moyen calculé pour l'ensemble des courriels envoyés doit être inférieur à 20 %	2	
c) Le taux de clics moyen calculé pour l'ensemble des courriels envoyés doit être inférieur à 17 %	3	
d) Le taux de clics moyen calculé pour l'ensemble des courriels envoyés doit être inférieur à 15 %	4	
e) Le taux de clics moyen calculé pour l'ensemble des courriels envoyés doit être inférieur à 12 %	5	

3.2 Infrastructure IT

3.2.1 Inventaire

Exigence	Cat.	Nb périph.
a) L'organisation candidate doit maintenir à jour un inventaire exhaustif de l'infrastructure TIC ainsi que de tous les éléments connectés sur le(s) réseau(x) de travail (PC, iMac, SmartPhone,	3	20

Exigence	Cat.	Nb périph.
tablette, objet internet, etc.).		
b) L'organisation candidate doit maintenir à jour un inventaire exhaustif des services sur le cloud contenant des données.	2	

3.2.2 Chiffrement

Exigence	Cat.	Nb périph.
a) Les canaux de communication depuis l'extérieur (y.c. VPN) sont chiffrés et contrôlés au moins tous les 2 ans.	3	
b) Identifier quelles données doivent être chiffrées (lors de la transmission et/ou lors du stockage) et s'assurer de leur chiffrement.	4	
c) Les données présentes sur les périphériques mobiles (ordinateurs, SmartPhone, tablette, objet internet, etc.) sont systématiquement chiffrées.	3	

3.2.3 WiFi

Exigence	Cat.	Nb périph.
a) Les réseaux WiFi doivent être chiffrés (WPA2 au minimum) et protégés par un mot de passe* (16 caractères minimum).		
b) Le réseau WiFi invités doit être séparé du réseau de travail.	2	
c) Le réseau WiFi interne doit être séparé du réseau de travail si les collaborateurs peuvent se connecter avec des appareils non répertoriés dans l'inventaire (p. ex. Smartphones, périphériques privés, …), qui ne doivent en aucun cas utiliser le réseau de travail.	3	
d) Un réseau logique (VLAN) dédié aux téléphones IP (IP-Phones) séparé du réseau de travail doit avoir été mis en place.	4	

* qui ne doit pas être un mot de passe par défaut.

3.2.4 Accès physique

Exigence	Cat.	Nb périph.
a) Toutes les installations hébergeant des données doivent être sécurisées contre les accès physiques de personnes non autorisées.		
b) L'accès au centre de calcul par des externes est contrôlé (p.ex. liste avec les personnes qui accèdent, quand, de quel fournisseur, etc.).	3	
c) Lors de leur élimination, tous les supports de données le sont en veillant à la destruction définitive des données qui s'y trouvent.		

3.2.5 Scans internes

Exigence	Cat.	Nb périph.
a) Aucune vulnérabilité considérée avec un score CVSS supérieur ou égal à 9,0 ne doit être signalée par un scan depuis l'intérieur des réseaux de travail.*	2	

*Un hôte présentant une vulnérabilité avec un score CVSS supérieur ou égal à 9,0 ne peut être toléré que dans un réseau logique séparé et sans accès internet.

3.2.6 Scans externes

Exigence	Cat.	Nb périph.
a) Aucune vulnérabilité avec un score CVSS supérieur ou égal à 7,0 ne doit être signalée par un scan des adresses IP publiques de l'infrastructure depuis l'extérieur .		
b) Un hôte publiquement accessible et présentant une vulnérabilité avec un score CVSS supérieur ou égal à 7,0 et inférieur à 9,0 ne peut être toléré que lorsque qu'une règle de pare-feu en restreint l'accès en-dehors des zones géographiques nécessaires à la bonne marche des affaires.		

3.3 Organisation

3.3.1 Protection des données

Exigence	Cat.	Nb périph.
a) L'organisation candidate déclare respecter la réglementation en matière de protection des données (voir annexe 1).		

Les principes en matière de protection des données inclus dans la LPD (obligatoire pour toute entreprise en Suisse) ainsi que le RGPD, lorsqu'il est applicable.

3.3.2 Prestataires tiers

Exigence	Cat.	Nb périph.
a) Lorsque l'accomplissement de certaines exigences dépend d'un ou plusieurs sous-traitants, l'organisation candidate exige un engagement sur la mise en œuvre de mesures de sécurité, par exemple par un label ou une certification au moins équivalent.	3	

L'usage du « Cloud » est considéré comme un service fourni par un sous-traitant.

3.3.3 Ressources humaines

Exigence	Cat.	Nb périph.
a) L'organisation candidate doit maintenir à jour une liste des permissions d'accès pour toutes les catégories de données et types de collaborateurs (plan de droit).	3	30
b) L'organisation candidate doit contrôler au moins une fois par année que la liste des permissions d'accès correspond aux droits effectivement attribués.		20
c) Aucun collaborateur ne doit disposer d'un accès administrateur sur son poste local, hormis le personnel de l'informatique.	3	
d) L'organisation candidate a fait signer à chaque collaborateur un document définissant leurs droits et devoirs vis-à-vis des ressources informatiques.		
e) L'organisation candidate dispose d'une politique de sécurité des systèmes d'information.		30

3.3.4 Procédures, routines

Exigence	Cat.	Nb périph.
a) Les mises à jour des systèmes d'exploitation des périphériques et serveurs sont appliquées et contrôlées régulièrement.		
b) Les mises à jour des logiciels, hors logiciels métiers, des périphériques et serveurs sont appliquées et contrôlées régulièrement.		
c) Les mises à jour des équipements du réseau sont appliquées et contrôlées régulièrement.	3	
d) La présence et la mise à jour d'un antivirus sur tous les périphériques est contrôlée régulièrement.		
e) Les alertes de sécurité sont centralisées et traitées régulièrement.	3	30
f) Un pare-feu est présent entre le réseau de travail et l'extérieur.	2	
g) Le fonctionnement, la configuration et la mise à jour du pare-feu sont vérifiés régulièrement.	3	

3.3.5 Sauvegardes

Exigence	Cat.	Nb périph.
a) L'organisation candidate doit avoir mis en place un système de sauvegarde des données.		
b) L'intervalle de la sauvegarde est d'un minimum une fois par semaine.		
c) L'intervalle de la sauvegarde est d'un minimum une fois par jour.	3	10
d) L'organisation candidate doit pouvoir restaurer l'état de son système et de ses données à l'état d'il y a 1 mois.		
e) L'organisation candidate doit pouvoir restaurer l'état de son système et de ses données à l'état d'il y a 3 mois.	3	50
f) L'organisation candidate doit pouvoir restaurer l'état de son système et de ses données à l'état d'il y a 6 mois.	5	200
g) Le bon fonctionnement de la sauvegarde est contrôlé au moins	2	

Exigence	Cat.	Nb périph.
une fois par semaine.		
h) Une copie des données existe dans un second emplacement distant d'au moins 10 km.	2	
i) Il n'est pas possible pour une personne seule (y.c. un administrateur) de détruire toutes les sauvegardes.	4	100
j) Un test de récupération des données sauvegardées les plus récentes et les plus anciennes doit être effectué au minimum annuellement.	3	50

3.3.6 Résilience

Exigence	Cat.	Nb périph.
a) Il existe un plan et des procédure de reprise en cas d'interruption de la production informatique.	4	150
b) Les procédures de reprises sont testées au moins une fois par an.	5	200

3.3.7 Mots de passe

Les politiques de mot de passe doivent être implémentées de manière à obliger chaque collaborateur à les respecter.

Exigence	Cat.	Nb périph.
a) Les mots de passe ont une longueur de 10 caractères au minimum, dont des majuscules, minuscules, chiffres et caractères spéciaux.		

4 Annexe 1 - Principes en matière de protection des données :

L'organisation candidate s'engage à respecter les principes reconnus en matière de protection des données:

- Licéité (ou légalité) : le traitement de données personnelles ne doit pas enfreindre de lois (LPD et RGPD si applicable). Il doit reposer sur une base légale, sur le consentement éclairé ou sur un intérêt prépondérant public ou privé.
- Bonne foi : les données ne doivent en principe pas être collectées et traitées à l'insu de la personne concernée ou contre sa volonté. Elles ne doivent pas non plus être collectées par tromperie intentionnelle;
- Proportionnalité : le traitement des données personnelles doit être nécessaire, adéquat et le moins intrusif possible ;
- Finalité : les données personnelles ne doivent être traitées que dans le but indiqué lors de leur collecte, qui est prévu par la loi (LPD et RGPD si applicable ou obligation légale) ou qui ressort des circonstances ;
- Exactitude : celui qui traite des données personnelles doit s'assurer qu'elles sont correctes et prendre toute mesure appropriée pour les mettre à jour cas échéant, en particulier permettant d'effacer ou de rectifier les données inexactes ou incomplètes ;
- Sécurité : les données personnelles doivent être protégées contre tout traitement non autorisé, par des mesures organisationnelles et techniques appropriées ;
- Transparence de la collecte : la collecte de données personnelles et sa finalité doivent être reconnaissables pour la personne concernée.
- Toutes autres obligations légales s'appliquant au secteur d'activité de l' organisation candidate.