cetic
Your Connection to ICT Research

Multitel
INNOVATION CENTRE

Keep it secure | digital wallonia .be

Bâtir la cybersécurité de votre PME sur des fondations solides

Christophe Ponsard

Coordinateur Recherche-Innovation-Entreprise

Digital Wallonia Champion

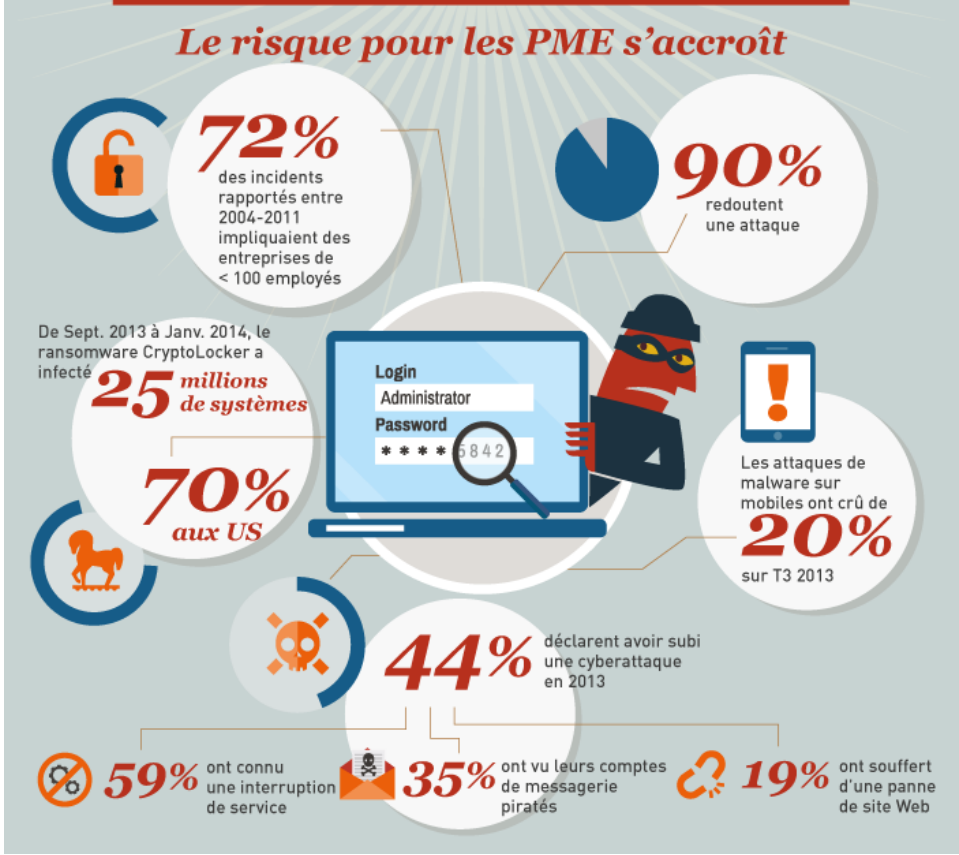
Cybersecurity Forum, Nivelles, 13 Septembre 2020

digital wallonia .be | Agence du Numérique

INFOPOLE CLUSTER TIC

PME et cybersécurité

- Une romance tumultueuse !
- Un mal nécessaire ?
- Une opportunité et un atout ?



- Définitivement une plus-value pour l'entreprise

KIS - Bilan et Perspectives sur 5 axes

1. CONFIANCE - labellisation d'acteurs à même d'accompagner les PMEs wallonnes dans la gestion de la sécurité

2. AIDE - incitants, mise en place d'aides à l'investissement dans la sécurité informatique

3. SENSIBILISATION des entreprises, des services publics, des citoyens sur l'importance de la sécurité informatique

4. EDUCATION et FORMATION à la sécurité informatique

5. RAYONNEMENT INTERNATIONAL

digital wallonia .be | Agence du Numérique

Axe 1 – CONFIANCE - Dispositif Keep It Secure (KIS)

- Cadre de base : audit de sécurité global
- Problèmes → Solutions personnalisées
- Liste de prestataires de qualité (= évalués par le dispositif)
- Alignement avec des initiatives fédérales et internationales

Périmètre du dispositif KIS

- Grandes entreprises
- Secteur Institutionnel
- Audit GDPR

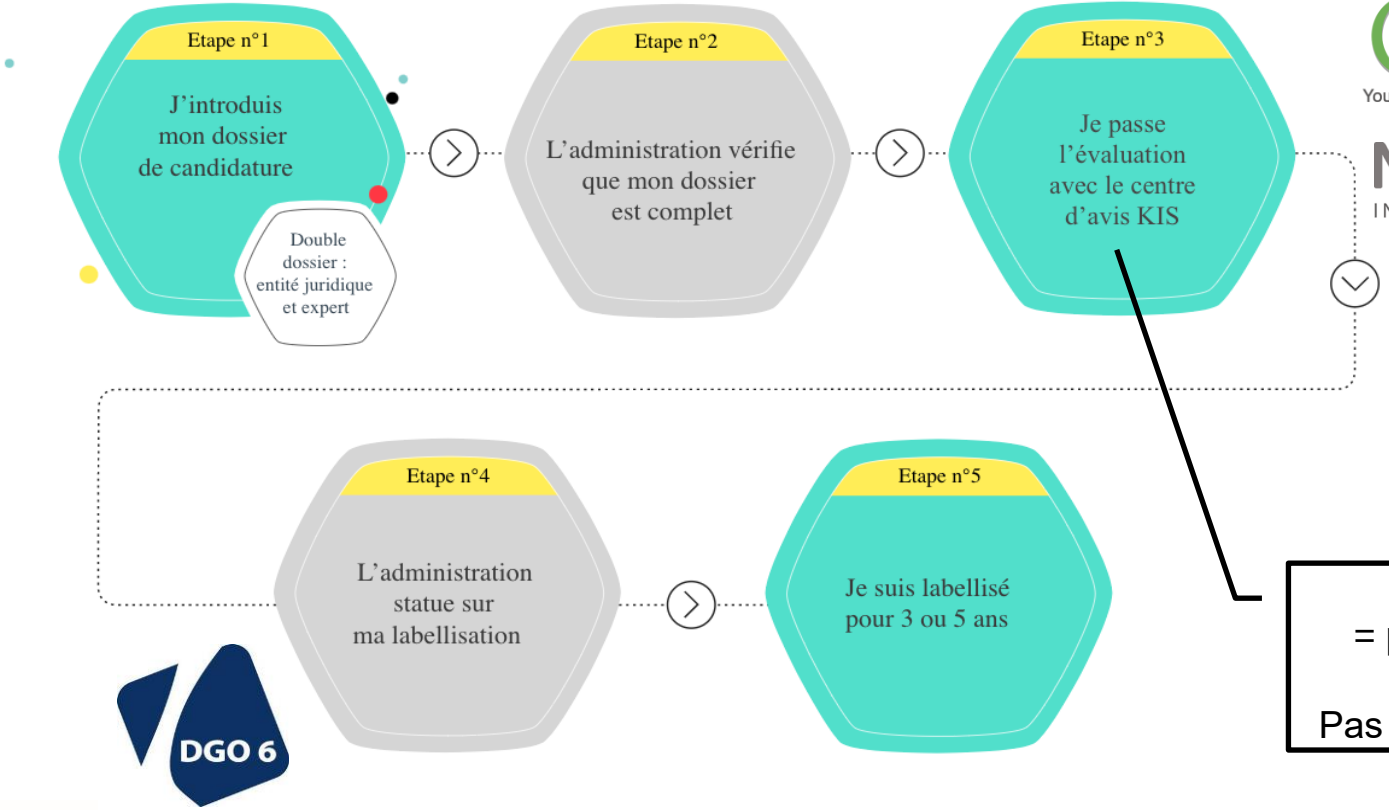
- AdN → Evaluation des prestataires
  - Connaissance large du domaine de la sécurité
- Prestataires → Audit des PME
  - Prendre en compte du contexte
  - Rapport global, plan d'actions
  - Soutien financier (voir axe 2)

Le dispositif KIS (et capacité requises)

- Profilage des PME ➔ mesures adaptées
- Contrôle de base :
  - Normes officielles
  - Initiatives européennes et mondiales
  - Evolutif (voir cadre fédéral et européen)

CIS Center for Internet Security®

Devenir un prestataire KIS



cetic
Your Connection to ICT Research

Multitel
INNOVATION CENTRE

digital wallonia .be
Agence du Numérique

Bases de KIS - Panorama européen (2018)

Name	Type	Country	Organisation	SME	Controls	Tools	Scheme	Maturity	Since
Cyber Essentials	Label	UK	Gov.	Yes	5 main controls	Online self assess.	Accreditation and certification	2 levels	2013
ANSSI Certif.	Label	France	ANSSI	Yes	Unknown	Unknown	Based on Common Criteria	2 levels	2015
BSI	Advice	Germany	Gov.	Yes	ISO27K based	Threat catalogue			2008
VdS	Certif.	Germany	Private	Yes	4 areas	online self-assess.	Approved service providers	4 levels	2017
Italian Frame work	Frame work	Italy	CINI	Yes	CSF based 11 guidelines	Unknown	Unknown	4 levels	2015
ISO27K	Standard	Intl	ISO	No	11 areas 130 controls	Many ISMS tools	Accreditation and certification	No (scope based)	2013 (latest)
NIST CSF	Frame work	US/Intl	NIST	Some	5 functions exhaustive mapping	CSF Reference Tool	Not Applicable	4 tiers	2015
ISSA 5173	Standard	UK	ISSA	Yes	10 categories	Unknown	Unknown	3 levels	2011
CIS Top 20	Good practices	US/Intl	Center of Internet Security	Yes	20 controls	Support for control automation	Informal use	3 levels (6+10+4)	2008
ECSO	Meta Schema	Europe	NPO	Some	N/A	N/A	Governance aspects	2 key levels with tunable sub-levels	2018

Référentiels CIS 20 et NIST CSF

Basic CIS Controls

1	Inventory and Control of Hardware Assets	2	Inventory and Control of Software Assets
3	Continuous Vulnerability Management	4	Controlled Use of Administrative Privileges
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	6	Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7	Email and Web Browser Protections	8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols and Services	10	Data Recovery Capabilities
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	12	Boundary Defense
13	Data Protection	14	Controlled Access Based on the Need to Know
15	Wireless Access Control	16	Account Monitoring and Control

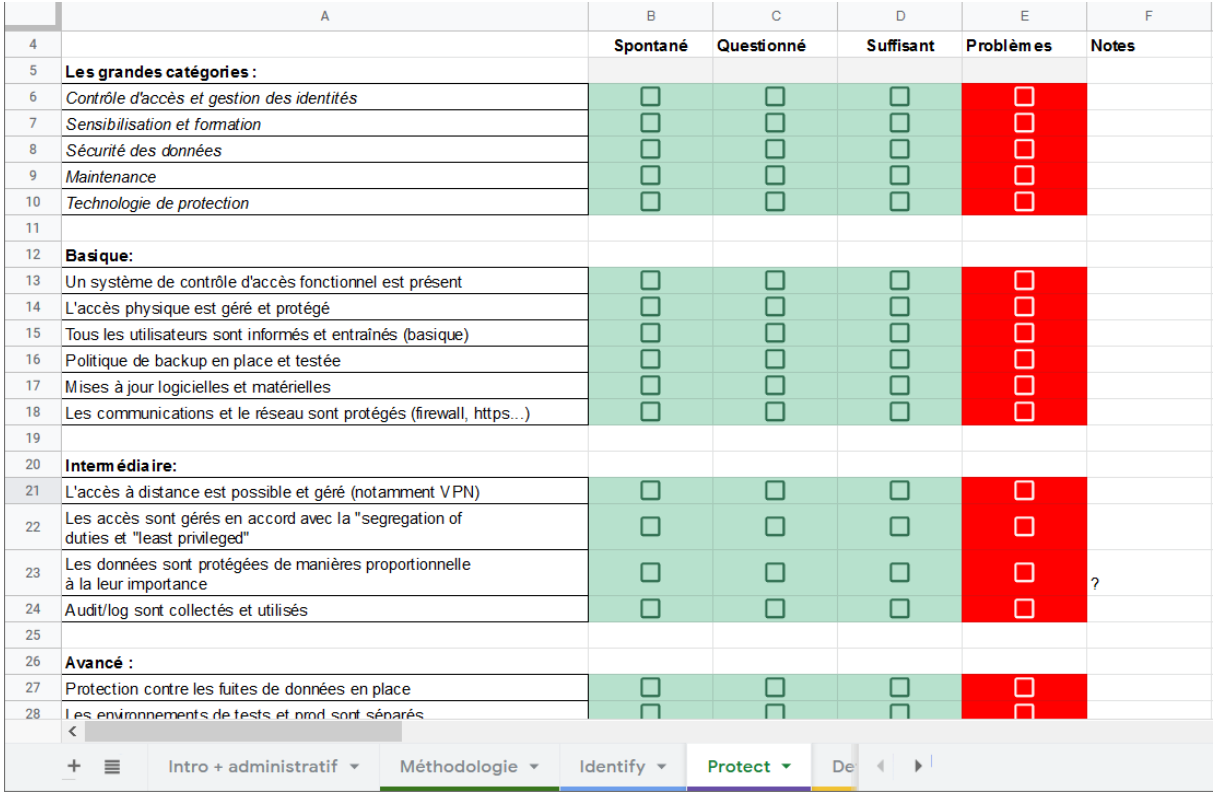
Organizational CIS Controls

17	Implement a Security Awareness and Training Program	18	Application Software Security
19	Incident Response and Management	20	Penetration Tests and Red Team Exercises

Levels	Basic	
1	15	Wireless Access Control
	7	Email and Web Browser Protections
	17	Implement a Security Awareness and Training Program
	18	Application Software Security (spécifique PME développeur)
	3	Continuous Vulnerability Management
	10	Data Recovery Capabilities
	13	Data Protection
	8	Malware Defenses
2	5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
	9	Limitation and Control of Network Ports, Protocols and Services
	1	Inventory and Control of Hardware Assets
	2	Inventory and Control of Software Assets
	11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
3	4	Controlled Use of Administrative Privileges
	12	Boundary Defense
	14	Controlled Access Based on the Need to Know
	6	Maintenance, Monitoring and Analysis of Audit Logs
	16	Account Monitoring and Control
	19	Incident Response and Management
	20	Penetration Tests and Red Team Exercises

Check liste

- Conduite des évaluations
- Couverture
  - Technique
    basée sur les référentiels
  - Audit/soft skills
    focus PME
    contextualisation
- Evaluation multi-niveau
  - Basique ➔ avancé
  - Echelle % niveau de spontanéité
  - Aspect internalisé/externalisé
    un peu… pas trop…
    pointu=normal (ex. pentest)

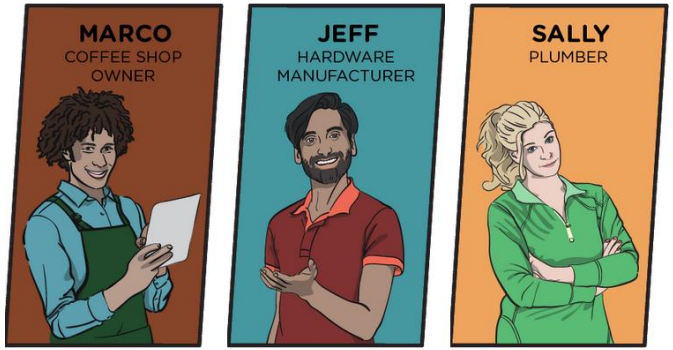


	A	B	C	D	E	F
4		Spontané	Questionné	Suffisant	Problèmes	Notes
5	**Les grandes catégories :**					
6	*Contrôle d'accès et gestion des identités*	☐	☐	☐	☐	
7	*Sensibilisation et formation*	☐	☐	☐	☐	
8	*Sécurité des données*	☐	☐	☐	☐	
9	*Maintenance*	☐	☐	☐	☐	
10	*Technologie de protection*	☐	☐	☐	☐	
11						
12	**Basique:**					
13	Un système de contrôle d'accès fonctionnel est présent	☐	☐	☐	☐	
14	L'accès physique est géré et protégé	☐	☐	☐	☐	
15	Tous les utilisateurs sont informés et entraînés (basique)	☐	☐	☐	☐	
16	Politique de backup en place et testée	☐	☐	☐	☐	
17	Mises à jour logicielles et matérielles	☐	☐	☐	☐	
18	Les communications et le réseau sont protégés (firewall, https...)	☐	☐	☐	☐	
19						
20	**Intermédiaire:**					
21	L'accès à distance est possible et géré (notamment VPN)	☐	☐	☐	☐	
22	Les accès sont gérés en accord avec la "segregation of duties et "least privileged"	☐	☐	☐	☐	
23	Les données sont protégées de manières proportionnelle à la leur importance	☐	☐	☐	☐	?
24	Audit/log sont collectés et utilisés	☐	☐	☐	☐	
25						
26	**Avancé :**					
27	Protection contre les fuites de données en place	☐	☐	☐	☐	
28	Les environnements de tests et prod sont séparés	☐	☐	☐	☐	

Intro + administratif | Méthodologie | Identify | Protect | De

Audit via des cas pratiques orientés PME

- Exemple 1 : Magasin traditionnel
  - Quelques employés/PC
  - Un seul site, logiciel compte/stocks
  - Pas de vente en ligne
  - Présence d'une connexion WIFI



- Exemple 2 : Entreprise multi-sites
  - Plus d'employés, postes informatiques
  - Echanges d'information entre les sites, accès externes
  - …

- Exemple 3: Entreprise très connectée
  - Site web, vente en ligne
  - …

Bilan des activités (fin 2019)

- 25 experts de 21 entreprises (maintenant environ une 30aine)
- Taille de l'entreprise:
  - TPE: domaine d'activité = domaine d'expert (unique)
  - intermédiaires = réseau d'experts en cybersécurité
  - ME: plus large éventail d'activités, pool d'experts cybersécurité

Size	# companies
1	10
2-5	7
6-10	2
>10	2
Total	21

- Répartition entre les domaines:
  - BEAUCOUP de dev (web)
    - souvent OK techniquement
    - mais manque de vision % organisation
  - experts cybersécurité tous acceptés
    - attention au contexte PME
  - Auditeurs et consultants informatiques en entreprise
    - bonnes capacités d'évaluation des risques
    - Vérification du niveau requis d'expertise technique en cybersécurité: généralement OK

Domain	Total	# full accept	# cond. accept	# reject
devops	7	3	3	1
cybersecurity	6	6	0	0
web developer	6	3	2	1
GDPR expert	6	4	0	2
IT audit/strategy	5	4	1	0

Bilan des activités (suite)

- Métrique de classement
  - Spontané: 10/10
  - Interrogé: 6.7 / 10
  - Basique: 3,3 / 10
  - Problématique: 0/10

$$\frac{30.\#\{spontaneous\} + 20.\#\{questioned\} + 10\#\{basic\}}{3.\#\{audited\}}$$

Phase	Spont.	Quest.	Basic	Disc.	Score
Identify	60%	10%	23%	11%	7,4
Detect	62%	15%	22%	6%	7,9
Protect	78%	5%	15%	7%	8,6
Respond	60%	3%	21%	21%	6,9
Recover	53%	6%	24%	21%	6,5

- score plus élevé pour la protection
- suivi par la détection et de l'identification = phases « amont »
- phases de réaction et récupération moins bien couvertes (biais possible)

Réflexions et points d'attention

- N'impose pas de méthodologie
  - mais mieux vaut disposer d'une démarche systématique
    qu'elle soit personnelle ou basée sur un référentiel (constat assez variable)
  - vérifiée sur base de référentiels compatibles PME
- Démarche personnelle
  - Etre suffisamment bon sur les aspects techniques et organisationnels
  - Partage d'expérience encouragé au sein d'une entreprise (template, méthodo…)
  - Pour une entreprise spécialisée: soit labelliser un expert responsable (qui délègue) soit plusieurs experts
    frein financier à la seconde option levé ➔ encouragé (reconnaissance, réalité, formation,…)
- RGPD: ne PEUT pas être le focus central
  - Cependant contexte possible, du moment que l'audit cybersécurité soit complet
- Processus généralement très constructif… ➔ volonté de mieux protéger les PME
  même si lenteurs administratives (aggravées par le COVID) ➔ tjs intérêt du prestataire

Résumé et lien avec le schéma fédéral

Axe 2 – AIDE - Chèque Cybersécurité

Objectifs :

- permettre aux PMEs d'investir dans la sécurité informatique
  en tenant compte de leurs moyens aussi bien financiers qu'humains et de leurs compétences
- encourager les prestataires compétents en cybersécurité à venir en aide aux PME

Le Chèque-cybersécurité permet aux PME/TPE de se faire aider par un prestataire

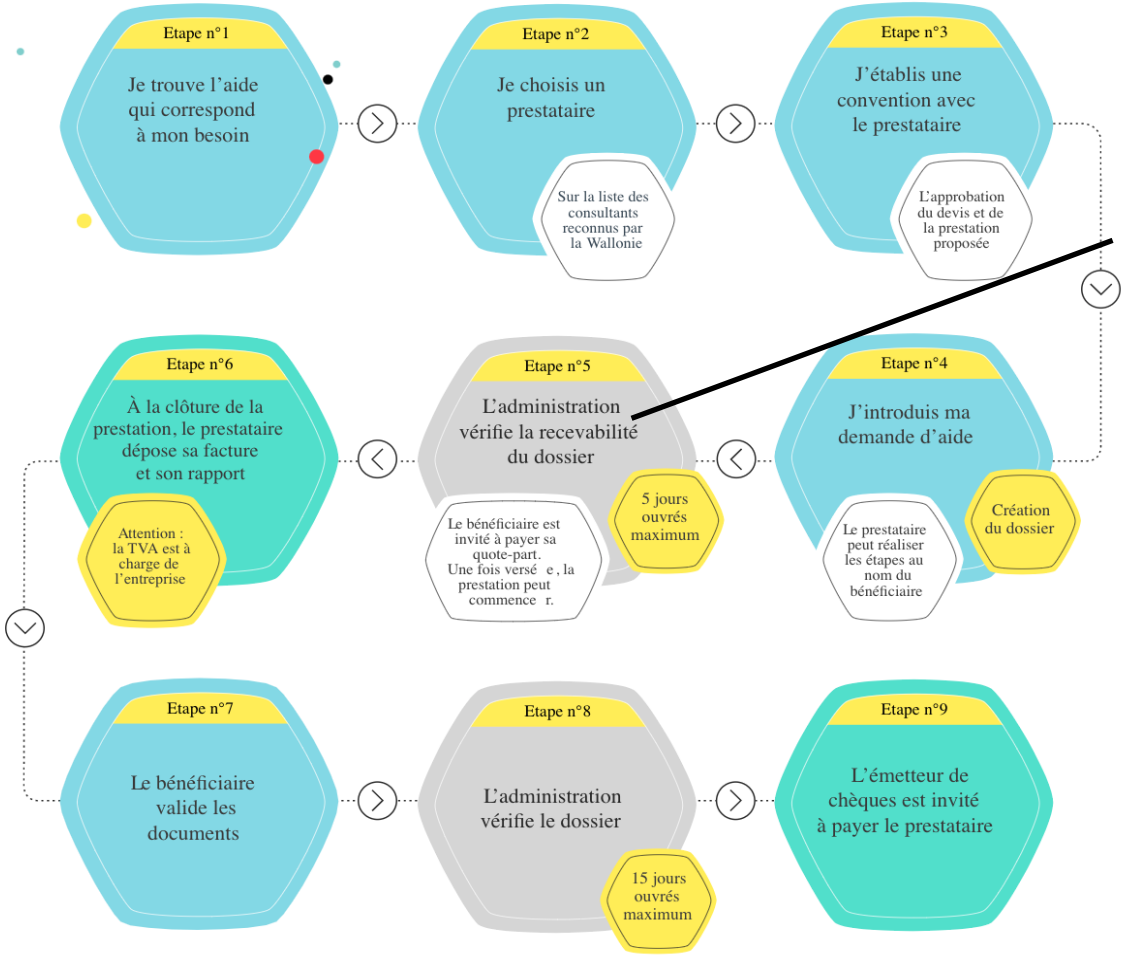
- pour réaliser un audit/diagnostic de la cybersécurité de son entreprise
- ce consultant, ou un autre, pourra ensuite mettre en place les actions préconisées

https://www.cheques-entreprises.be/cheques/cybersecurite

A ce jour, **105 bénéficiaires ont pu être accompagnés par 29 experts**

pour un montant total de 630.000 €

Processus des Chèques (Cybersécurité)



Exemples: restriction de code NACE
Prestation de mise en conformité pure (GDPR)

digital wallonia .be
Agence du Numérique

Axe 3 - Sensibilisation

Objectifs :

- augmenter le niveau d'information générale des PMEs wallonnes
- sensibiliser les entreprises et citoyens aux enjeux de la cybersécurité au-delà la protection des données

Les actions menées se sont en coordinations avec le niveau fédéral et l'Europe. En 2019

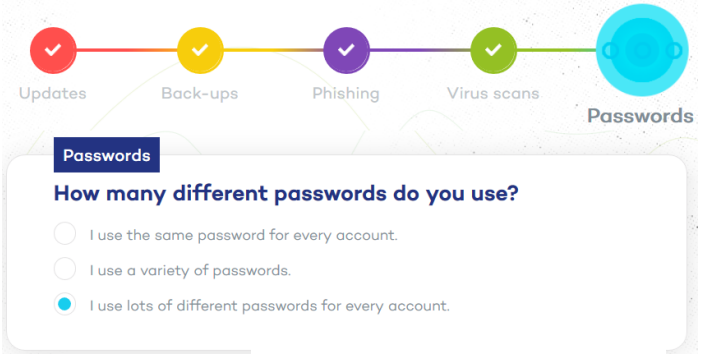
- Cyber Security KIT par la Cyber Security Coalition : https://www.cybersecuritycoalition.be/resource/cyber-security-kit-french/
- Plateforme Safe on web par le Center for Cybersecurity Belgium (CCB): https://www.safeonweb.be/fr
- Le mois européen de la cybersécurité avec chaque année un focus spécifique ➔ **ce mois d'octobre !**
- La réalisation d'une synthèse sur les outils de sensibilisation permettant d'accompagner efficacement les PME (campagnes, ateliers, gamification, applications spécifiques,...)

En 2020, un premier Atelier Digital/Webinaire Cyber & Sécurité organisé par l'INFOPOLE
en étroite collaboration avec edn Wallonia, les Chèques-entreprises et l'Agence du Numérique.
Plus à suivre… en mode adapté !

Quelques actions de sensibiliation

SME Security Scan

Cyber security KIT
https://www.cybersecuritycoalition.be/resource/cyber-security-kit-french



Digital Health Index
https://www.safeonweb.be

Axe 4 – Education et Formations

Objectifs :

- développer et faire connaître l'offre de formations pour diverses audiences: chefs d'entreprise, personnes actives en entreprise ou des chercheurs d'emploi
- relayer vers les acteurs du grand public ciblant des risques spécifiques (enfant, ados, fracture numérique)

A l'aide d'une série d'acteurs spécialisés dans le domaine notamment :

- les acteurs de formations actifs en Wallonie tels que Technofutur, Technobel, eCampus ;
- les fédérations sectorielles qui organisent des formations pour leurs membres ;
- les hautes écoles et les universités également impliquée dans le comité de gouvernance ;
- l'Agence du Numérique via son programme école numérique

Exemples en cours: Learn4KIS et eCampus

Learn4KIS

- contenu pédagogique pour TPE/PME wallonnes pour **former des référents en cybersécurité**
- approche en blended learning sur mesure pour ces entreprises avec impact minimal
- mené conjointement par Technofutur TIC et le CPEHN qui s'appuieront sur Numéria en opération
- validation du contenu par le CETIC au niveau technique et cohérence avec KIS
- les premières formations du projet devraient démarrer au 1er trimestre 2021

Eurometropolitan eCampus

- formation de spécialistes et de managers généralistes en informatique dans les organisations privées et publiques.
- dispensé en collaboration avec Multitel un cycle de formations en cybersécurité depuis plusieurs années
- le programme couvre: aspect internes, externes, protection des données, IA, IoT
- également: partenariat avec la Haute école Condorcet pour un Bachelier spécialisé en Cybersécurité
- Cyles de formations à la directive NIS ➔ également organisé au niveau de workshops au fédéral

Axe 5 – Rayonnement International

Objectifs:

- Identifier les bonnes pratiques et solutions
- favoriser la coopération transrégionale et la visibilité de la Wallonie

La Wallonie est concrètement impliquée dans le projet Interreg européen **CYBER** (2018-2023)

- accent sur le partage de bonne pratiques et la coopération transrégionale en cybersécurité
- place prépondérante à la PME, acteur vital dans l'économie wallonne
  dans la continuité du travail effectué avec KIS

Les acteurs de KIS sont également impliqués avec l'**ECSO** pour les actions à long terme:

- Échanges d'expérience au de la des partenaires CYBER
- Interaction avec les projets pilotes SPARTA, ECHO, …
- Développement d'un label « Cybersecurity Made in Europe »
- Evolution de la structure européenne: mise en place des « competence centers », DIH, etc

Questions ?

Agence du Numérique

www.digitalwallonia.be
info@digitalwallonia.be
@digitalwallonia
facebook.com/digitalwallonia

Avenue Prince de Liège, 133
B-5100 Jambes
+32 (0)81 778080

digital wallonia .be | Agence du Numérique