Annexe : Courte description des 13 lauréats et leur projet

5 appels à projets visant à contribuer au renforcement de la cyber-résilience des PME ont été lancés le 27 juillet 2022 et se sont clôturés le 31 octobre 2022.

Chaque appel à projet représente une thématique par laquelle un renforcement de la cyber-résilience des PME est envisagé.

Thème 1 : Mesures organisationnelles

Objectif : Sensibiliser et activer les PME quant à leur cybersécurité et leur préparation face aux cyber-incidents (évaluation des actifs, procédures essentielles).

2 projets ont été sélectionnés pour un budget de 773.469 €.

1) **NSZ et Safeshops : BeCyberSafe**

BeCyberSafe offre un programme de formation (webinaires, podcasts, écrits) pour sensibiliser les commerçants à la cybersécurité dans l'e-commerce. Les informations seront disponibles sur une plateforme numérique.

2) **Unizo : ORG2CS – Organisatorische maatregelen**

Le projet ORG2CS est un guide de cybersécurité pour les PME, visant à les sensibiliser à son importance, à évaluer leur situation actuelle et à leur offrir des options de prévention et de réponse aux cyber-attaques. Le contenu du guide sera facilement accessible, même pour les PME ayant peu de connaissances en cybersécurité.

Thème 2 : Mesures techniques

Objectif : sensibiliser et activer les PME vis-à-vis de l'importance d'utiliser les bons outils de défense, de les maintenir à jour et de pouvoir en interpréter les résultats, et leur offrir des solutions adaptées pour combler les vulnérabilités techniques.

1 projet pour un budget de 679.170 €

3) **Jimber : Network Isolation**

Le projet Network Isolation vise à fournir aux PME un réseau hautement sécurisé en se concentrant sur l'isolation du réseau, un élément spécifique essentiel de la cybersécurité. Il offre aux PME un accès au logiciel Network Isolation, un produit innovant sur le marché, pendant 12 mois, tout en identifiant leurs besoins spécifiques et vulnérabilités.

Thème 3 : Formation et accès aux compétences

Objectif : former les PME et les aider à trouver la meilleure approche pour acquérir les compétences requises en cybersécurité (renforcement des connaissances, trajets d'amélioration au niveau sectoriel, intégration de la cybersécurité dans les formations, identification précise des compétences nécessaires).

7 projets sélectionnés pour un budget de 2.262.024,67 €.

4) **Federatie van Algemene Bouwaannemers (FABA) : Bevordering Cyberweerbaarheid van KMO's: de snelbouwstenen van een Cyberveilige(re) Bedrijfsvoering**

Le projet vise à former les entrepreneurs et employés du secteur de la construction sur les compétences nécessaires pour renforcer la cybersécurité de leur entreprise. Il est conçu de manière accessible, avec un processus en trois phases : la sensibilisation et la motivation préalables, une formation sur deux ans et demi en présentiel et à distance, et enfin, le suivi post-formation avec des KPI liés à la formation et des tests de phishing. Cibler spécifiquement une partie du public-cible avec laquelle le candidat a des affinités facilitera l'accès de la formation à ce segment d'entrepreneurs.

5) **Psybersafe : Psybersafe – Behavioural science based cyber security awareness training**

Psybersafe favorise le changement de comportement en proposant des formations interactives et ludiques, adaptées aux PME. Les sessions durent de 5 à 10 minutes par employé par mois pour convenir aux entreprises ayant peu de temps. Les formations abordent des sujets pertinents pour les débutants tels que les mots de passe, les fuites de données et le GDPR, avec des solutions proposées pour chaque apprentissage.

6) **Xerius (blended learning) : Cyberveilig ondernemen**

Le projet Cyberveilig ondernemen offre un parcours d'apprentissage comprenant 8 modules interactifs, accessibles sur une plateforme développée et utilisée par Xerius. Les webinaires complémentaires permettent d'approfondir les connaissances et d'interagir avec les formateurs. Le projet se concentre spécifiquement sur les chefs d'entreprise actuels et futurs, en proposant une approche concise et facile d'accès.

7) **Headmind Partners Belgium : BE Aware – Your safety is our success!**

Le projet BE Aware propose aux PME des exercices de sensibilisation à la cybersécurité via des techniques de gamification et de jeu de rôles. L'objectif est de fournir des formations originales et captivantes, comprenant un exercice de crise pour gérer les cyber-incidents et une formation en escape room pour la sensibilisation à la cybersécurité.

8) **NVISO : CyBErWise**

Le projet CyBErWise développe un outil de jeu pratique et interactif, offline et online, pour sensibiliser les PME et les indépendants à la cybersécurité. Son objectif est de présenter et renforcer les concepts clés de la cybersécurité, incluant l'identification des comportements souhaitables, la détection des signes d'incidents et l'identification des domaines d'amélioration. L'outil sera convivial, informatif, engageant et facile à intégrer dans le quotidien.

9) **Consortium Sirris Howest VUB UCLouvain : CyberActive – Activating Cybersecurity skills in value chains for manufacturing and digital services**

Le projet CyberActive propose une approche complète pour former et sensibiliser les entreprises manufacturières et de services numériques à la cybersécurité. Il combine des sessions de formation en ligne et en personne d'une durée de 2 heures, des courts métrages instructifs pour renforcer la sensibilisation, ainsi que du matériel de formation comprenant 18 sets de diapositives.

10) Cyber Way Finder : LEARN, SECURE, REPEAT

Le projet LEARN, SECURE, REPEAT propose un programme de formation en 3 phases progressives, adapté aux besoins individuels des participants. Les séries d'ateliers de cybersécurité abordent des sujets tels que l'inventaire des actifs, l'analyse des risques, la sensibilisation aux incidents et la gestion des accès. Les formations seront personnalisées par secteur, en collaboration avec les organisations représentatives.

Thème 4 : Accompagnement professionnel

Objectif : accompagner professionnellement les PME dans l'amélioration de leur cybersécurité (diagnostic/audit complet, état du marché, soutien à la mise en œuvre et suivi)

2 projets sélectionnés pour un budget de 1.256.520 €.

11) Cresco : Cybersecurity Improvement Trajectory

Le projet Cybersecurity Improvement Trajectory propose des audits individuels pour créer un guide interactif, offrant des documents et services faciles à utiliser de manière autonome par les entreprises. Ce guide partagera des expériences et des meilleures pratiques basées sur des cas réels de trajectoires d'amélioration de la cybersécurité, et il sera largement applicable par les PME.

12) Jimber : Light Security Audit

Le projet Light Security Audit propose un audit technique de cybersécurité pour les PME, suivi d'un plan d'action clair et étape par étape avec des solutions. Les instructions précises sur la façon de remédier aux lacunes sont fournies. L'objectif est de sensibiliser les PME aux risques cyber et de les motiver à prendre des mesures de protection supplémentaires. Un suivi est effectué un an après pour évaluer la mise en œuvre des solutions choisies et déterminer si des actions supplémentaires sont nécessaires.

Thème 5 : Projets transversaux spécifiques

Objectif : améliorer la cybersécurité de deux groupes spécifiques de PME, à savoir les petits commerçants et les entrepreneuses, à partir d'une approche régionale.

1 projet sélectionné pour un budget de 156.650 €.

13) IFAPME et Creative District : Cybersecurity (La semaine de la Cybersécurité)

Le projet Cybersecurity vise à sensibiliser, former et accompagner les PME, TPE et indépendants pour renforcer leur cyber-résilience. Il adopte une approche globale en simplifiant les contenus, en privilégiant la proximité et en tenant compte des réalités du terrain. Le lancement de "La semaine de la Cybersécurité" garantira le succès des étapes ultérieures du projet en termes de sensibilisation. La formation se concentre sur des techniques rapidement applicables dans les activités des PME, ainsi que sur les initiatives existantes. Les ateliers thématiques seront gratuits. L'accompagnement comprend des séances de consultation avec un expert en cybersécurité.