SYNTHÈSE D'EXPÉRIMENTATION DU CYBERDIAG

EDEC Commerce
Axe 3
Fiche action 8

EDEC COMMERCE

LES 8 BRANCHES IMPLIQUÉES DANS CETTE ACTION SONT :

- Bricolage,
- Commerce à distance,
- Commerce à prédominance alimentaire (détail et gros),
- Commerce de détail de l'horlogerie-bijouterie,
- Commerce succursaliste de la chaussure,
- Import-Export,
- Optique-lunetterie de détail,
- Professionnels de la photographie.

Un accompagnement de proximité initié dans le cadre de l'EDEC Commerce

Le 3 octobre 2017, les treize branches professionnelles du Commerce et de la Distribution ont signé un EDEC (Engagement de Développement des Emplois et des Compétences) avec le Ministère du Travail et le Forco (devenu l'Opcommerce) en tant qu'organisme relais.

Au sein de l'axe 3 dédié à la cybersécurité, il y a 3 fiches action dont la fiche action 8 'Diagnostic accompagnement cybersécurité : Cyberdiag'. Celle-ci visait la conception d'un diagnostic pour évaluer l'organisation SI des entreprises et leur capacité à se protéger des cyber-attaques et un accompagnement dans le renforcement de leur cybersécurité.

L'objectif sous-jacent de ce 'Cyberdiag' est aussi de faire prendre conscience aux TPE/PME de l'importance de la cybersécurité, et de les accompagner dans la co-construction d'un plan d'actions qu'elles pourront mettre en œuvre. Un **cahier des charges validé par le COTECH** (COmité TECHnique composé de l'Etat, des 8 branches professionnelles impliquées sur cette fiche action et de l'Opcommerce), a permis de sélectionner un prestataire pouvant construire et mener à bien le projet sous forme d'expérimentation, et visant à produire une offre de service par l'Opcommerce pour le compte de ses entreprises adhérentes.

PRÉSENTATION DÉMARCHE CYBERDIAG

Le Cyberdiag doit permettre dans un premier temps, de faire un état des lieux de la sécurité informatique d'entreprises des 8 branches professionnelles impliquées et d'évaluer leur capacité à résister et à se prémunir des cyber-attaques ; puis à les accompagner à renforcer leur capacité de résistance. Cette expérimentation financée à 100% par l'Etat et l'Opcommerce n'a aucun coût pour les entreprises participantes.

UN PROJET EN 4 PHASES :

01 PHASE 1
Identification des pratiques cyber des TPE/PME à travers des entretiens et questionnaire en ligne.

02 PHASE 2
Construction d'un diagnostic orienté Commerce et Distribution.

03 PHASE 3
Expérimentation : test du diagnostic et évaluation de la satisfaction client.

04 PHASE 4
Restitution du rapport et de sa note de synthèse.

RECRUTEMENT DES ENTREPRISES :

Différentes sources :
- Les branches impliquées,
- L'Opcommerce,
- Le formulaire de contact du site internet dédié.

L'expérimentation a réuni un total de 26 entreprises participantes. 88% d'entre elles ont un effectif inférieur à 50 salariés, cible privilégiée de l'expérimentation.

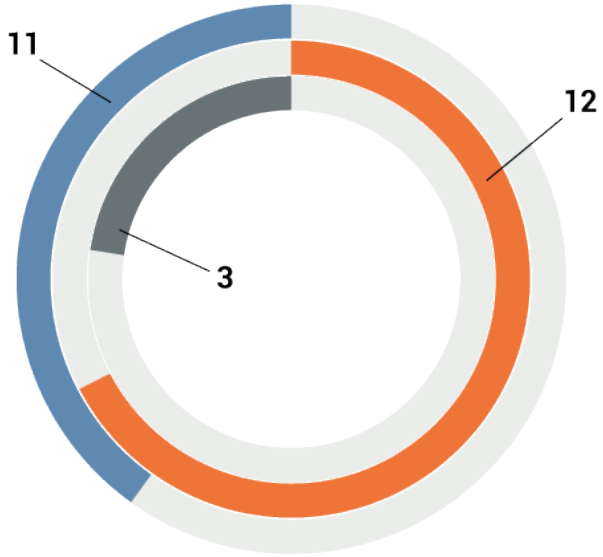
Création d'outils de communication :

- Un site internet **www.cyberdiag-tpe-pme.com** pour :
  - Communiquer sur l'expérimentation et expliquer la démarche,
  - Accèder aux ressources et aux outils de diagnostic de manière sécurisée (autodiag, tutos...).

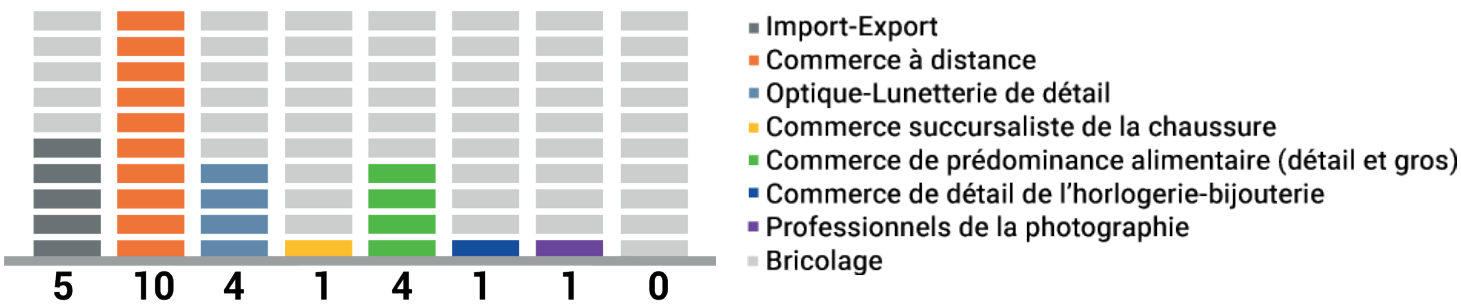
- Une vidéo

- Un triptyque

Nombre d'entreprises par taille

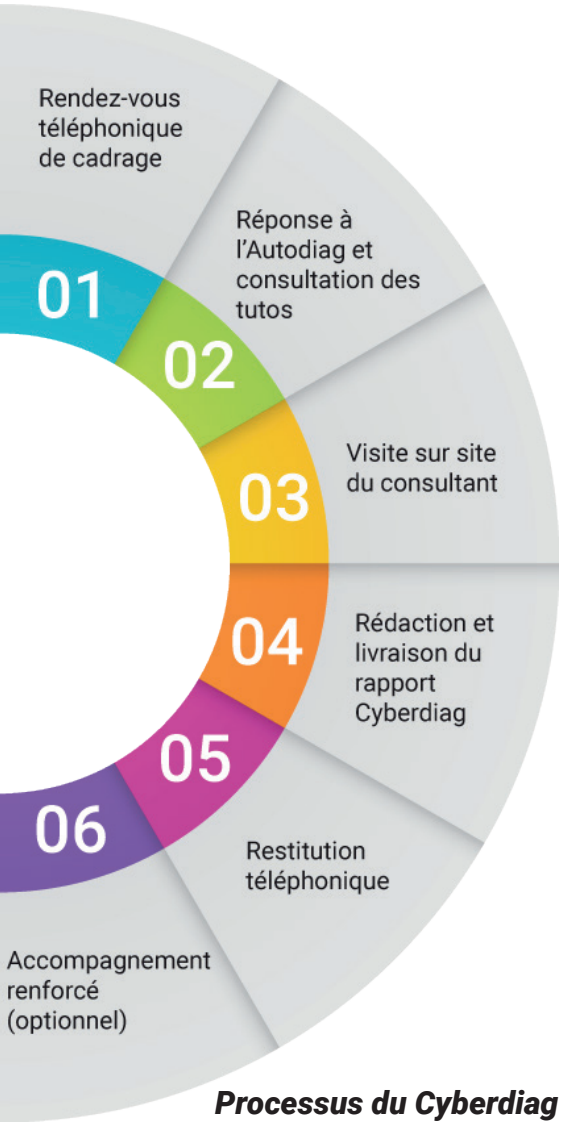


Sur un prévisionnel initial de 56 entreprises, ce sont 26 entreprises qui ont expérimenté le Cyberdiag.



Nombre d'entreprises par branche

PROCESSUS D'EXPÉRIMENTATION DU CYBERDIAG :



Processus du Cyberdiag

1. Rendez-vous téléphonique de cadrage : Un chef de projet prend contact avec l'entreprise candidate afin de valider la prestation au niveau technique et administratif.

2. Autodiag : Avant la visite sur site de l'expert en cybersécurité, l'entreprise participante est invitée à **compléter un questionnaire en ligne** sur le site dédié. Cet Autodiag permet au chef d'entreprise d'évaluer le niveau de maturité initial de sa structure en matière de SSI. Un scoring lui donne accès à des tutos lui permettant de répondre aux vulnérabilités les plus courantes des TPE/PME et de rehausser rapidement son niveau de sécurité.

3. Visite sur site : L'expert en cybersécurité se rend sur le site de l'entreprise et procède à des entretiens avec le dirigeant et le responsable informatique et/ou le prestataire informatique afin de recueillir toutes les informations nécessaires au diagnostic et à l'élaboration du rapport.

4. Rédaction et livraison du rapport : Suite à sa visite sur site, **l'expert rédige un rapport d'audit.** Celui-ci fait l'état des lieux de la sécurité informatique actuelle ainsi que des recommandations d'actions à mener pour l'améliorer. L'approche du rapport se veut pédagogique et tend à vulgariser les termes techniques afin d'être compréhensible et appropriable par l'interlocuteur quel que soit son niveau d'expertise.

5. Restitution téléphonique : L'expert et l'entreprise ont un entretien téléphonique pour échanger sur le rapport et répondre aux éventuelles interrogations. **Un plan d'action est défini** en prenant en compte les problématiques de l'entreprise pour mettre en œuvre les recommandations formulées par degré de criticité. A ce stade, l'entreprise peut choisir d'effectuer les préconisations seule ou choisir un accompagnement renforcé.

6. Accompagnement renforcé : l'entreprise ayant choisi cette option est soutenue par l'expert qui met en œuvre à ses côtés les actions prioritaires.

EVALUATION DE FIN D'EXPÉRIMENTATION :

- **100% des entreprises évaluées sont satisfaites du dispositif et le recommanderaient.**
- **90% des entreprises n'auraient pas expérimenté le cyberdiag sans une prise en charge financière intégrale.**

UNE EMPREINTE TPE/PME

L'analyse des problématiques cybersécurité des entreprises ne révèle pas une empreinte spécifique au Commerce et à la Distribution. Les usages, pratiques et risques sont assimilables à une spécificité TPE/PME en lien avec l'effectif de l'entreprise.

Les vulnérabilités les plus communément rencontrées sont partagées par toutes les branches. Elles sont le reflet de la maturité des TPE-PME en matière de SSI. Elles peuvent être, pour la plupart, corrigées sans un effort trop conséquent et ne demandent pas d'investissement ni même de compétences spécifiques.
Ce qu'il manque aux TPE/PME c'est une prise de conscience des risques liés au monde du numérique et du temps pour mettre en place certaines mesures de sécurité de manière uniforme.

POINTS FORTS DES ENTREPRISES

Une surface d'attaque restreinte due au faible nombre d'équipements informatiques :
Le nombre d'équipements présents au sein du parc informatique étant souvent réduit, la probabilité qu'une personne externe malveillante exploite une vulnérabilité sur l'un de ces équipements est plus faible.

Une tendance à déléguer l'infogérance du parc informatique à un tiers professionnel qualifié :
50% des TPE/PME externalisent l'infogérance de leur parc informatique. Cette délégation permet de garantir un certain niveau de sécurité et de réactivité en cas d'incident.

PRECONISATIONS

Il parait important que les TPE/PME acquièrent des réflexes les amenant à renforcer systématiquement leur cybersécurité, à savoir :

- Définir leur politique SSI en lien avec la stratégie de l'entreprise (objectifs, niveau d'exigence, priorités…),
- Evaluer leur niveau de maturité en cybersécurité au travers d'un diagnostic cybersécurité, permettant une prise de hauteur :
  - *Analyse de la situation et identification des carences,*
  - *Mise en place de mesures correctives,*
- Lancer des campagnes de sensibilisation/formation en direction des collaborateurs : la majorité des incidents de sécurité proviennent de l'exploitation de failles humaines. Un personnel formé est un moyen puissant de se prémunir face à des cyber-attaques,
- Accompagner financièrement les TPE/PME sur la cybersécurité en leur facilitant l'accès à des prestations de qualité afin de les encourager à se sécuriser et à s'investir dans le sujet.

PRINCIPALES VULNÉRABILITÉS

L'absence de politique de mots de passe robustes
Pour une majorité d'entreprises, aucune politique de mots de passe n'a été définie et les mots de passe utilisés sont rarement renouvelés. Ces mots de passe sont également réutilisés sur plusieurs applications. Le risque encouru est une intrusion sur le système d'information au travers d'une usurpation d'identité.

Le défaut de configuration des postes de travail et des droits d'administration
Des données sensibles sont stockées sur les disques durs internes des postes de travail mais ne sont pas chiffrées. De plus, les utilisateurs travaillent, pour la plupart, à partir d'un compte d'administrateur local de leurs postes. La limitation des droits des salariés sur les postes de travail, réduira fortement l'impact en cas d'attaque.

Un besoin de sensibilisation aux problématiques de cybersécurité
Les salariés sont très peu sensibilisés aux problématiques de cybersécurité et plus particulièrement aux attaques les plus répandues.
Ce manque de sensibilisation se traduit par de mauvaises pratiques informatiques qui réduisent drastiquement le niveau de sécurité global du SI. Un salarié vigilant et conscient des risques est le premier rempart contre les cyber-attaques.

La stratégie de sauvegarde
La sauvegarde des données de l'entreprise est un élément central. Pour autant, de nombreuses TPE/PME ont mis en œuvre une stratégie de sauvegarde qui n'est pas cohérente avec leurs besoins et objectifs stratégiques.

Un sentiment d'absence d'exposition aux risques
La prise en compte des enjeux de cybersécurité par les entreprises est inégale et dépend du secteur d'activité ainsi que du nombre de collaborateurs. Dans le contexte actuel où les cyber-attaques se multiplient, les TPE/PME sont très vulnérables aux attaques de masse. Un manque de conscience des risques qui s'explique par une charge de travail importante et des fonctions multitâches.

CHIFFRES CLÉS

15	26	26	22	18	10
Autodiag complétés	Diagnostics sur site	Rapports rédigés et livrés	Restitutions téléphoniques	Entreprises accompagnées	Evaluations complétées