Cette action bénéficie de l'expertise et du soutien financier du ministère du travail, dans le cadre de l'EDEC des branches du commerce et de la distribution

Complément au rapport d'expérimentation

Analyse spécifique branche Import-Export

EDEC Commerce 2017-2020

Axe 3 – Cybersécurité

Fiche Action 8 – Cyberdiag

Rapport rédigé par Phosforea en mai 2020

Sous la direction de la Direction Offre de Service et Innovation de l'Opcommerce

PREAMBULE

L'expérimentation Cyberdiag a été menée en 2019/2020 dans le cadre de l'EDEC Commerce porté par les branches du Commerce, le Ministère du Travail et l'Opcommerce en tant qu'organisme relais.

Il s'agissait de concevoir un diagnostic visant à évaluer l'organisation SI de l'entreprise et sa capacité à se protéger des cyber-attaques puis à l'accompagner dans le renforcement de sa cybersécurité.

Le rapport d'analyse de l'expérimentation du Cyberdiag, tenant compte des 8 branches professionnelles impliquées dans l'action, a été publié sous l'intitulé de ***'Rapport d'expérimentation du Cyberdiag'.***

Ce document est un complément au rapport, constituant une analyse spécifique dédiée à la branche professionnelle de l'Import-Export. Il vise à apporter un éclairage sur les chiffres et à faire un examen spécifique dédié. Il est important de noter que le nombre d'entreprises participantes ne permet pas de tirer des conclusions pour la branche au niveau national, mais ce document donne des indicateurs et des tendances en termes de pratiques en matière de cybersécurité.

Sur 8 branches impliquées dans l'expérimentation, la branche professionnelle de l'Import-Export est la 2ème branche la plus représentée dans l'utilisation du Cyberdiag, après le Commerce à distance.

SOMMAIRE

LEXIQUE

SI (Systèmes d'Information) : Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un ordinateur. *(Source : Wikipedia).*

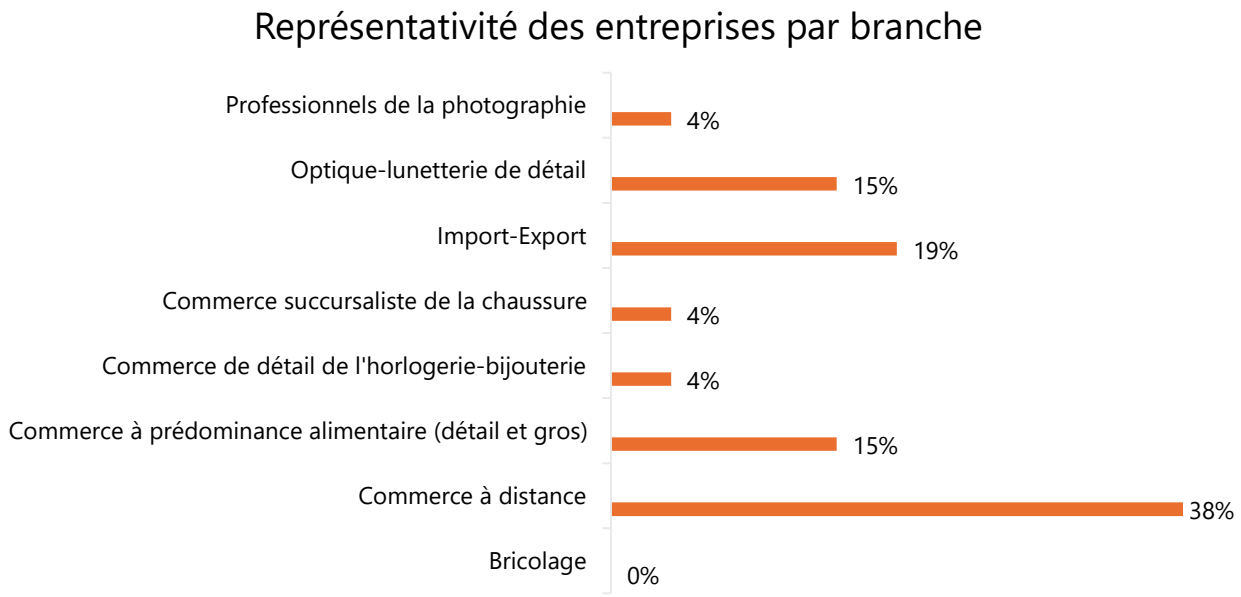
SSI : Sécurité des Systèmes d'Information.

1. Experimentation du Cyberdiag

Rappel du cadre de l'expérimentation

Dans le cadre du Cyberdiag, chaque branche professionnelle impliquée devait être équitablement représentée en nombre et en taille d'entreprises. Le COTECH a donc décidé que chacune des 8 branches, devait proposer 7 entreprises participantes à l'expérimentation, soit un total de 56 entreprises pour l'opération.

Ci-dessous le graphique des entreprises participantes par branche :



Sur une base de 26 entreprises ayant expérimenté le Cyberdiag, les branches professionnelles de l'Import-Export et du Commerce A distance et représentent à elles deux plus de la moitié (57%) des entreprises expérimentant le Cyberdiag.

1.1 Recrutement des entreprises

Spécificités de l'Import-Export – Entrée des entreprises

Pour la branche de l'Import-Export ce sont, au démarrage du projet, 11 entreprises intéressées par l'expérimentation du Cyberdiag :

BRANCHE IMPORT-EXPORT ENTREE DES 11 ENTREPRISES INTERESSES PAR LE CYBERDIAG	
Entrée Branche	
Import-Export	**1**
50/299	1
Entrée Site Internet	
Import-Export	**5**
11/49	3
50/299	2
Entrée l'Opcommerce	
Import-Export	**5**
-11	2
11/49	3
Total	**11**

Il est à noter que, suite à leur accord de principe initial, 6 entreprises sont finalement sorties du projet. Les raisons de ces désistements sont de plusieurs ordres :

- 2 entreprises dont le SI était géré en Europe (Pays-Bas et Royaume Unis) :
    - 1 moins de 11 salariés,
    - 1 de 50/299 salariés.
- 4 entreprises intéressées mais n'ayant pas répondu dans les temps :
    - 2 de 11/49 salariés,
    - 2 de 50/299 salariés.

En revanche, 5 entreprises ont été expérimentatrices du Cyberdiag. Ces entreprises ont eu divers canaux d'entrée :

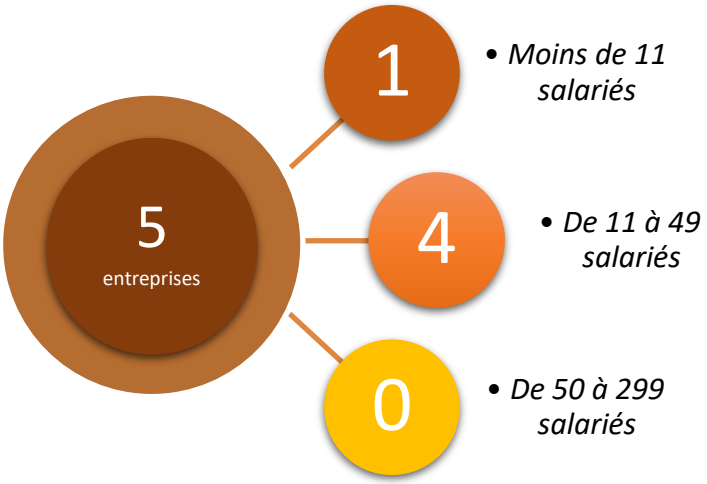
BRANCHE IMPORT-EXPORT 5 ENTREPRISES ENTREES DANS L'EXPERIMENTATION	
Entrée site internet dédié	
Import-Export	**1**
11/49	1
Entrée l'Opcommerce	
Import-Export	**4**
-11	1
11/49	3
Total	**5**

⇨ *Sur un prévisionnel initial de 7 entreprises par branche, pour la branche de l'Import-Export, ce sont au final 5 entreprises qui ont été expérimentatrices du Cyberdiag soit 71% du prévisionnel.*

Spécificités de l'Import-Export – Répartition des entreprises recrutées

Au regard de la figure suivante, il est constaté que le Cyberdiag a été utilisé à 100% par des entreprises de moins de 50 salariés dont à 80% par les entreprises de 11 à 49 salariés. L'objectif d'atteindre les TPE/PME donc été atteint.

Répartition des entreprises de la branche par tranche d'effectif



1.2 Autodiag et diagnostic/audit sur site

Rappel du cadre de l'expérimentation

Autodiag

Avant la visite sur site de l'expert en cybersécurité, les entreprises participantes sont invitées à compléter l'Autodiag. Il s'agit d'un questionnaire sécurité, disponible sur le site Internet dédié, www.cyberdiag-tpe-pme.com au travers de l'espace personnel de l'entreprise.

L'Autodiag permet au chef d'entreprise d'évaluer le niveau de maturité initial en matière de SSI de sa structure (obtention d'un scoring) et d'accéder à des tutoriels lui permettant une mise à niveau cybersécurité rapide.

L'Autodiag permet par ailleurs, au consultant de préparer sa venue sur site dans la perspective d'un diagnostic/audit de qualité.

Diagnostic/audit sur site

L'expert se rend sur le site de l'entreprise et, sur la base d'un référentiel unique construit sur les bonnes pratiques promues par l'ANSSI, il effectue le diagnostic/audit autour de 15 thématiques. Le niveau de maturité global de l'entreprise en matière de SSI se décline selon 3 niveaux : faible, moyen et satisfaisant. Naturellement, ce niveau est défini à partir de la moyenne des notes obtenues pour les 15 thématiques.

Spécificités de l'Import-Export

Concernant l'Autodiag, sur les 5 entreprises expérimentatrices :

- 3 entreprises ont complété l'Autodiag (1 moins de 11 salariés et 2 de 11/49 salariés),
- 2 entreprises ne l'ont pas complété (2 de 11/49 salariés)

Concernant le rapport de diagnostic/audit, les 5 entreprises expérimentatrices ont toutes réceptionné et lu le rapport et bénéficié de la restitution téléphonique.

1.3 Restitution du rapport et accompagnement

Rappel du cadre de l'expérimentation

Suite à sa visite sur site, l'expert rédige un rapport de diagnostic/audit de l'état des lieux de la sécurité informatique actuelle de l'entreprise. Ce rapport effectue des recommandations d'actions à mener pour améliorer sa cybersécurité.

L'approche pragmatique et pédagogique du rapport tend à vulgariser les termes techniques afin d'être compréhensible et appropriable par l'interlocuteur quel que soit son niveau d'expertise dans le domaine.

Le rapport et envoyé par mail chiffré à l'entreprise puis est débriefé au travers d'un entretien téléphonique avec la visée de 4 objectifs :

1. Présenter les conclusions du diagnostic/audit de manière détaillée et illustrée au travers du rapport,
2. Répondre aux éventuelles questions,
3. Présenter les recommandations et co-construire le plan d'action,
4. Définir l'accompagnement à mettre en place (optionnel). A ce stade, l'entreprise détermine les actions que le prestataire exécutera pour et/ou avec elle, ou si elle est en capacité de mettre en œuvre le plan d'action avec ses ressources internes et donc de ne pas souhaiter l'accompagnement.

Spécificités de l'Import-Export - Restitutions

Focus sur les 5 entreprises de la branche, participantes au Cyberdiag :

- Les 5 entreprises ont bénéficié de l'envoi chiffré et sécurisé du rapport de diagnostic/audit et de la restitution téléphonique ;
- Une entreprise a mis en place des actions préconisées par le consultant lors de son diagnostic/audit sur site, sans attendre l'envoi du rapport et la restitution téléphonique :
    - ➢ Ceci démontre non seulement une réelle proactivité de l'entreprise à l'issue du diagnostic/audit sur site, mais aussi un réel pragmatisme du plan d'action préconisé.

Spécificités de l'Import-Export – Accompagnement

Les 5 entreprises ont choisi l'option 'accompagnement'. Au total ce sont 20 jours d'accompagnement qui ont été effectués en direction des entreprises, répartis entre 2,5 et 5 jours par entreprise.

Révéler la nature des accompagnements choisis par les entreprises pourrait dévoiler leurs faiblesses aussi ces informations ne seront pas abordées en vue de préserver leur sécurité.

1.4 Evaluation

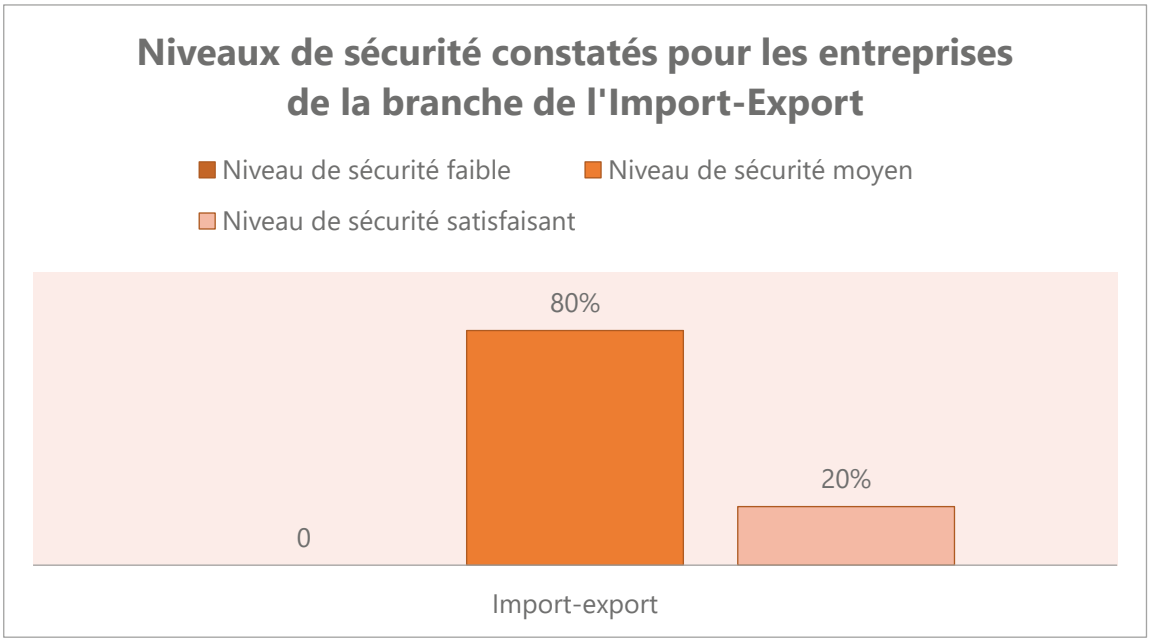
Une entreprise de moins de 11 salariés a répondu au questionnaire d'évaluation. Cette entreprise est « très satisfaite » de la prestation de l'auditeur sur site, de la qualité du rapport ainsi que celle de l'accompagnement. Elle recommanderait le Cyberdiag à une autre entreprise du commerce mais n'aurait pas participé si le projet n'avait pas été financé à 100%.

1.5 Quelques chiffres

2. RETOUR D'EXPERIENCES

L'Import-Export est une des branches où les entreprises sont les plus conscientes des enjeux de cybersécurité et des risques qui pèsent sur leur SI. **Dans ce secteur d'activité souvent concurrentiel, les risques liés au contexte international et aux déplacements sont bien pris en compte par les TPE/PME participantes**.

Sur les 5 entreprises accompagnées, 3 d'entre elles ont un contrat avec un prestataire qui leur permet de déléguer l'infogérance de leur parc informatique. Les 2 autres emploient des collaborateurs à temps plein qui possèdent des compétences informatiques et sont sensibilisés aux problématiques de cybersécurité. Cette prise en compte de la SSI systématique garantit à ces entreprises un niveau de sécurité moyen pour 80% d'entre elles, à satisfaisant pour 20% (figure ci-dessous).



Néanmoins, **les vulnérabilités les plus constatées au sein des entreprises de la branche Import-Export ne sont pas propres au secteur d'activité** puisque ce sont celles que l'on retrouve dans les autres branches, à savoir : la politique interne de mots de passe, la configuration des postes, la stratégie de sauvegarde...

Plus vertueusement, pour illustrer une somme de bonnes pratiques, nous prendrons pour exemple une entreprise ayant le niveau de sécurité le plus élevé évalué lors de l'expérimentation Cyberdiag et qui appartient à la branche Import-export.

Le niveau de maturité de cette entreprise en matière de SSI n'est pas seulement lié au secteur d'activité auquel elle appartient, sinon à son contexte. Cette entreprise possède des filiales à travers le monde entier (Etats-Unis, Chine, Afrique du Sud, etc.). Le SI de ces filiales est interconnecté en permanence au siège (en France) qui forme le nœud central du SI.

Ainsi, le référent informatique et sécurité en charge de l'infogérance de ce SI est une personne compétente qui a mis en place des mesures de sécurité cohérentes avec les objectifs stratégiques de l'entreprise.

Lorsque le référent informatique et sécurité n'est pas qualifié pour certaines tâches liées à l'administration du SI, il les délègue à des tiers professionnels qualifiés (ex : mise en place des règles du pare-feu). Même s'il délègue certaines prestations, il contrôle les actions réalisées par les prestataires et s'assure qu'ils respectent les clauses écrites dans leurs contrats.

La différence significative avec la majorité des autres TPE/PME est, qu'une personne de l'entreprise maîtrise complètement le SI, y compris le périmètre de prestations des fournisseurs de services.

Enfin, en cas d'absence de ce référent, il existe un second collaborateur capable de le remplacer dans ses fonctions. Il existe également une documentation relative au SI et les processus sont, pour la plupart formalisés et connus de tous les collaborateurs.

3. CONCLUSION

En conclusion, le niveau de maturité d'une entreprise en matière de SSI dépend certes de son secteur d'activité mais également du contexte dans lequel elle évolue.

Les conclusions du '***Rapport d'expérimentation du Cyberdiag'*** montrent qu'il n'y a pas de tendances spécifiques aux métiers du commerce et de la distribution mais un facteur « taille » propre aux TPE-PME.

En effet, celles-ci sont globalement moins conscientes des risques cyber et donc moins préparées face aux cybermenaces. Elles sont par ailleurs, globalement, plus fragiles financièrement que les grandes structures qui octroient des moyens financiers à la cybersécurité et sont de ce fait moins bien protégées.

En termes de préconisations, il parait important que les TPE/PME puissent avoir des réflexes visant à les amener à renforcer systématiquement leur cybersécurité, à savoir :

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

8 branches professionnelles du commerce impliquées dans le Cyberdiag :

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

Rapport rédigé dans le cadre de l'expérimentation du Cyberdiag

EDEC Commerce (2017-2020), Axe 3 – Cybersécurité

Par Phosforea - Mai 2020
paco.cervantes@phosforea.com - 07 60 10 83 83
https://www.phosforea.com/