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 Commerce à distance

EDEC Commerce 2017-2020

Axe 3 – Cybersécurité

Fiche Action 8 – Cyberdiag

Rapport rédigé par Phosforéa 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 du Commerce à distance (CAD). 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 du **Commerce à distance est la branche la plus représentée dans l'utilisation du Cyberdiag.**

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).*

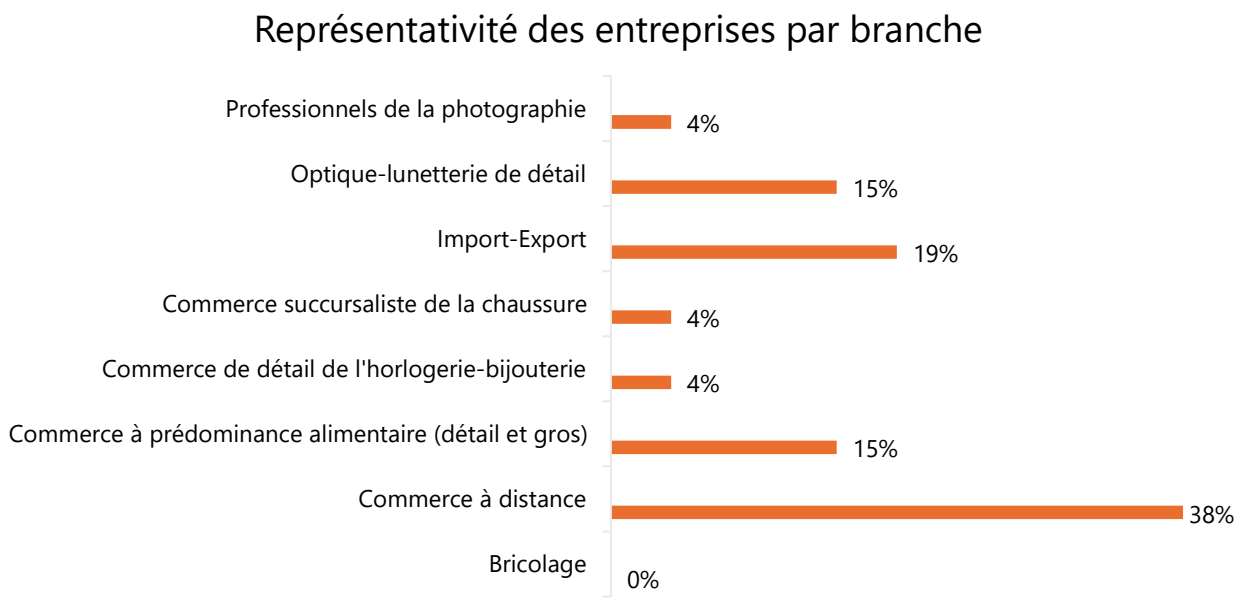
SSI : Sécurité des Systèmes d'Information.

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 du Commerce à distance et de l'Import-Export représentent à elles deux plus de la moitié (57%) des entreprises expérimentant le Cyberdiag. 10 entreprises du Commerce à distance ont pris part à l'expérimentation, soit 38% des entreprises participantes

1.1 Recrutement des entreprises

Spécificités du Commerce à distance – Entrée des entreprises

Pour la branche du Commerce à distance ce sont, au démarrage du projet, 10 entreprises intéressées par l'expérimentation du Cyberdiag :

Synthèse de 10 entreprises entrées dans le Cyberdiag	
ENTREE SITE INTERNET	
Commerce à distance	**1**
-11	1
ENTREE L'OPCOMMERCE	
Commerce à distance	**9**
-11	4
11/49	2
50/299	3
Total	**10**

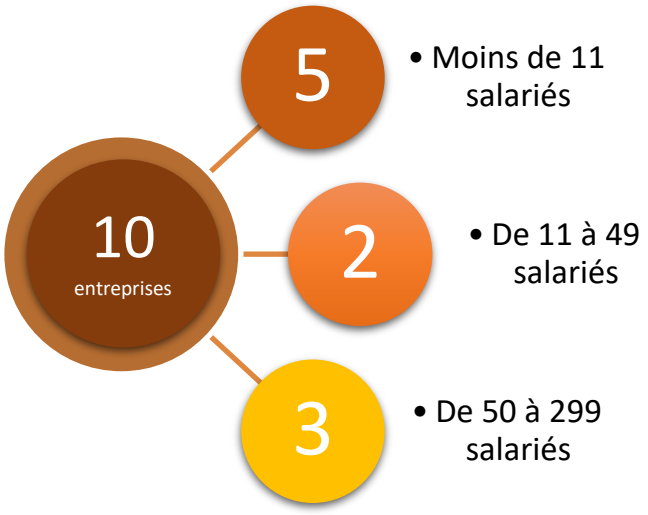
⇨ *Sur un prévisionnel initial de 7 entreprises, ce sont au final 10 entreprises de la branche qui ont été expérimentatrices du Cyberdiag.*

- *En effet, les entreprises du Commerce à distance, habituées de l'Internet et des réseaux sociaux, ont conscience des dangers liés à ces technologies aussi ont-elles été naturellement intéressées par le Cyberdiag.*

Spécificités du Commerce à distance – Répartition des entreprises recrutées

Au regard de la figure suivante, il est constaté que le Cyberdiag a été utilisé à 70% par des entreprises de moins de 50 salariés et à 50% par les entreprises de moins de 11 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 du Commerce à distance

Concernant l'Autodiag, sur les 10 entreprises expérimentatrices :

- 8 entreprises ont complété l'Autodiag (4 moins de 11 salariés et 2 de 11/49 salariés et 2 de 50/299 salariés),
- 2 entreprises ne l'ont pas complété (1 moins de 11 salariés et 1 de 50/299 salariés).

Concernant le rapport de diagnostic/audit, les 10 entreprises expérimentatrices l'ont réceptionné, lu et ont bénéficié de la restitution téléphonique.

1.3 Restitution téléphonique et plan d'action

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 est 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 du Commerce à distance - Restitutions

Focus sur les 10 entreprises de la branche, participantes au Cyberdiag :

- Les 10 entreprises ont bénéficié de l'envoi chiffré et sécurisé du rapport de diagnostic/audit et de la restitution téléphonique ;
- 3 entreprises ont mis en place des actions préconisées par le consultant lors de son diagnostic/audit sur site (restitution à chaud de fin de visite), sans attendre l'envoi du rapport et la restitution téléphonique :
    - Ceci démontre non seulement une réelle proactivité des entreprises à l'issue du diagnostic/audit sur site, mais aussi un réel pragmatisme du plan d'action préconisé.

Spécificités du Commerce à distance – Accompagnement

Sur les 10 entreprises, 8 ont choisi l'option '***accompagnement'***. 2 entreprises n'ont pas bénéficié de l'accompagnement car :

- Une entreprise de moins de 11 salariés allait déménager et avait les compétences en interne pour appliquer le plan d'action dans ses nouveaux locaux ;
- Une entreprise de moins de 11 salariés n'a pas pu bénéficier de l'accompagnement car la restitution s'est faite tardivement : restitution téléphonique effectuée en janvier 2020 ; mise en œuvre du plan d'action décalé à plusieurs reprises ; date de délai de réalisation du plan d'action dépassée ; clôture de l'expérimentation.

Au total ce sont 36,5 jours d'accompagnement qui ont été effectués en direction des 8 entreprises, répartis entre 2 et 10 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

Ce sont 6 entreprises de la branche qui ont répondu au questionnaire d'évaluation ce qui représente 60% des entreprises participantes mais également 60% des entreprises ayant répondu à l'évaluation sur l'ensemble de l'expérimentation. Voici ce qui ressort pour ces 6 entreprises :

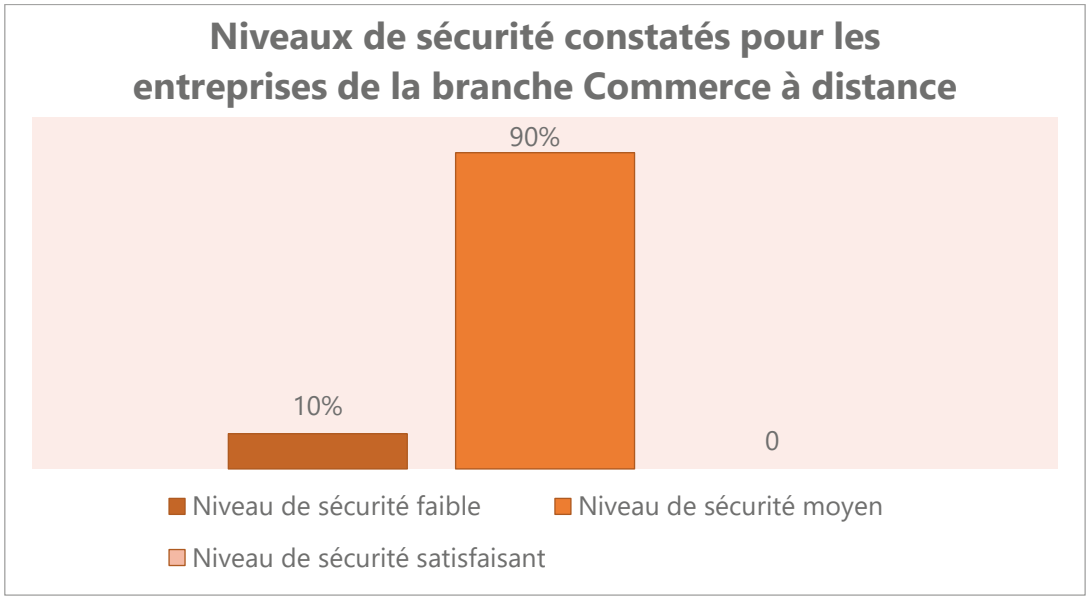
- 100% sont « très satisfaites » ou « plutôt satisfaites » par la qualité de l'intervention de l'auditeur sur site ainsi que par la qualité du rapport d'audit ;
- 5 entreprises n'auraient pas effectué le Cyberdiag s'il n'avait pas été financé à 100% ;
- 1 entreprise aurait effectué le Cyberdiag même s'il était payant ;
- 100% recommanderaient le Cyberdiag à une entreprise du commerce.

1.5 Le Cyberdiag en quelques chiffres

2. Retour d'experiences

Le Commerce à distance est une des branches où les entreprises sont le plus conscientes des enjeux de cybersécurité et des risques qui pèsent sur leur SI. C'est la branche où les entreprises mettent le plus en œuvre des mesures de sécurité pertinentes, bien que parfois incomplètes, pour diminuer les risques de cyberattaques. Ceci est certainement dû à **une plus grande dépendance aux outils numériques (site web vitrine ou marchand, outils logistiques en ligne, etc.).**

Sur 10 entreprises auditées, 90 % ont un niveau de sécurité moyen. 10 % ont un niveau de sécurité faible, mais cela ne représente qu'une entreprise sur 10 au total (graphique ci-dessous).



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

Pour l'entreprise dont le niveau de sécurité du SI est faible, cela s'explique par le fait que le dirigeant a une confiance totale en ses collaborateurs lorsqu'ils utilisent l'outil informatique. En effet, ces derniers ne sont pas à l'aise avec l'outil informatique et par conséquent, ils utilisent les postes de l'entreprise pour une utilisation basique et restreinte.

Le dirigeant pense donc qu'il ne peut pas y avoir de comportements à risque compte tenu des profils de ses salariés. Ainsi, il ne voit pas l'utilité de mettre en place des mesures de sécurité relatives aux postes, au réseau, etc. Pour autant, les collaborateurs ne sont pas moins exposés aux attaques actuelles (ex : cryptolocker) et sont particulièrement vulnérables puisqu'ils ne sont pas sensibilisés aux problématiques de cybersécurité.

Les entreprises du Commerce à distance se caractérisent par un élément qui occupe une place centrale dans leur SI : le site e-commerce. Sur les 10 entreprises accompagnées, 60% d'entre elles délèguent le développement et/ou l'infogérance de leur site Web à un prestataire. Bien que le site e-commerce des entreprises soit au cœur de leur stratégie, la prise en compte de la sécurité au niveau du site Web reste souvent partielle et très variable d'une entreprise à l'autre. Pour un tiers de ces entreprises, un prestataire a mis en place un pare-feu (appelé WAF : Web Application Firewall) pour protéger le site Web de diverses attaques. La sécurité s'arrête principalement à ce seul dispositif, qui est une première barrière pour contrer les attaques, mais qui ne devrait pas être la seule. Ces entreprises sont satisfaites de cette mesure SSI et ne contrôlent pas en amont, les pratiques de développement de leurs prestataires ni même la façon dont ils infogèrent le site Web. Elles ne se soucient pas, par exemple, de savoir si leurs prestataires effectuent une veille régulière des vulnérabilités afin de s'assurer que le site Web de l'entreprise n'est pas concerné.

50 % des entreprises ne savent pas si les prestataires prennent en compte la SSI quand ils infogèrent et/ou développent leur site Web. En général, les personnes interviewées lors de la visite de nos experts en cybersécurité sur leur site, affirment ne pas connaître le contenu du contrat qui les lie à leur prestataire, détaillant les clauses et le périmètre de la prestation. Dans ce cas de figure, les TPE/PME ont une grande confiance en leur prestataire et n'ont pas conscience de l'impact que pourrait avoir une attaque ciblant leur site Web.

Une seule entreprise a prestataire ayant intégré la SSI (au moins partiellement) dans l'infogérance de son site Web. Pour preuve, l'entreprise reçoit des rapports générés par des scans de vulnérabilités réguliers. Néanmoins, aucune personne au sein de l'entreprise n'a la compétence technique pour comprendre ce qui est décrit dans ces rapports.

Concernant les 4 entreprises qui développent et infogèrent leur site Web, toutes n'ont pas mis en œuvre les mêmes mesures de sécurité. Parmi elles, seule une entreprise a mis en place un WAF pour protéger son site Web. Idéalement, ce type de protection devrait être déployé pour chaque site Web car le WAF représente une barrière de sécurité importante.

Sur ces 4 entreprises : **1 entreprise dispose d'un site Web créé à partir d'un CMS** (Content Management System ou Système de gestion de contenu). Le CMS constitue un moteur de site Internet contenant de nombreuses fonctionnalités, notamment dans le cas du e-commerce, toutes les fonctionnalités liées à la vente en ligne. Ce type de solution permet de créer un site e-commerce à moindre coût sans avoir de connaissance particulière en développement Web. L'avantage de ce type de solution (ex : PrestaShop) est qu'elle est sécurisée et permet de se prémunir des attaques les plus courantes. Ainsi, la prise en compte de la SSI dépend peu de l'utilisateur qui n'a plus qu'à paramétrer le CMS. **3 entreprises n'ont pas créé leur site Web depuis un CMS** et n'intègrent pas la SSI dans le développement de leur site. Aucun de leur développeur n'a été formé au développement sécurisé (qui est pourtant primordial).

Cependant, même s'ils manquent de formation, il existe des guides comme « l'OWASP Top 10 » qui présente les 10 vulnérabilités les plus couramment rencontrées et explique comment les corriger.

Parmi ces 4 entreprises qui développent et infogèrent leur site Web en interne, seule la moitié d'entre elles a déjà effectué des tests d'intrusion ou des scans de vulnérabilité pour tester la résistance du site Web aux attaques d'un robot ou d'un attaquant plus expérimenté. Il convient de souligner que sur ces 2 entreprises, l'une lance un scanner de vulnérabilités toutes les semaines et l'autre effectue ce même type de scan tous les 3 mois. Pour cette dernière, le rapport généré à l'issue du scan est envoyé à la banque qui vérifie que le dispositif de paiement en ligne intégré au site Web est conforme à la norme PCI-DSS *(Payment Card Industry Data Security Standard)*. Cette norme vise à réduire la fraude en ligne.

Enfin, sur les 4 entreprises, 1 seule s'assure que les développeurs effectuent une veille régulière des vulnérabilités qui pourrait concerner le site Web. Cette veille est importante car elle permet d'appliquer des patches de sécurité en cas de faille avérée. Les attaquants sont particulièrement attentifs aux vulnérabilités qui sont publiées, il est donc impératif que les développeurs déploient des patches de sécurité rapidement.

La prise en compte de la SSI dans le développement/l'infogérance du site Web par les entreprises est partielle. Néanmoins, les entreprises qui délèguent cette mission à des prestataires leur font généralement confiance et ne contrôlent pas ou peu les actions que ceux-ci réalisent. Il est courant que ces prestataires ne prennent pas en compte la SSI dans leur prestation. Sans qu'elles en aient conscience, les entreprises qui sont concernées par ce cas de figure courent de grands risques. En effet, l'impact d'une attaque sur leur site Web pourrait se révéler conséquent (impact financier, image…).

En revanche, **les entreprises qui disposent de ressources internes pour développer/infogérer leur site Web semblent mieux protégées contre les attaques** mais un effort est à fournir pour que leurs développeurs soient formés au développement sécurisé et qu'ils prennent le temps d'effectuer une veille régulière des vulnérabilités.

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 faiblesses,
  - 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 sécuriser et 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/