AXE 3 : OUTILLER LES ENTREPRISES POUR LE DEVELOPPEMENT DE LA CYBERSECURITE ET FAIRE EVOLUER LES COMPETENCES

CONTEXTE

A noter que le préfixe **Cyber**, fait référence à toutes les techniques liées à la société du numérique et notamment à l'informatique et à l'internet.

Digitalisation des processus de l'entreprise : nouveaux risques…

Aujourd'hui, face aux dernières innovations technologiques et numériques, les entreprises ont un niveau de maturité différent.

Que l'on parle de SI *(Système d'Information)* en vase clos, d'adoption de plateforme collaborative, de mobilité, de télétravail, de l'impact du digital, etc. toutes les entreprises semblent conscientes des risques inhérents à des pratiques émergentes et malveillantes mais tardent à prendre les mesures de sécurité qui s'imposent.

Pour autant, des signaux forts sont apparus ces deux dernières années avec un nombre de cyberattaques en augmentation pour lesquelles l'Etat *(ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information)* souligne la nécessité de disposer d'une capacité de détection précoce et la mise en place d'une organisation à contrer les attaques les plus subtiles comme les plus massives.

Un risque majeur pour les entreprises

(Rapport du CLUSIF-Club de la Sécurité de l'Information Français 2016 – « Menaces informatiques et pratiques de sécurité en France »)

L'informatique est perçue comme stratégique mais pour beaucoup d'entreprises, la sécurité reste encore une histoire de mise en place de solutions techniques, onéreuses et rapidement dépassées…

Les freins principaux à la mise en place d'une **Politique de Sécurité de l'Information (PSI**), sont le manque de moyens budgétaires, les contraintes organisationnelles et le manque de personnel qualifié *(signe d'une continuelle difficulté à recruter dans le secteur de la SSI).*

Cependant, la prise de conscience progressive des risques à ne pas mettre en place de PSI est liée au fait que les TPE/PME sont souvent dépendantes de grands clients qui exercent une pression sur leurs fournisseurs quant à la maîtrise de la sécurité de l'information.

Le monde connecté d'aujourd'hui génère en permanence une multitude de données *(la 'data', ce nouvel 'or noir')* que les entreprises, professionnels et analystes du secteur, utilisent pour prendre des décisions, faire des projections, émettre des prévisions et plus encore *(la data nourrit la recherche sur l'Intelligence Artificielle qui en a en effet besoin pour développer de nouvelles compétences. On peut s'interroger sur une IA développée à partir d'une data compromise).* **Les attaques visant à compromettre l'intégrité des données d'une entreprise peuvent engendrer un arrêt total de son activité.**

Les malveillances et les incidents de sécurité ne faiblissent pas et vont crescendo ces dernières années : les vols de données peuvent avoir de lourdes conséquences car elles ont le pouvoir de faire tomber une entreprise, voire l'ensemble des entités qui y sont liées. Mais la plus grande menace pourrait venir des attaques qui passeront inaperçues pendant des années jusqu'à ce que leur potentiel de nuisance ne soit enfin révélé. **Le principal enjeu est donc la confiance.** La prise de décision se faisant au niveau des dirigeants d'entreprises, des investisseurs ou encore des consommateurs, elle sera biaisée s'ils ne peuvent se fier aux informations dont ils disposent.

Face à la menace de perdre des millions, voire leur réputation, le temps des politiques de sécurité 'parapluie' est globalement terminé. Les organisations se doivent d'évoluer pour atteindre un niveau de maturité suffisant en matière de SI. Il y va de leur survie, au regard des enjeux qu'elles portent et des données dont elles ont la responsabilité.

Pour illustrer…

Début 2014, l'opérateur téléphonique **Orange** a subi deux cyberattaques à deux mois d'intervalle. Celles-ci ayant pour conséquence le vol de près de 2 millions de données personnelles clients. Le risque étant l'utilisation de ces données pour tenter de faire du 'phishing' auprès des consommateurs *(envoi de messages personnalisés demandant à leurs victimes de donner leur mot de passe ou leur numéro de compte bancaire… en vue de s'en servir ou de créer des 'packs identitaires' pour les revendre à des personnes malveillantes sur le darknet).*

Juillet 2015, le site **Ashley Madison** est victime du vol de données personnelles clients *(noms, courriels, comptes, préférences…).* Celles-ci seront rendues publiques 1 mois plus tard. Cette attaque a eu des conséquences telles, que sont déplorées des démissions, des divorces, des batailles judiciaires liées aux conséquences de la fuite de données, des suicides…

Aux USA, plusieurs **hôpitaux** ont été des cibles de 'ransomwar'. Cette pratique consiste à s'infiltrer sur un système d'information *(généralement au travers d'emails frauduleux)* puis à en chiffrer tous les fichiers, et enfin à exiger une rançon contre une clé de déverrouillage. Les patients ont été rapidement transférés vers d'autres établissements alentours évitant ainsi des morts.

Ces exemples sont frappants tant il est vrai qu'une prise de conscience doit avoir lieu. Les cyberattaques se sont développées et la France n'est pas épargnée. En 2016, ce sont en effet, 24.000 cyberattaques qui ont été bloquées par les dispositifs nationaux selon Jean-Yves Le Drian, Ministre de La Défense dans un entretien au JDD du 08/01/2017.

Les cybermenaces impactent la confiance des clients des entreprises

(Etude cabinet Vanson Bourne pour FireEyes 05/2016 «Au-delà de l'aspect financier, le coût réel des violations de données»)

Selon une étude menée en mai 2016 par le cabinet indépendant Vanson Bourne pour FireEye auprès d'un panel représentatif de 5.500 consommateurs dont 1.000 en France, il apparaît que **la confiance des consommateurs a été affectée par les cyberattaques** ayant frappé un certain nombre de grandes entreprises dans le monde *(Outre les précédents exemples : Linkedin, PokemonGo, TV5Monde, United Airlines, Le journal Le Monde …).*

Les consommateurs sont plus méfiants et hésitent désormais à donner des informations personnelles :

- 66% d'entre eux s'attendent à être informés immédiatement en cas de violation de données et 91% dans les 24 heures ;
- 33% indiquent que les violations de données de grande envergure ont érodé l'image des entreprises dans leur ensemble ;
- 73% seraient prêts à tourner le dos à une entreprise dont le manque d'engagement des dirigeants sur les questions de sécurité serait en cause dans le vol de leurs données : la négligence est le premier motif de perte de confiance ;
- 60% d'entre eux engageraient des poursuites judiciaires contre l'entreprise victime en cas de vol et d'exploitation de leurs informations personnelles à des fins criminelles. Au-delà de la perte de clients, les conséquences pourraient être plus graves encore pour les entreprises : la réglementation européenne exige de révéler aux consommateurs de telles atteintes aux données personnelles, ouvrant donc la voie à des poursuites massives ;
- 70 % des consommateurs, suite aux cas récents de violations de données, déclarent qu'ils fourniront dorénavant moins d'informations personnelles aux entreprises ;
- 51% d'entre eux considèrent désormais la sécurité comme un facteur important, voire déterminant dans leur décision d'acte d'achat ;
- 48% seraient disposés à payer plus pour une meilleure sécurité de leurs données de la part du fournisseur.

Le coût d'une sécurité déficiente

Dans un monde interconnecté, hyper-connecté, les informations propres à l'entreprise et propres aux clients peuvent rapidement tomber dans les mains des pirates de la toile par le biais de moyens multiples : mails malveillants, phishing, ransomware, cyberespionnage… Par ailleurs, les attaques par déni de service, défiguration du site web portent atteinte visiblement à l'entreprise. Toutes ces armes menacent un actif devenu stratégique : **la Data**. Or les portes d'entrée pour l'atteindre se sont multipliées : wifi, mobiles, réseaux, cloud, objets connectés…

Selon le rapport annuel de Symantec d'avril 2016, portant sur les cybermenaces :

- 77% des cyberattaques visent les PME,
- 31% des PME ne prennent aucune mesure de sécurité proactive.

Comme on vient de le voir, s'exonérer d'une Politique de Sécurité de l'Information peut avoir sur l'entreprise des conséquences qui pourraient être dramatiques. De plus, la législation européenne s'est fortement renforcée invitant toutes les entreprises de l'UE à se mettre en ordre de marche pour l'échéance de mai 2018 sous peine d'être fortement sanctionnées.

Législation et protection des données

Le **GDPR** *(General Data Protection Regulation)* est le nouveau texte européen en matière de protection des données personnelles. Adopté par le Parlement européen le 14 avril 2016, ses dispositions seront applicables dans l'ensemble des 28 États membres à compter du 25 mai 2018. Il remplacera l'actuelle Directive sur la protection des données personnelles adoptée en 1995. De nombreuses formalités auprès de la CNIL *(Commission Nationale de l'Informatique et des Libertés)* vont ainsi disparaître mais en contrepartie, la responsabilité des organisations sera renforcée.

Le GDPR repose sur le droit fondamental inaliénable que constitue, pour chaque citoyen, la protection de sa vie privée et de ses données personnelles et impose de ce fait, des devoirs aux entreprises. Il renforce la responsabilité et la transparence.

A échéance de fin mai 2018, toute entreprise devra savoir, à tout moment, de quelles données elle dispose, leur localisation, l'objet de leur collecte et leur mode de gestion *(stockage, sécurisation, transfert, effacement).* De plus, elle devra être en capacité de savoir si leur intégrité a été compromise et dans tel cas, y remédier rapidement tout en notifiant l'évènement à la CNIL et à l'ANSSI.

Les sanctions au manquement du règlement peuvent aller jusqu'à 4% du chiffre d'affaires annuel mondial ou 20 millions d'euros. De plus, l'entreprise devra indemniser sans plafonnement, toute personne lésée matériellement ou moralement par un traitement non conforme de ses données.

Les différentes obligations du GDPR orientent l'entreprise vers deux approches :

- **Une approche cyber-sécurité** qui consiste à réduire les risques d'intrusion, d'attaques ou les effets de catastrophes naturelles ou causées par l'homme dans le cadre de l'utilisation des moyens informatiques et de communication ;
- **Une approche cyber-résiliente** qui consiste en la capacité à se préparer et à s'adapter à des conditions en perpétuelle évolution ainsi qu'à récupérer rapidement ses capacités suite à des attaques délibérées, des accidents, des catastrophes naturelles ou encore des incidents dans le cadre de l'utilisation de moyens informatiques et de communication (*Élaboration d'un plan de continuité d'activité…).*

Les entreprises conformes en mai 2018 bénéficieront d'une sécurité juridique et d'une avance concurrentielle qu'elles pourront mettre en avant auprès de leurs clients.

Perspectives et prospective

Aujourd'hui la question de l'entreprise n'est plus de savoir si elle sera attaquée mais plutôt, de savoir quand elle le sera.

Toute violation de données étant la résultante d'une faille humaine et/ou d'une faille dans la sécurité, il est essentiel dans ce cas, de déterminer avec précision quelles données ont été compromises et les mesures à prendre.

Le point de départ pour l'entreprise consisterait à :

- **savoir quelles sont les informations qu'il est important de protéger** et faire une estimation des coûts d'une compromission et des pertes associées, ce qui impose une **culture de la prévention et de la résilience** ;
- **sensibiliser/informer ses salariés** aux enjeux de sécurité, aux règles à respecter et aux bons comportements à adopter en matière de sécurité des systèmes d'information, à travers des actions de sensibilisation et de formation ;
- **se préparer à être en conformité avec le GDPR.**

Accompagner les branches du commerce et de la distribution

La prise de conscience des risques informatiques augmente au fur et à mesure que les attaques se développent et que la législation se renforce. Dans ce contexte insécure en cours de structuration, **les entreprises ont besoin d'être accompagnées au travers :**

- **d'un diagnostic/accompagnement 'Cyber-diag',** duquel pourra découler un plan d'action formation/compétences et/ou stratégique ;
- **d'un Kit de sensibilisation/formation des salariés aux pratiques digitales sécures, au travers d'un outil digital** *(appli mobile…) ;*
- **d'une cartographie des formations en cybersécurité.**

Fiche Action 8	DIAGNOSTIC ACCOMPAGNEMENT CYBERSECURITE : CYBERDIAG

OBJECTIFS	Les entreprises investissent dans des technologies et services de sécurité en pensant que ceux-ci la protégeront des cyberattaques, pour ensuite se rendre compte qu'elles sont malgré tout victimes d'intrusions. Un tel constat devrait les inciter à la réflexion et à une remise à plat de leur approche de la sécurité à la faveur du GDPR applicable au 28 mai 2018. Afin d'accompagner les entreprises dans cette démarche, proposer : - **Un Cyber-Diag :** Un cabinet spécialisé réalise un diagnostic de l'organisation SI *(inventaires des outils, identification des pratiques collaboratives et des circuits d'information).* ➢ **Effectue des préconisations :** ✓ Le consultant procède à la restitution du Cyberdiag et effectue des préconisations, ✓ Le consultant accompagne l'entreprise dans la construction d'un plan d'actions : Politique de Sécurité de l'Information et Protection des Données *(PSI/PDO)* en vue du GDPR.
CIBLE	Les branches professionnelles signataires de l'EDEC et plus précisément les 9 branches suivantes : - Bricolage - Commerce à prédominance alimentaire *(détail et gros)* - Commerce de détail de l'horlogerie-bijouterie - Commerce succursaliste de la chaussure - Commerce succursaliste de l'habillement - Grands magasins et Magasins populaires - Horlogerie commerce de gros - Import/Export - Optique-lunetterie de détail Les entreprises des moins de 300 salariés, des branches professionnelles signataires se positionnant sur la Fiche Action 8 de l'EDEC, **soit plus de 22.000 entreprises** *(22.360).*
DECLINAISON	**Etablir une Politique de Sécurité de l'Information et de Protection des Données** **Déterminer le niveau de protection à mettre en place :** - Spécificité du secteur d'activité, - Niveau de sophistication des menaces auxquelles l'entreprise est confrontée, - Désigner un Délégué à la Protection des données. **Cartographier le traitement des données, prioriser les actions à mener et gérer les risques :** - Identifier les données sensibles à sécuriser, - Déterminer les forces et les faiblesses du système de sécurité actuel, - Hiérarchiser les faiblesses, - Elaborer le plan d'action pour éliminer les faiblesses. **Etablir et animer la PSI/PDO ainsi qu'une conduite du changement sécurité :** - Organiser les processus internes.

	- Documenter la conformité pour pouvoir l'actualiser, la réexaminer.
PARTENAIRES	- DGEFP - ANSSI - CNIL
RESSOURCES	- Les branches professionnelles relevant du Forco et leurs entreprises adhérentes, - Mise en place de groupes de travail avec les partenaires *(DGEFP/Forco/Branches/ Prestataire…),* - Sélection d'un prestataire pour effectuer des **Cyberdiag** par Appel A Proposition pour mise en concurrence.
FINANCEMENT	- DGEFP - Forco
INDICATEURS DE RESULTATS	- Nombre de diagnostics effectué auprès des entreprises, - Nombre de formations découlant de ce diagnostic, - Les analyses et préconisations effectuées pourront venir alimenter la cartographie des formations en cybersécurité.

Fiche Action 9	INGENIERIE PEDAGOGIQUE INNOVANTE APPLI MOBILE DE SENSIBILISATION/FORMATION : CYBERKIT

OBJECTIFS	Les entreprises investissent dans des technologies et services de sécurité en pensant que ceux-ci la protégeront des cyberattaques, pour ensuite se rendre compte qu'elles sont malgré tout victimes d'intrusions. Les salariés sont la première source de défense de l'entreprise, sous réserve qu'ils signalent le moindre événement qui éveille leurs soupçons : la sensibilisation et la formation à la Sécurité Informatique sont des axes majeurs. Afin d'accompagner les entreprises dans la sensibilisation/formation de leurs salariés, leur proposer : - **Un Cyber-Kit** de sensibilisation/formation des salariés aux pratiques digitales sécures, au travers d'un outil digital : accompagnement des salariés des branches dans la montée en compétences sur la sécurité numérique Pour ce faire : - **Construire une ingénierie de formation pédagogique innovante et utilisable sur une application mobile.**
CIBLE	Les branches professionnelles signataires de l'EDEC et plus précisément les 8 branches suivantes : - Bricolage - Commerce à prédominance alimentaire *(détail et gros)* - Commerce de détail de l'horlogerie-bijouterie - Commerce succursaliste de la chaussure - Commerce succursaliste de l'habillement - Grands magasins et Magasins populaires - Horlogerie Commerce de gros - Import/Export Les entreprises des branches professionnelles signataires se positionnant sur la Fiche Action 9 de l'EDEC, **soit plus de 15.000 entreprises** *(15.096).*
DECLINAISON	**S'appuyer sur les bonnes pratiques de sécurité informatique pour faire monter en compétences les salariés grâce au micro/mobile learning** - S'appuyer sur un consultant choisi par AAP pour construire une ingénierie de formation utilisable au travers d'une appli mobile pour se former au quotidien et durablement, - Repérage de l'existant, des préconisations ANSSI, des spécificités commerce et distribution, - Produire une ingénierie de formation en séquences sur application mobile permettant d'avoir une boite à outils autoportante, d'ancrage du savoir pour retenir et appliquer des concepts clés de la cybersécurité, - Expérimenter par une approche innovante une pédagogie ludique et opérationnelle en s'appuyant sur les managers en entreprise pour promouvoir l'outil et proposer à leurs équipes de se former 10mn chaque jour !
PARTENAIRES	- DGEFP - ANSSI - CNIL - Expert pédagogie digitale et mobile
RESSOURCES	- Les branches professionnelles relevant du Forco et leurs entreprises adhérentes,

	- Mise en place de groupes de travail avec les partenaires *(DGEFP/Forco/Branches/ Prestataire…),* - Sélection d'un prestataire pour effectuer le CyberKit par Appel d'Offres pour mise en concurrence.
FINANCEMENT	- DGEFP - Observatoire Prospectif du Commerce
INDICATEURS DE RESULTATS	- Production Appli mobile pédagogique Cybersécurité - Utilisation Appli mobile avec marge de progression des savoirs intégrée

Fiche Action 10	CARTOGRAPHIE DES FORMATIONS EN CYBERSECURITE

OBJECTIFS	Alimenté par un groupe de travail composé de représentants de la formation professionnelle et/ou de la formation initiale et du Secteur du Commerce et de la Distribution, - Proposer une cartographie formations en cybersécurité et éventuellement identifier les formations manquantes. - Accompagner les salariés des entreprises des branches du Commerce et de la Distribution dans leur montée en compétences pour faire face aux évolutions technologiques, et à l'agilité des comportements des cyberattaquants.
CIBLE	Les branches professionnelles signataires de l'EDEC et plus précisément les 8 branches suivantes : - Bricolage - Commerce à prédominance alimentaire *(détail et gros)* - Commerce de détail de l'horlogerie-bijouterie - Commerce succursaliste de la chaussure - Commerce succursaliste de l'habillement - Grands magasins et Magasins populaires - Horlogerie Commerce de gros - Import/Export Les entreprises des branches professionnelles signataires se positionnant sur la Fiche Action 10 de l'EDEC, **soit plus de 15.000 entreprises** *(15.096).*
DECLINAISON	- Méthodologie du cabinet pour construire la cartographie
PARTENAIRES	- DGEFP - ANSSI - CLUSIF - CNIL…
RESSOURCES	- Les branches professionnelles, - Les entreprises, - Mise en place de groupes de travail avec les partenaires *(DGEFP/Forco/Branches/ Prestataire…).* - Sélection du prestataire de la cartographie, par Appel A Proposition pour mise en concurrence. - Utilisation des diagnostics et préconisations pour alimenter la cartographie *(sous réserve de confidentialité sur le nom des entreprises).*
FINANCEMENT	- DGEFP - Observatoire Prospectif du Commerce
INDICATEURS DE RESULTATS	**Production :** - Cartographie des formations en cybersécurité dans le secteur du Commerce et de la Distribution, - Production d'outils de communication vers les acteurs du secteur du Commerce et

	de la Distribution pour une appropriation de la cartographie, - Mise en place d'une méthodologie d'évolution de la cartographie.