la nouvelle revue du courtage
ÉDITION RÉGIONALE OCCITANIE

PLANETE CSCA OCCITANIE
#4
SEPTEMBRE 2021

La parole du Président

> *C'est dans ces moments que l'expertise et l'accompagnement des courtiers doivent se montrer les plus pointus.*

Chères adhérentes,
chers adhérents,

Au printemps, j'appelais de mes vœux le retour de nos échanges en présentiel, et c'est désormais chose faite ! Nous avons eu le plaisir de tenir une première réunion le 7 juillet dernier, à l'Holiday Inn Toulouse Airport, avec une trentaine de participants. Notre matinée a porté sur un thème cher à notre organisation professionnelle : la formation, avec la participation du représentant local de notre opérateur de compétences, l'OPCO ATLAS, Jérôme Penso. Emilie Amisse, Responsable Affaires sociales et Formation Professionnelle de PLANETE CSCA a décrypté les nouveautés en matière d'affaires sociales et Michel Accary, Directeur du Développement, s'est concentré sur une démonstration de la plateforme de formation digitale de PLANETE CSCA RH. Nous avons pu échanger à l'issue de la session entre pairs, et avec notre partenaire Aésio.

Le chemin de la reprise reste semé d'embûches, entre des secteurs économiques qui sont tirés par la demande, et d'autres qui anticipent une baisse durable de leurs activités, notamment l'aéronautique, fleuron de notre région. Nous devrons nous mobiliser pour trouver des solutions pour tous ces clients, dans un contexte incertain, où les pénuries de main d'œuvre ou de matières premières compliquent la tâche de chacun. C'est dans ces moments que l'expertise et l'accompagnement des courtiers doivent se montrer les plus pointus. Notre interview est d'ailleurs consacrée aux risques Cyber, avec une organisation de la Gendarmerie spécifique à notre région, et pilote pour lutter contre la Cybercriminalité. Merci à Laurent Leberon, Lieutenant-colonel Chargé de projets sécurité économique et protection des entreprises pour la région Occitanie, et à Karine Béguin Chef de la section appui judiciaire, pour leurs éclairages et leurs conseils.

Poursuivre nos temps d'échanges entre notre Comité Directeur et nos adhérents reste ma priorité, c'est pourquoi je vous propose de noter dès à présent la date du 14 octobre pour une prochaine réunion qui nous permettra de rassembler aussi nos partenaires assureurs.

À cette occasion, nous remettrons nos premières Étoiles du Courtage, des trophées qui récompensent les porteurs de risques de prédilection des courtiers. La matinée d'information sera consacrée à la digitalisation et aux outils à la disposition des cabinets de courtage. J'espère vous y voir nombreux !

Dans cette perspective, je vous souhaite une bonne rentrée, pleine de tonus pour aborder avec énergie une période de renouvellements qui s'annonce, cette année encore, synonyme de challenges !

Bien confraternellement.

David Verkinder
Président PLANETE CSCA Occitanie

PAROLE D'EXPERTS

La gendarmerie : bras armé de lutte anti Cyber criminalité

Laurent Leberon est Chargé de projets sécurité économique et protection des entreprises pour la Région de Gendarmerie d'Occitanie et **Karine Béguin**, Chef de la section d'appui judiciaire RGO. Tous deux basés à Toulouse, ils expriment leur engagement au service de la sensibilisation et de la prévention en matière de Cyber sécurité.

[La Nouvelle Revue du Courtage / LNRC] **Quelle serait votre appréciation de l'état de la menace ?**

[***Karine Béguin***] Avant d'exercer à Toulouse, j'ai œuvré durant 20 ans dans la lutte contre la Cyber criminalité au sein du Centre de Lutte contre la Criminalité à Pontoise. Depuis 2013, le phénomène le plus prégnant reste celui du *ransomware*. Après avoir concerné des particuliers, qui naviguaient sur des sites mal protégés, ou n'étaient pas équipés d'antivirus, ces attaques se sont progressivement dirigées vers des cibles plus importantes. Pour des particuliers, les rançons demandées avoisinaient les 200 à 300 €, en cartes prépayées permettant de faire des achats sur internet. Les pirates s'en sont pris ensuite à des PME/PMI de moins de 50 salariés, souvent sans DSI. La criminalité s'est ainsi structurée, acquérant des moyens financiers et techniques pour recruter des techniciens capables de développer des outils pour détourner les systèmes d'information des entreprises. Même les grandes entreprises peuvent être victimes d'attaques, les rançons étant aujourd'hui plutôt exigées en crypto-actifs, par exemple en bitcoins.

[***Laurent Leberon***] Les entreprises ne sont pas ciblées au hasard. Elles ont d'une part des obligations légales de publier certaines informations (comptes annuels) et d'autre part communiquent volontairement sur leur entité (site de l'entreprise, organigramme détaillé en ligne). Les hackers ont ainsi accès en *open source* à une importante quantité des données sensibles. Les dirigeants partent du principe que leur système d'information est robuste. En l'absence de sinistre, ils font souvent l'impasse sur des dispositifs prédictifs. Mais l'évolution rapide dans la transition numérique rend les circuits existants rapidement obsolètes. Les hackers ont pris conscience de cette posture et ils utilisent toutes les failles dans les différentes mises à jour des systèmes.

[***Karine Béguin***] Le SI d'une entreprise fonctionne comme son poumon : il comporte les données comptables, les données clients, celles qui concernent les salariés et enfin les informations sur la fabrication de ses produits (ou de ses services). S'il est coupé, l'entreprise ne peut plus répondre à la demande, entretenir des relations avec ses clients… Chaque heure de suspension de son activité coûte à l'entreprise énormément d'argent.

[***Laurent Leberon***] J'irais au-delà de la métaphore de Karine : la donnée, c'est le sang de l'entreprise. Protéger les données est une nécessité. La DATA est à la fois l'objet et le mobile du crime. Or aujourd'hui, les sphères personnelle et professionnelle sont devenues poreuses. On utilise parfois ses outils professionnels pour un usage personnel, et inversement. Cela développe des fragilités que des personnes malveillantes savent exploiter. Les usages numériques tendent à demander une réponse à n'importe quel moment, y compris quand les personnes ne sont pas vigilantes.

[***Karine Béguin***] Aujourd'hui, on parle beaucoup de cyber criminalité, mais en vérité, le chiffre qui fait foi est celui de la délinquance, le recensement des faits qui sont portés à notre connaissance. Ces chiffres ne reflètent pas l'état réel de la menace : nous

sommes face à un « chiffre gris » de la cyber criminalité. L'analyse incomplète du phénomène ne permet donc pas d'évoluer au même rythme que la criminalité qui, elle, déploie des moyens considérables. Néanmoins nous nous félicitons des dispositifs de prévention et d'information que sont l'ANSSI et Cyber'Occ[1].

Dans les faits, il faut distinguer deux situations :

- soit les infractions sont dirigées contre le SI lui-même en vue de bloquer celui-ci et d'arrêter l'activité de l'entreprise, c'est le cas des *ransomware* ;
- soit les infractions sont commises au moyen des nouvelles technologies de l'information et de la communication. La fraude au président ou l'escroquerie au changement de RIB en sont des exemples.

Un SI est un système socio-technique. La cyber criminalité vise à altérer le bon fonctionnement ou bloquer les systèmes d'information, ce qui rend le sujet particulièrement grave pour les organisations.

Par ailleurs, dans certains territoires moins développés économiquement, ce genre d'atteinte revêt une sensibilité particulière. Un employeur d'importance moyenne ne peut se permettre de laisser ses collaborateurs sans activité car, dans ce cas, il paralyse un territoire.

[LNRC] Quelles sont vos priorités ?

[***Laurent Leberon***] Nous poursuivons deux objectifs principaux : participer à la réduction des vulnérabilités et développer une culture de sécurité. Pour cela, nous travaillons autour de trois axes :

- Le préventif : nous intervenons en présentiel ou distanciel auprès des chambres consulaires, des organismes paritaires, des ordres, des clubs d'entreprises qui nous sollicitent, partout dans les 13 départements que nous couvrons ;
- Le défensif : nous recueillons des renseignements pour anticiper au mieux les phénomènes naissants ;
- Le judiciaire : quand un chef d'entreprise vient déposer plainte, nous devons agir avec efficacité et rapidité pour faire face à la menace.

[***Karine Béguin***] Nous souhaitons aussi faire comprendre aux entreprises attaquées qu'elles doivent porter les faits à notre connaissance. Quand une entreprise est la cible des pirates, elle peut avoir peur des conséquences sur son image. Craignant que les clients ne se détournent d'elle pour aller à la concurrence, elle peut renoncer à déposer plainte en espérant réduire le préjudice réputationnel. Son réflexe serait plutôt de régler le conflit à bas bruit, par exemple payer la rançon et vite, pour reprendre une activité classique. Or rien ne lui garantit que les données lui seront restituées dans leur intégralité et dans toute leur intégrité. Par ailleurs, ça ne garantit en rien l'entreprise qu'une nouvelle attaque similaire ou différente ne sera pas perpétrée contre elle à plus ou moins longue échéance. Si ça a marché une fois, pourquoi ne pas recommencer ?

[LNRC] Comment prévenir le risque ?

[***Laurent Leberon***] Dans une Cyber attaque, on peut recenser trois risques majeurs, qu'il ne faut pas sous-estimer :

- Le risque économique : vol de données, de savoir-faire, pertes d'exploitations, coût de reprise de l'activité ;
- Le risque réputationnel ;
- Le risque juridique : le chef d'entreprise est responsable pénalement et civilement.

[***Karine Béguin***] Une fois que les pirates ont trouvé l'accès à votre système d'information, rien ne vous garantit que la clé de déchiffrement qu'ils vous envoient après paiement de la rançon ne sera pas accompagnée d'un virus espion, pas nécessairement actif, mais permettant d'accéder de nouveau aux données.

Nous conseillons de ne pas payer la rançon et de déposer plainte, ce qui n'enclenche aucune « machine administrative » vis-à-vis du plaignant, les dirigeants d'entreprise peuvent se rassurer sur ce point.

Le dépôt de plainte nous permet de recouper l'attaque avec d'autres faits jusqu'à parvenir à identifier de manière formelle un individu. De nombreuses compagnies d'assurances exigent d'ailleurs que les dirigeants effectuent cette démarche avant toute indemnisation.

[***Laurent Leberon***] En amont, nous jugeons indispensable les actions de prévention. Les entrepreneurs doivent considérer les sécurités (physiques et numériques) comme des investissements et non comme des coûts.

Tout ce qui a trait au numérique est à la fois hybride et clivant :

- hybride car ces sujets engagent la responsabilité du dirigeant, mais ils se situent pour les salariés à la limite des sphères personnelle et professionnelle. Faut-il les laisser s'exprimer librement sur les réseaux sociaux sur ce qui se passe dans l'entreprise ?
- clivant parce qu'ils opposent les générations mais aussi les pro et les résistants au changement. Or le télétravail à marche forcée a nécessité d'adopter des comportements en urgence, rarement anticipés, peu ou pas préparés, ce qui a eu pour conséquence de multiplier les fragilités.

La gendarmerie s'inscrit dans la profondeur des territoires ; elle a toute légitimité pour agir en protégeant le fort tissu de TPE/PME qui sont implantées dans son périmètre d'action. De façon générale, la Gendarmerie base son action sur les principes de subsidiarité et complémentarité. En matière de lutte contre la cyber criminalité, nous avons une approche globale et structurée partout en France, avec des échelons territoriaux interfacés avec d'une part des compétences régionales et d'autre part une expertise nationale. Cette pyramide opérationnelle permet un partage d'informations rapide qui facilite le travail des enquêteurs.

[***Karine Béguin***] Il en est de même en matière judiciaire, avec une section spécifiquement créée au Tribunal Judiciaire de Paris (section J3), dédiée à la Cyber criminalité. Si une victime est identifiée à Toulouse, le référent Cyber régional recevra des notes de cette section, avec des protocoles de traitement et des instructions. Mais le TJ de Paris peut aussi faire jouer son droit de récupérer le dossier s'il dispose d'éléments en lien avec d'autres faits. Face à une menace élevée, nous sommes prêts à agir.

[LNRC] La crise sanitaire a-t-elle entraîné un nombre plus important d'attaques ?

[***Karine Béguin***] La hausse du nombre de plaintes au niveau national n'est pas significative, mais nous notons un développement des attaques par prise de contrôle à distance. Les entreprises ont dû réagir rapidement pour ouvrir des accès à leurs serveurs. Les hackers savent scanner les ports et en testant des mots de passe triviaux comme 1234/admin/admin ou 0000, cela peut donner des résultats. Les règles basiques de la sécurité informatique ont été bafouées devant l'urgence de la situation.

[***Laurent Leberon***] Les vols de données peuvent passer inaperçus et nous n'avons pas assez de recul pour observer si les intrusions ou les extractions de données ont augmenté. Il faut en moyenne 197 jours pour détecter une intrusion et 69 jours pour y remédier, soit près de 9 mois en tout !

[LNRC] En quoi votre organisation en région Occitanie est-elle originale ?

[***Laurent Leberon***] Le Général commandant la Région de Gendarmerie d'Occitanie a validé la mise en place d'un dispositif « pilote », reposant sur:

- La création d'un poste de chargé de projets Sécurité Economique et Protection des Entreprises ;
- L'étroite collaboration avec les enquêteurs de la Section d'Appui Judiciaire, les enquêteurs Nouvelles technologies ou délinquance financière, les référents sécurité économique ou sûreté ;

[1] Dans le cadre des travaux de la Stratégie Régionale de l'Innovation (SRI), la Région Occitanie a confié à l'agence de développement économique d'Occitanie, AD'OCC, la création du Centre Régional Cyber sécurité Cyber'Occ.

- Les réservistes, experts dans leur domaine, qui peuvent agir en prévention ou comme des vigies pour partager des informations en lien avec notre périmètre géographique,
- Les membres de la Réserve Cyber Citoyenne (RCC).

Nous pouvons réaliser gracieusement des diagnostics de vulnérabilité, avec des questionnaires fermés sur différentes familles d'atteintes, des consultations sûreté, ce qui rentre parfaitement dans notre mission de sensibilisation. La RCC est en mesure de procéder à des analyses de la maturité du système d'information. Ces actions visent à élever le niveau de conscience des acteurs économiques, prioriser leurs actions de protection et donc se faire accompagner par des professionnels : les cabinets d'audit, les entreprises de Cyber sécurité ou les DPO qui agissent sur le respect du RGPD.

Aujourd'hui, nous sommes conscients que notre ambition doit être mesurée face à ce dispositif naissant : ses résultats devront être mesurés dans le temps. Nous sommes en train de construire avec humilité. En termes de prévention, notre ambition se résume à une formule : « peu mais mieux ». La région Occitanie est vaste et dynamique. Elle compte deux métropoles majeures (Toulouse 3e ville de France et Montpellier 7e ville de France). Toulouse est la deuxième ville universitaire de France. Un grand donneur d'ordre et autant de matière grise aiguisent les convoitises.

Propos recueillis par Céline Meslier

Bonnes pratiques : ce qu'il faut retenir

Les bonnes pratiques relèvent du bon sens et passent par des gestes simples : il ne s'agit pas que de technologie mais avant tout de responsabilité et de processus.

RÈGLE 1 : S'intéresser au sujet avant que les Cyber criminels ne s'intéressent à vous !
Cartographier les risques et les menaces est un acte fondateur pour comprendre ses vulnérabilités et y remédier.

RÈGLE 2 : Limiter son exposition aux risques !
Éviter de communiquer trop précisément son organigramme, son organisation interne.
Il est obligatoire de déposer ses comptes annuels, en revanche il existe des exceptions à la publication de ces derniers. Renseignez-vous !

RÈGLE 3 : Mettre en place des procédures !
Pour prévenir la fraude au président, instaurer un process de vérification des ordres : pratiquer le contre appel.
Si les dirigeants ou cadres commerciaux voyagent, veiller à ce qu'ils n'emportent pas à l'autre bout du monde la totalité des données de l'entreprise : voyager uniquement avec ce que l'on accepte de perdre.

RÈGLE 4 : Entretenir des relations de proximité avec la Gendarmerie.
Connaître son premier allié en cas de crise : Se présenter à la brigade permet de gagner du temps et d'agir vite en cas de sinistre : des moyens d'action existent mais la plus grande réactivité est de mise.

Agenda

14 OCTOBRE 2021
Réunion trimestrielle thématique

LES ÉTOILES DE PLANETE CSCA

Votre Comité directeur a le plaisir de vous convier à sa prochaine réunion trimestrielle thématique le 14 octobre 2021 de 9h à 14h30, dans les environs de Toulouse (lieu à confirmer).

Au programme, une matinée d'échanges sur l'avenir des activités du courtage réservée aux adhérents, suivie de la remise des Étoiles du courtage pour la région Occitanie et de notre traditionnel cocktail annuel avec les partenaires compagnies.

Nous comptons sur votre présence, dans le strict respect des règles sanitaires en vigueur à la date de l'évènement !

Plus d'informations et inscriptions à venir, consultez notre site internet :

bit.ly/37bogbw

Visitez le mini site du Collège Occitanie - Syndicat PLANETE CSCA
www.planetecsca.fr/syndicat/college-occitanie