Lettre d'information économique

Sommaire

Octobre 2019

Editorial

La DRSD en soutien des PME-ETI

Le ministère des Armées a lancé, il y a un peu plus d'un an, un plan rénové de soutien aux PME-ETI auquel concourt spécifiquement la DRSD sur le volet protection-sécurité en attirant leur attention sur les menaces - en particulier cyber - auxquelles ces entreprises sont confrontées.

La DRSD s'est pleinement engagée à travers des opérations de sensibilisation spécifiques, soit seule soit au sein d'évènements organisés plus largement par la Délégation Générale de l'Armement (DGA).

Les retours positifs nous encouragent à poursuivre cet effort et à le renforcer pour toucher le plus grand nombre d'entre vous et vous permettre de prendre les mesures de protection, souvent basiques, pour éviter de mettre en péril vos informations ou savoir-faire stratégiques.

L'exemple du Cluster Primus Défense & Sécurité illustre l'effet démultiplicateur d'une union des compétences et de l'efficacité d'une coopération bien comprise public-privé, que montre également le bilan du salon du Bourget.

Les menaces sont de tout ordre, normatifs comme la norme américaine ITAR, d'autant plus redoutable en raison de ses effets rétroactifs possibles, ou plus simples mais toujours efficaces par le biais de ce que l'on appelle les intrusions consenties à l'instar, par exemple, des visites de délégations étrangères. Face à ces menaces, pas toujours évitables, la pertinence d'un plan de continuité et de reprise d'activité est mise en évidence à travers la norme ISO 22301.

Bonne lecture !

Le général de corps d'armée Eric Bucquet
directeur du renseignement et de la sécurité de la défense

ACTION PME en région

La DRSD engagée aux côtés des PME-ETI

L'instruction ministérielle n° 5871 du 3 septembre 2018 relative au Plan ACTION PME du ministère des Armées fixe à la Direction du Renseignement et de la Sécurité de la Défense (DRSD) la mission de mener des actions de sensibilisation au profit des Petites et Moyennes Entreprises (PME) et des Entreprises de Taille Intermédiaire (ETI) stratégiques du secteur de la défense, dans les domaines de la sécurité économique et de la cybersécurité.

Dans ce contexte réglementaire, la Direction zonale du renseignement et de la sécurité de la défense en zone Nord-Est (DZ NE) a organisé, le 23 mai 2019, une conférence sur les enjeux de la sécurité économique, y compris dans le domaine de la cyberdéfense.

Cette sensibilisation a réuni, à Lille, un tiers des PME et ETI sollicitées sur le territoire de la zone de défense Nord (Hauts-de-France). Les dirigeants et les officiers de sécurité (OS) des entreprises se sont montrés particulièrement attentifs et intéressés par les interventions des différents experts en contre-ingérence économique et cyber de la DRSD.

En outre, la démonstration de cyberattaques grâce à une plateforme technique "CENTAURE" réalisée par la section zonale de contre-ingérence cyber a permis de répondre aux préoccupations majeures actuelles des entreprises concernant les cyberattaques et leurs conséquences. Les experts cyber de la direction zonale, par leurs conseils avisés, ont délivré les recommandations nécessaires pour y faire face. Les discussions ont permis d'offrir des pistes de réflexion à l'auditoire pour trouver au sein de leur organisation respective les moyens de s'en prémunir.

Ces rencontres donnant lieu à des échanges entre la DZ NE et les PME et ETI stratégiques sont unanimement appréciées. Elles permettent à ces entreprises focalisées, à juste titre, sur leur développement économique de prendre conscience de leurs vulnérabilités et notamment celles liées à leur personnel.

Cluster Primus

Quand l'union fait la force !

Dans un contexte globalisé qui évolue rapidement, et face à la pression d'une concurrence toujours plus incisive, la compétitivité économique d'un pays ou d'une région dépend de plus en plus de réseaux d'affaires et d'innovations efficaces.
Certains acteurs économiques ont pris conscience que, pour faire face à une concurrence exacerbée, les entreprises, notamment les ETI et PME, doivent développer leur compétitivité et entretenir un système relationnel fortement ancré sur leur territoire afin d'augmenter durablement leurs opportunités d'affaires et de croissance.
Le Cluster Primus Défense & Sécurité, créé en 2013 sous l'impulsion de son président, Gilles Laborde, en région Midi-Pyrénées, en est la représentation. Avec plus 40 membres, l'objectif est de fédérer les entreprises du territoire, de générer une dynamique de complémentarité des compétences et de créer des synergies concrètes de développement sur des marchés à forts potentiels.

Un entretien avec Gilles Laborde, par ailleurs président de Cegelec Défense, met en lumière une dynamique forte de développement entre les PME et ETI pour favoriser interactivité et coopération avec tous les acteurs privés et publics de l'environnement territorial.

Qu'est ce qui en a motivé la création ?

« *La naissance de ce cluster résulte de la volonté de quelques dirigeants de PME d'unir leurs forces pour développer des opportunités de marchés tant sur notre territoire qu'à l'international. Une envie commune de fédérer les savoir-faire, les ressources et les technologies afin d'adresser des clients toujours plus exigeants, en recherche de produits innovants. Le maître mot du cluster Primus réside dans l'efficacité économique et l'augmentation du chiffre d'affaires des partenaires. Par ailleurs, la particularité du cluster est de sélectionner ses membres avec une approche qualitative, ceci reposant sur la nécessité de ne générer aucune concurrence entre membres mais justement des complémentarités business grâce au maintien d'un dialogue constant. S'il émerge un compétiteur, celui-ci devient le client d'un autre membre.* »

Comment devient-on membre du cluster ; avez-vous des exigences particulières ?

« *La manifestation d'intérêts doit résulter d'une réelle motivation à partager les mêmes valeurs.*

Nous veillons à ce que la motivation du nouvel entrant soit réelle et repose sur les quatre objectifs que nous nous fixons :

- *chasser en meute, car l'union fait la force ;*
- *diminuer les coûts ;*
- *développer et entretenir un réseau d'affaires permettant des collaborations concrètes ;*
- *permettre à l'ensemble des membres d'être présents sur les salons.* »

.../...

Cluster Primus

Pouvez-vous préciser les opportunités, les avantages pour les entreprises du cluster ?

« *Afin de répondre aux attentes de chacun, nous organisons des rencontres thématiques sélectionnées en fonction des attendus réels et concrets des membres. L'approche collaborative, fondement même du cluster, a permis, par exemple, de sélectionner des pays d'intérêts pour certains de nos membres comme le Maroc et les Emirats Arabes Unis, voire l'Asie.*
Nous nous organisons en désignant un ambassadeur ayant une parfaite connaissance du pays ou de la zone et un autre ambassadeur rompu à la connaissance purement business. Ces deux ambassadeurs sont les référents experts sur lesquels vont pouvoir s'appuyer les entreprises souhaitant se développer sur ces zones-là.
Par ailleurs, nous avons également un animateur désigné au sein de notre organisation qui, en dehors d'animer les réunions à thématique commerciale, se charge, par exemple, de mener une veille sur les appels à projets existants et de procéder à la diffusion au profit de tous. Ceci permet de développer de réelles synergies et ainsi de concrétiser des accords de partenariats.
En tant que relai local de proximité et d'experts, le cluster PRIMUS assure des services d'aides à la constitution de dossiers de prospection et d'assure-export (COFACE). Nous délivrons également des conseils pratiques sur le plan juridique, sur la protection avec des sujets comme la résilience, ou sous l'angle des ressources humaines. En effet, l'approche réseaux du cluster favorisant la détection de compétences clés, la gestion du turn-over s'en trouve facilitée.

Un autre avantage, et non des moindres, consiste également à rassembler les forces afin de réaliser des projets complexes. Je m'explique : poussées par le cluster, les PME et/ou ETI vont chacune apporter leurs briques de services, de produits, de technologies pour la réalisation d'un produit afin de répondre à des projets d'envergure (shelters déployables pré-équipés pour connexions extérieures, Data center SAIO – Shelter all in One : hébergement serveurs, stockage des données et routeurs). C'est donc une prise de marchés par des entreprises françaises.

Actuellement la politique de la Ministre des Armées se tourne vers le soutien à l'innovation des start-up, PME et ETI françaises, notamment à travers le plan ACTION PME lancé en mai 2018. Ce plan est déployé par l'ensemble des acteurs du ministère des Armées, dont la DGA en tête de file, et sur l'ensemble du territoire. »

Quelle est votre perception d'ACTION PME ?

« *Nous notons, depuis maintenant plus d'une année, une volonté forte d'aide aux PME-ETI par les services de l'Etat. Il s'opère effectivement un soutien fort et réel sur notre territoire. De nombreux évènements sont programmés à l'adresse des PME, notamment à travers le plan ACTION PME, dont la DRSD est un partenaire fort. Le cluster Primus a pris cette dynamique en marche et travaille en étroite collaboration avec les services de la DGA.*

.../...

Cluster Primus

Cet accompagnement des PME par la DGA, grâce à l'organisation de manifestations régulières, permet à nos membres de participer à des tables rondes sur des sujets comme le "Panorama des exportations d'armements", le programme "Fonds Européen de Défense" (FED) ou encore "l'Enterprise European Network" (EEN).

Le DGA – PME Tour a permis de réunir 80 entreprises régionales pour bénéficier de 8 ateliers sur des sujets concrets tels que le financement du développement et des innovations, l'accès au guichet européen, la prévention-protection des informations, la cybersécurité. Ces manifestations ne sont pas sans intérêt ; elles sont pour nos membres l'occasion de participer à de nombreuses rencontres "B to B" et entretiens individuels avec des experts DGA Export. »

Le cluster compte s'élargir à d'autres secteurs d'activité, voire s'implanter dans d'autres régions. Y-a- t-il des synergies à opérer ?

« Des manifestations d'intérêt ont déjà émergé. *Donc oui, nous envisageons la création de Clusters Primus régionaux et locaux : la Bretagne, la Nouvelle-Aquitaine, l'Ile-de-France, l'Hérault sont les prochaines pistes. Chaque cluster régional sera construit sur le même modèle que celui de Toulouse. Des synergies efficaces existent en effet. A Toulouse, la création du label « Transport Terrestre Intelligent » en est une illustration. L'association de quatre clusters que sont Automotech, Mipirail, Primus Défense & Sécurité et Robotics Place a permis de répondre au besoin du label à la recherche d'une brique sécurité manquante."*

Le cluster Primus Défense & Sécurité a pu combler ce manque grâce au soutien très fort de la région. Ce label compte aujourd'hui plus de 200 acteurs d'Occitanie et représente 25 800 emplois. La compétitivité des entreprises repose sur un paradoxe : d'un côté la nécessité de s'ouvrir pour conquérir des marchés, de l'autre, celle de protéger ses savoir-faire et ses innovations. »

Au vu de votre expérience : quels conseils donneriez-vous aux adhérents en termes de développement et de sécurité économique ?

« La réussite et la croissance passent par la préservation et la protection de ses savoir-faire, de ses innovations. Il faut garder à l'esprit que la vente d'un produit ou d'une solution n'implique pas d'en révéler les modes de conception ou de fabrication. Dans nos domaines d'activité où la concurrence est rude, la discrétion est de mise ! Des séances de sensibilisation internes sont indispensables pour inciter les collaborateurs à la discrétion sur certains de leurs sujets.
Dans le même ordre d'idée, lorsque des collaborateurs quittent la société, ils partent parfois avec des savoir-faire et des connaissances sensibles. Une attention particulière peut être portée sur ce point notamment via les clauses de confidentialité. " Vous montrez que vous savez ! Et bien ça c'est dangereux ! ".
En résumé pour maintenir sa compétitivité, je dirais : " Maintenir la connaissance ! " et " Éviter les bavardages dans les lieux publics ! "».

ISO 22301 : une norme internationale et une méthode

En France, quatre entreprises sur cinq annoncent avoir déjà subi une cyberattaque et plus de 30 % n'y sont pas préparées.

Or, la question n'est plus de savoir si une entreprise va se faire attaquer mais quand cela va se produire. La gestion de crise réduite à une simple liste de numéros d'urgence à appeler ne suffit plus. Il est nécessaire d'être préparé et, à cet effet, la norme ISO 22301 donne toutes les indications pertinentes sur l'utilité et la mise en place d'un plan de continuité et de reprise d'activité (PCA – PRA).

Une norme mondialement reconnue…

ISO 22301, première norme internationale de gestion de continuité des activités, a été développée pour aider les organisations à minimiser les risques liés à une situation de crise.

Cette norme ISO « Sécurité sociétale – Systèmes de Gestion de la Continuité des Activités – Exigences » est devenue le standard pour la gestion de la continuité des activités. Cette norme décrit un système de management global. Elle spécifie également les exigences en matière de planification, d'implémentation, de mise en œuvre, d'exploitation, de suivi, de maintenance et d'amélioration continue afin de se protéger en cas d'interruption d'activités potentielles, de sinistres ou d'attaques, de s'y préparer et d'en réduire la probabilité.

…délivrant une certification …

La certification "Lead Implementer 22301" atteste que la personne certifiée possède les connaissances et les capacités pour mettre en place un Système de Management de la Continuité d'Activité (SMCA).

La mise en place d'un SMCA permet d'anticiper les incidents et d'éviter qu'ils se transforment en crise majeure, mais aussi d'établir les processus de gestion globale des risques afin d'identifier les menaces potentielles et les impacts sur les opérations. Pour une entreprise, ce système de management vise à préserver la réputation, la marque et la valeur qu'elle génère tout comme les intérêts des principales parties prenantes (clients, fournisseurs, sous-traitants...). Elle renforce donc la crédibilité et instaure un climat de confiance vis-à-vis de l'ensemble des partenaires.

…incitant à une amélioration continue.

Le système de management d'amélioration en matière de continuité d'activité prévoit de :

- mener une analyse des risques afin d'en diminuer les effets et occurrences ;
- déterminer les options de continuité, les activités prioritaires, ressources humaines, techniques, informatiques, locaux, …;
- décrire les procédures et organisations qui permettent de redémarrer dans le contexte du sinistre ;
- inclure la communication vers les parties prenantes ;
- mettre en place des procédures de surveillance et d'alerte ;
- faire des exercices et tests pour valider les objectifs de continuité.

ITAR

Une norme américaine aux vulnérabilités méconnues

Aujourd'hui, nombreux sont les secteurs d'activité qui intègrent des composants d'origine américaine. Si votre entreprise connaît cette situation et que votre production a vocation à être exportée, les autorités américaines imposent le respect d'un certain nombre de réglementations. Parmi les dispositions à portée extraterritoriale appliquées par les Etats-Unis, la norme ITAR (International Traffic in Arms Regulation) concerne tout particulièrement le secteur de la défense.

ITAR, de quoi s'agit-il ?

La norme ITAR a été mise en place en 1976. Son but premier était de contrôler les flux d'armes afin d'éviter une prolifération vers le bloc de l'Est. En 1991, elle a été réformée afin de devenir également un outil de lutte contre le terrorisme. Aujourd'hui, cette norme permet aussi aux Etats-Unis d'effectuer un contrôle strict de la traçabilité, jusqu'au client final, de tout armement destiné à l'export et détenant une technologie ou un composant américain. Toute entreprise travaillant avec un de ces composants inscrit sur la « USML » (United States Munitions List) doit le déclarer, suivre une procédure spécifique et se soumettre à un accord préalable de l'administration américaine. Cette règlementation peut être contraignante en termes de coûts, d'autonomie stratégique et commerciale et d'emploi du personnel. Surtout, l'administration américaine peut émettre une « charging letter », sollicitant l'industriel afin que ce dernier prouve son respect des obligations imposées par ITAR. Il a la possibilité de faire réaliser son audit par des cabinets privés, généralement anglo-saxons.

Quels sont les bons réflexes à avoir ?

Tout d'abord, manipuler un composant inscrit sur cette liste requiert une grande rigueur. Toute intégration d'un élément ITAR dans un produit non-ITAR entraîne l'application des normes ITAR pour le produit tout entier. Une gestion et la traçabilité minutieuse des composants ITAR utilisés ainsi que du produit final sont indispensables (personnel, composants, produits, acteurs intermédiaires,..), pour assurer une maîtrise totale du processus au sein de l'entreprise.

De plus, si votre entreprise est concernée, il est nécessaire d'intégrer ce sujet dans une veille thématique afin d'identifier tout changement de l'USML. Au même titre que le risque douanier, les risques d'application de la norme ITAR doivent faire l'objet d'une analyse préalable afin de se prémunir contre les désagréments liés à un contrôle *a posteriori* (blocage des livraisons, audits…) et les éventuelles poursuites sur le sol américain. L'analyse de risque, faite par l'entreprise et à laquelle la chaîne "sûreté" doit être associée, est impérative car elle permet de cerner la problématique et doit avoir pour finalité la mise en place de procédures internes pour en minimiser l'impact. Cette analyse est indispensable pour toute entreprise de défense qui exporte, qu'elle agisse directement ou comme sous-traitant, afin d'éviter que cette norme impacte l'organisation et l'activité de l'entreprise et ses réseaux commerciaux. Les avantages à recourir, dans la mesure du possible, à des solutions "ITAR free" sont multiples : gagner en flexibilité et autonomie dans la gestion de ses projets, éviter de s'exposer à des audits intrusifs et des sanctions et pouvoir exporter plus librement tout en préservant ses réseaux d'affaires.

Protection

Accompagner la visite d'une délégation étrangère

Les entreprises ont besoin de recevoir régulièrement et parfois pendant plusieurs jours, voire plusieurs semaines, des délégations étrangères dont certaines sont susceptibles d'utiliser les infrastructures locales, depuis la salle de réunion jusqu'aux laboratoires en passant par des bancs d'essais.
L'aspect répétitif de ces visites, la connaissance des acteurs ou les sujets abordés peuvent donner le sentiment que les risques sont minimes ou maîtrisés.
Pour autant, il n'en est rien. L'expérience a montré que les pays ingérents profitaient d'une certaine naïveté des Français dans leurs relations avec les visiteurs étrangers. Les libertés laissées aux collaborateurs français dans des entreprises sont souvent bien plus restreintes que celles que nous leur donnons en France.

Comme souvent, si le niveau de sécurité de l'entreprise dans ce moment est directement lié au soin que l'officier de sécurité apporte dans sa préparation et dans sa conduite, il dépend surtout de l'implication des dirigeants dans la sécurité et de leur fermeté.
Les points de vigilance qui suivent ne sont que des exemples du plan d'action qu'il convient de mettre en place dans ce domaine et d'adapter en fonction des délégations.

Avant la visite : anticipation et cadrage du périmètre de la visite

- en interne identification des acteurs internes et des visiteurs ;
- définition stricte de la mission, de sa durée et de son périmètre ;
- rappel sur la conduite à tenir lors de la visite ;
- sensibilisation des parties prenantes sur les techniques habituelles de prises de contact individuelles ;
- sensibilisation sur les savoir-faire ou équipements sensibles qui pourraient intéresser la délégation afin de détecter toute tentative d'approche sur ces sujets ;
- prise de contact avec le poste de la DRSD territorialement compétent dès que la visite est connue.

L'organisation et le strict respect des itinéraires dits de "notoriété" ou parcours de visites, avec leurs consignes inhérentes, sont souvent les meilleurs gages d'une visite sans détournement d'information sensible.

Vis-à-vis de la délégation :

- échange avec un seul interlocuteur sur la composition de la délégation ;
- avertissement préalable sur le fait que seuls les membres qui auront fait l'objet d'une demande d'accès seront accueillis (ne pas admettre de flou sur l'identité) ;
- demander en amont un document d'identité ;
- idéalement, envoyer un mail visant à informer la délégation des mesures de sécurité en vigueur.

.../...

Protection

Pendant la visite : vigilance et fermeté

Accueil

L'accueil est le moment clé pour celui ou celle qui, dans la délégation, a des visées intrusives, voire offensives. Le premier test que fait généralement une délégation concerne soit la personne, soit les papiers, soit les moyens numériques. Habituellement, il est précisé qu'une personne est absente et que c'est telle autre personne, non prévue, qui finalement la remplace. Les arguments suivants sont souvent avancés : « il a fait le voyage ; il est venu exprès », « nous vous avons envoyé un mail »… La fermeté dans ce domaine entraîne plus de respect que de mépris. Il en est de même pour tout ce qui concerne les documents d'identité ainsi que les moyens numériques qui peuvent être emportés. Certains pays testent volontairement et peuvent déléguer des personnes qui ne font le voyage que pour tester un papier ou le passage clandestin d'un téléphone ou d'un objet connecté.

Briefing initial

Ce premier briefing doit être conduit par l'OS. Les limites de ce qui peut être fait ou non doivent être clairement posées et ne surtout pas être relativisées par un personnel de l'entreprise que l'aspect un peu direct du briefing gênerait. Les itinéraires ainsi que les salles doivent être clairement identifiés. Les conséquences pour ceux qui ne s'y plieraient pas doivent également être connues.

Conduite

Les personnes doivent systématiquement être accompagnées, même au bout d'une semaine, même pour aller aux sanitaires, y compris pendant les repas ;

- idéalement un membre de la structure de sécurité se charge de cet accompagnement, à défaut, un opérationnel spécialement sensibilisé s'en occupe ;
- elles doivent porter un badge apparent qui permet de les différencier visuellement ;
- elles ne doivent pas s'approcher d'ordinateurs du réseau ni d'écrans sur des postes de travail ;
- elles se déplacent en groupe et attendent en groupe ;
- tout écart dans le comportement doit être signalé à l'OS et faire l'objet d'un rappel à l'ordre à l'intéressé ainsi qu'au responsable de la délégation. Une exclusion doit être envisagée en fonction de la fréquence ou de la gravité des écarts ;
- les discussions doivent rester cantonnées aux sujets préalablement établis et validés (OS et directeur de programme) et ne doivent pas dériver vers d'autres centres d'intérêts.

.../...

Protection

En-dehors de la visite : ni naïveté, ni débordement

Les aspects conviviaux font partie des visites de délégation et sont un moyen privilégié de tisser un lien plus personnel qui compliquera ensuite l'application stricte des consignes de sécurité le lendemain. Si une décontraction apparente doit être cultivée, chaque parole ou chaque geste doit être maîtrisé, même lorsque des passions communes sont trouvées et même surtout si des passions communes sont trouvées.

Après la visite : RETEX et information de l'OS

La visite doit faire l'objet d'un RETEX avec l'OS et le chef de programme. Toute insistance sur un point précis est par exemple un indice de ce que cherche le pays visiteur.

L'OS doit sensibiliser tous ceux qui approchent de près ou de loin la délégation, surtout lorsque celle-ci est restée longtemps présente sur site, des possibilités de reprise de contact pouvant avoir lieu par la suite. Les personnes contactées doivent informer l'OS des échanges extra-professionnels qui pourraient être tentés.

En conclusion

Pour un client, le niveau de sécurité démontré par une entreprise est une marque de la confiance qu'on peut lui accorder en termes de vigilance. Pour l'entreprise, cette démonstration ne doit pas être associée à de la défiance, mais juste à la manifestation d'un savoir-faire supplémentaire. Il est à rappeler que la mise en place de Zones à Régime Restrictif (ZRR), disposant d'une existence légale, au sein des emprises industrielles permet de mieux en contrôler les accès, y compris dans le cadre de la visite de délégation.

SIAE 2019 : quels enseignements ?

La 53e édition du Salon international de l'aéronautique et de l'espace (SIAE) s'est tenue du 17 au 23 juin 2019 au parc des expositions du Bourget (93).

Par rapport à l'édition précédente (2017), cet événement a vu une hausse du nombre d'exposants et de délégations, avec une fréquentation restée globalement constante. Les actions de sensibilisation et d'accompagnement de la DRSD, menées en amont et pendant le salon au profit des sociétés françaises exposantes, ont été particulièrement appréciées. Elles ont notamment permis de leur présenter, de manière actualisée, les risques d'ingérences auxquels elles demeuraient exposées, y compris les PME et start-up innovantes.
Comme précédemment, certains de ces risques se sont concrétisés durant cette édition, au travers de tentatives de captations d'informations par des acteurs étrangers, à des fins de concurrence commerciale, ou encore de rattrapage technologique : approches humaines et questions intrusives, prises de vues et accès à des zones sans autorisation, vols de matériel ou d'informations...

Le dispositif mis en place par la DRSD durant le salon, en étroite coordination avec l'ensemble de ses partenaires institutionnels et industriels nationaux, a permis de déjouer efficacement la majorité de ces tentatives. La concrétisation de certaines de ces menaces démontre, s'il en est besoin, la nécessité du maintien, voire de l'accroissement, d'une vigilance permanente et effective de l'ensemble des acteurs, y compris des sociétés qui en sont les premières victimes.

Restons en contact

Direction zonale Île de France

prsd-villacoublay.cmi.fct@intradef.gouv.fr