La DRSD accentue sa « cyberisation »

Général de brigade Pierre WINCKEL
Chef d'état-major
Direction du Renseignement et de la Sécurité de la Défense (DRSD)
Ministère des Armées

« La DRSD, au cœur du renforcement de la résilience de nos forces et de la BITD »

C'est en ces termes que l'avis n°369 de l'Assemblée nationale[1] introduisait les enjeux pour la DRSD liés à la loi de finances pour 2023 en particulier afin de moderniser les méthodes de travail de la direction, accélérer les processus de traitement des demandes d'habilitation et acquérir trois nouveaux dispositifs numériques dont le projet CERT sur lequel je reviendrai plus tard dans mon propos.

Notre mission historique et actuelle

Depuis 150 ans, la direction du renseignement et de la sécurité de la défense travaille à protéger le pays contre les menaces à l'encontre de la sécurité des militaires et de l'industrie de défense. Nous avons toujours su nous adapter aux besoins de nos bénéficiaires et aux évolutions des menaces.

Or, la menace cyber est devenue, en moins d'une décennie, l'un des principaux risques auxquels sont confrontées les organisations de toutes tailles. Les attaques se multiplient et peuvent avoir des conséquences graves sur la continuité d'activité, la réputation, la conformité ou la sécurité des données des entreprises de défense, et par induction, sur la sécurité de la défense nationale.

La loi de programmation militaire 2019-2025 avait permis à la DRSD, d'engager une remontée en puissance significative des effectifs de notre direction, qui concerne au premier chef le domaine cyber et d'acquérir de nouveaux outils performants et adaptés au domaine de la cyberdéfense.

La loi de finances 2023 et la prochaine LPM 2024-2030, en ligne avec la stratégie nationale permettent désormais à la DRSD de compléter le dispositif national de cyberdéfense aux cotés de l'ANSSI, du COMCYBER et de nos autres partenaires de la communauté cyber et ainsi d'assurer pleinement son rôle en matière de protection et de cybersécurité des entreprises de défense.

Le projet CERT entre en phase opérationnelle

Il y a un an presque jour pour jour, le GCA Eric BUCQUET, alors directeur de la DRSD, annonçait dans une Matinale du CyberCercle le lancement du projet CERT-BITD.

[1] Avis de M. Jean-Charles LARSONNEUR, fait au nom de la commission de la Défense nationale et des Forces armées de l'Assemblée nationale, enregistré le 19/10/2022.

Je suis heureux de vous informer que ce projet a abouti et que la DRSD a officiellement ouvert ce nouveau service de cybersécurité le 21 juin 2023.

Le nom de CERT des Entreprises de Défense, CERT *[ED]*, a finalement été retenu car plus exhaustif et intelligible que BITD - Base Industrielle et Technologie de Défense - dans lequel les TPE/PME de défense ne se retrouvaient pas.

Ce service de cybersécurité est une évolution logique de notre activité historique de sécurité physique, qui nous a permis de protéger nos bénéficiaires contre les risques liés aux personnes et aux biens matériels.

Aujourd'hui, la menace cyber est devenue un enjeu majeur pour toutes les organisations, quels que soient leur taille, leur secteur ou leur localisation. Les attaques informatiques se multiplient et se diversifient, visant à voler des données, à perturber des systèmes ou à nuire à la réputation. Les conséquences peuvent être désastreuses sur le plan financier, juridique ou opérationnel.

De l'effervescence législative

Face à ce défi, l'environnement règlementaire national et supranational se veut de plus en plus exigeant et les organisations doivent s'y conformer bon gré mal gré.

Le règlement général sur la protection des données (RGPD), entré en vigueur en 2018, impose des obligations renforcées en matière de sécurité des données personnelles.

La loi de programmation militaire (LPM), révisée en 2019, impose des mesures de protection aux opérateurs d'importance vitale (OIV) et la déclaration des incidents cyber vers l'ANSSI.

La directive sur la sécurité des réseaux et des systèmes d'information dite « directive NIS », transposée dans sa première version en France en 2019, impose des exigences de sécurité aux opérateurs de services essentiels (OSE) et aux fournisseurs de services numériques (FSN) toujours en lien avec l'autorité nationale.

La seconde version (directive européenne 2022/2257 « NIS-2 ») dont la transposition en droit français devrait intervenir en 2024 élargi le périmètre des organisations concernées, incluant des entités publiques et des entreprises de moindre taille dont possiblement des entreprises de la sphère de défense.

NIS-2 renforce les obligations de sécurité et de notification des incidents, et durci les sanctions pour les éventuels contrevenants.

La nouvelle directive européenne 2022/2555 sur la résilience des entités critiques, (REC) se superposerait au dispositif de sécurité des activités d'importance vitale (SAIV) inscrit en 2006 dans le code de la défense.

La cybersécurité à la DRSD

Pour répondre aux besoins des entreprises de la sphère de défense dans ce contexte complexe et évolutif, nous avons décidé de mutualiser les compétences et étendre les services dédiés à la cybersécurité, afin d'assurer des prestations de haut niveau adaptées à chaque situation.

La DRSD est désormais en mesure de remplir l'ensemble des missions suivantes :

- Conseiller les dirigeants d'entreprises de défense pour définir une politique et une gouvernance de la cybersécurité ;
- Réaliser des audits de sécurité, pour évaluer le niveau de maturité et de conformité aux normes et aux réglementations en vigueur dans le domaine de

la cybersécurité ;
- Aider à la mise en œuvre des mesures organisationnelles et des solutions de protection, de détection et de réaction adaptées aux besoins et aux contraintes de chaque projet ;
- Sensibiliser* les utilisateurs aux bonnes pratiques de la cybersécurité ;
- Conseiller et accompagner* les responsables de la sécurité dans la connaissance de leurs vulnérabilités et dans la protection de leurs systèmes informatiques / de leurs données ;
- Relayer* les campagnes préventives de recherche de compromission pilotées par l'autorité nationale (ANSSI / CERT-FR) ;
- Assister* les entreprises victimes de cyberattaques dans la qualification des incidents et dans la reprise de contrôle de leur système numérique.

Les entreprises de défense pourront joindre la permanence du CERT *[ED]* au numéro vert 0 805 046 300 (appel gratuit).

Conclusion

Je suis convaincu que la cybersécurité est un facteur clé de succès pour toute organisation moderne et responsable.

Le CERT *[ED]* et l'ensemble des experts cyber de la DRSD présents sur notre territoire national sont impatients d'accompagner l'écosystème de la sphère de défense dans cette démarche et de leur faire bénéficier de notre expertise.

*avec l'appui des experts du CERT *[ED]*