La BITD dans le cy(*ber*)clone

Général de corps d'armée Eric BUCQUET
Directeur du Renseignement et de la Sécurité de la Défense (DRSD)
Ministère des Armées

L'industrie de défense : une souveraineté nationale à protéger

Le rapport d'information du Sénat[1] n°605 exposait mi-2020 les difficultés traversées par les entreprises de la BITD et celles qu'elles devraient encore affronter, principalement dans le champ des investissements indispensables à leur croissance. Ce rapport s'intitulait « l'industrie de défense dans l'œil du cyclone ». Face à la menace croissante et aux attaques régulièrement constatées, les 4 000 entreprises de la base industrielle et technologique de défense (BITD) mais aussi les 10 000 entités suivies par la DRSD au titre de la protection du potentiel scientifique et technique de la nation (PPST) ne connaissent pas le calme relatif et précaire de l'œil du cyclone. Elles sont dans le cy(ber)clone.

Cybercriminalité et cyberespionnage sont entrelacés et rendent cette menace particulièrement dangereuse car plusieurs effets néfastes peuvent se cumuler pour non seulement piller mais aussi, *in fine*, détruire leurs cibles.

Quelles peuvent être les conséquences principales de ces attaques ?

Je placerai deux conséquences comme étant les plus graves possibles.
La première est le coût économique pour l'entreprise qui peut subir toute une gamme de pertes financières, depuis la « simple » escroquerie de type arnaque au président ou FOVI[2] jusqu'à la double voire triple extorsion de type rançonnage à laquelle peut venir s'ajouter non seulement le blocage de l'outil de production mais également l'exfiltration de données stratégiques et/ou personnelles (avec éventuellement une pression en cascade sur les victimes tierces). Cela peut conduire à la faillite d'une entreprise possiblement critique dans notre écosystème de défense. Sa mise en péril industriel pendant plusieurs semaines ou plusieurs mois, en raison de difficultés à assurer la livraison des commandes ou à facturer correctement ses clients, pourrait également fortement perturber en fin de chaîne de valeur la production d'un équipement stratégique.
La seconde est la compromission du secret de la défense nationale. Les niveaux de classification entrés en vigueur avec la nouvelle instruction générale interministérielle 1300 sur la protection du

[1] Rapport d'information de MM. Allizard et Boutant, fait au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, déposé le 8/7/2020.

[2] Faux ordres de virement – escroquerie avec usurpation d'identité.

secret de la défense nationale il y a un an ont consolidé la notion de protection de l'information et rappelé le rôle essentiel qu'elle joue pour l'exercice des activités régaliennes de l'État. Si les textes particuliers régissant l'aptitude d'un réseau à accueillir des informations secrètes imposent un cadre qui rend particulièrement difficile leur accès, la compromission du secret est d'une gravité majeure car elle étend les conséquences de l'attaque cyber au-delà du périmètre de l'entreprise, pouvant même se porter jusque sur les équipements de nos forces armées.

À qui profite le crime ?

Qui sait si les données exfiltrées par des criminels l'ont été afin d'obtenir le paiement d'une rançon ou pour répondre à la demande d'un commanditaire, qu'il s'agisse d'un concurrent malveillant ou d'un service d'espionnage étatique ?
La mission de la DRSD, qu'elle soit de protection du secret de la défense ou de service enquêteur[3], l'oblige à répondre à ce type d'interrogation. Il est donc important qu'elle soit rapidement informée des incidents cyber touchant les entreprises de la BITD. La rapidité de réaction facilite en effet la mise en place du processus de levée de doute et permet d'aider l'entreprise à faire face efficacement aux conséquences.

Comment mieux protéger l'écosystème de défense et faire face aux attaques ?

Depuis 150 ans[4], la DRSD travaille à protéger le pays contre les menaces à l'encontre de la sécurité des militaires et de l'industrie de défense. Le Service a historiquement pour cœur de métier la contre-ingérence des forces et la contre-ingérence économique auxquelles s'ajoute depuis déjà plusieurs années la contre-ingérence cyber.
C'est à ce titre et pour compléter le dispositif national qu'il a été décidé en 2021 d'initialiser un projet de CERT[5] sectoriel dédié à la protection des entreprises du périmètre défense : le CERT-BITD[6]. Appuyé par les plus hautes instances du ministère des armées, ce projet bénéficie par ailleurs du programme d'incubation de l'ANSSI.

Quid de la protection dans les territoires ?

Une des forces de l'organisation de la DRSD repose sur son maillage territorial qui lui permet une proximité et une réactivité d'intervention locale, indispensable face aux attaques de plus en plus fulgurantes. Par ailleurs, les échanges quotidiens entre les entreprises de la BITD et les agents de la DRSD, que ce soit au cours des sensibilisations, inspections, audits, processus d'habilitation…, favorisent un climat de confiance utile à l'alerte en cas d'attaque cyber. Les équipes cyber de la DRSD en région seront ainsi progressivement dimensionnées pour répondre aux exigences du CERT-BITD et disposeront également de formations complémentaires adaptées. Elles seront ainsi pleinement en mesure d'assurer la primo-intervention, la levée de doute et le conseil adapté au durcissement de la sécurité du système compromis, particulièrement utile pour les petites et très petites entreprises, souvent les plus démunies en capacité cyber. Lorsque cela sera nécessaire, elles seront appuyées par les experts de la direction centrale.

A terme, le CERT-BITD offrira plusieurs services.

[3] Code de la défense et IGI 1300 - protection du secret de la défense nationale - Légifrance
[4] Créée en 1872, la DRSD a fêté en présence du ministre des armées le 150ème anniversaire de la création de la section de statistiques qui est à l'origine du contre-espionnage et de la contre-ingérence militaire.
[5] *Computer Emergency Response Team*
[6] CERT sectoriel de la base industrielle et technologique de défense.

Le service le plus visible sera la réponse à incident. Ce dispositif permettra aux entreprises du périmètre de déclarer leurs incidents cyber grâce à une plate-forme spécifique et à la DRSD de réagir et de déclencher si besoin l'envoi d'un élément d'intervention cyber.

Un autre service sera la veille en vulnérabilités. Le maintien d'une veille réactive est en effet indispensable pour être en mesure de détecter au plus tôt une propagation cyber malveillante.

Cela conduit naturellement au troisième service : la connaissance de la situation cyber[7]. La présence de la DRSD au Campus Cyber inauguré en février 2022 à La Défense favorisera naturellement cet aspect.

Enfin, le quatrième service recouvrira la formation et la sensibilisation. Comme sur la route, respecter les règles et rouler dans un véhicule bien entretenu permet d'éviter beaucoup de problèmes ! La DRSD a déjà une capacité éprouvée de sensibilisation et je reste persuadé que l'effort doit être permanent sur cet axe.

Le CERT-BITD a déjà passé une phase de POC[8] sous l'égide de l'ANSSI et fera l'objet au second semestre 2022 d'une mise en œuvre limitée à une région pilote. Il a vocation à être étendu à tout le territoire métropolitain au second semestre 2023.

Ce CERT-BITD sera parfaitement intégré dans la stratégie nationale pour la cybersécurité lancée en 2021 par le Président de la République et représentera une brique « BITD » majeure dans le dispositif national de protection cyber des entreprises. Dès que le CERT-BITD sera effectif sur tout le territoire, les entreprises en lien avec la défense seront toujours sous la menace cyber… mais mieux armées pour résister aux cyclones !

[7] Service aussi connu sous l'acronyme anglais CTI, *Cyber Threat Intelligence*.

[8] *Proof of concept*