OIV : la détection des attaques passe sous le contrôle de l'Etat

L'Anssi (Agence nationale pour la sécurité des systèmes d'information) serre peu à peu la vis aux OIV (Opérateurs d'importance vitale), environ 250 organisations dont le bon fonctionnement est jugé essentiel au fonctionnement de la Nation. Après les premiers arrêtés sectoriels (sortis en juin et en août) encadrant la sécurité informatique de ces entités, l'agence s'attaque à un élément clef de son dispositif découlant de l'article 22 de la Loi de programmation militaire (LPM), votée fin 2013 : la notification d'incidents.

Rappelons que, pour les systèmes d'information dits d'importance vitale – que chaque entreprise doit définir par elle-même -, « *les opérateurs (d'importance vitale, NDLR) communiquent les informations dont ils disposent dès qu'ils ont connaissance d'un incident et les complètent au fur et à mesure de leur analyse de l'incident* », précise un décret paru en mars 2015. Et, pour ce faire, ils devront faire appel à des prestataires certifiés, les PDIS (Prestataires de détection d'incidents de sécurité). « *Au sein des OIV, trois niveaux de sécurité sont définis. Le plus élevé – C3 – devra être protégé par une société habilitée* », précise Denis Attal, directeur technique de Thales Critical Information Systems (CIC), une des sociétés engagées dans cette certification.

PDIS 1.0 face à la réalité du terrain

Cette dernière a en effet bel et bien démarré. Sur son site, l'Anssi indique avoir lancé *« une procédure expérimentale afin de tester le référentiel en conditions réelles* ». Plusieurs SOC (Security Operation Center), ces centres de supervision de la sécurité, sont aujourd'hui en passe d'être habilités, comme l'ont confirmé quelques sociétés avec qui nous nous sommes entretenus. « *Le processus habituel de l'Anssi consiste à tester le référentiel sur de premiers prestataires* », dit Alexandre Garret, directeur marketing Orange Cyberdéfense. Atos indique également avoir été sélectionné pour faire partie de la phase expérimentale du PDIS (avec son offre SOCaaS). Officiellement, les prestataires expliquent ne pas avoir de visibilité sur les dates d'attribution des premières certifications PDIS. Notons simplement que le référentiel a été publié en version 1.0.

Il ne s'agit pas là des premières certifications de l'Anssi ; il existe déjà de longues listes de prestataires de certification, les PSCE, et de prestataires d'audit, les Passi.

En parallèle, l'Anssi s'est d'ailleurs lancée dans une autre certification, celle des prestataires de réponse aux incidents de sécurité (ou PRIS). Là aussi, le processus d'habilitation est en cours. Mais, ici, l'agence publie une liste de quatre premiers prestataires engagés dans le processus (Conix, Lexfo, Lexsi – désormais propriété d'Orange – et Thales). S'y ajoute Airbus Defence and Space qui nous a confirmé avoir entamé la démarche. Cette future certification est toutefois très différente de celle concernant les SOC. Comme l'indique l'Anssi, la LPM n'impose pas aux OIV le recours à des PRIS.

« Un pic d'activité en 2017 et 2018 »

C'est donc le PDIS qui a les plus fortes chances d'avoir une influence certaine sur les investissements des grandes entreprises françaises. Car la certification va les pousser à externaliser au minimum une partie de la supervision de leurs infrastructures. Avec un effet contagion probable, comme l'a montré le récent contrat passé entre Engie et Thales, portant sur la supervision mondiale des infrastructures du groupe de 155 000 personnes par le SOC de Thales, situé à Elancourt, dans les Yvelines (en photo).

Pour les prestataires toutefois, l'effet d'entraînement ne sera pas immédiat. « *Il est difficile de quantifier la vitesse d'équipement des OIV et quelle partie du périmètre de leur système d'information va être classée C3*, dit Denis Attal, de Thales. *Pour l'instant, nous ne détectons pas de réelle accélération sur le marché, même si des grands comptes comme Engie ont fait le choix d'anticiper.* » Pour Orange Cyberdéfense, ce retard à l'allumage est assez habituel : « *quand un règlement sort, on assiste toujours à une phase d'attentisme. Mais, aujourd'hui, on voit le volume de dossiers grossir. Bien sûr, il y a les entreprises OIV qui sont obligées de se tourner vers les prestataires certifiés, mais aussi des entreprises qui ne sont pas soumises à la LPM mais sont tout même intéressées par les sociétés certifiées par l'Anssi.* » Le constat est d'ailleurs similaire pour Alexandre Jouys, le directeur commercial de Thales Services, qui voit lui aussi son 'pipe' se remplir : « *Certes, pour le moment, la législation n'a pas un effet d'entraînement net sur le nombre d'affaires signées. Mais on assiste à une augmentation du nombre d'appels d'offres. On peut s'attendre à un pic d'activité en 2017 et 2018* ».

Une certification PDIS coûteuse

Pour bénéficier du tampon de l'Anssi – et donc accéder au marché des OIV -, les prestataires n'ont d'autre choix que d'investir dans la certification. « *C'est un avantage concurrentiel d'être certifié mais cela passe par des investissements. Il faut notamment faire certifier ses équipes* », dit Denis Attal. Comme le précise Alexandre Garret, d'Orange Cyberdéfense, les investissements seront même probablement plus lourds avec le PDIS, qu'avec d'autres certifications, comme PRIS : « *Dans la réponse à incidents, on parle avant tout de certifier des individus et des processus. Les coûts de la certification seront avant tout liés à des investissements humains. On devrait se situer dans les mêmes eaux qu'avec la certification Passi, autrement dit des coûts non neutres mais absorbables et limités à moins de 100 000 euros. Le constat peut être différent avec le PDIS, qui nécessitera plus de mises à niveaux dans les processus et compte beaucoup d'exigences techniques. Ce sera probablement plus coûteux, même si cela dépend du niveau de départ du prestataire qui veut se faire certifier.* »

Sans oublier le fait que les prestataires sont confrontés à des référentiels d'exigence différents d'un pays à l'autre. Même si des discussions existent au niveau européen pour rapprocher les attentes des différents pays membres, rien n'est aujourd'hui abouti. « *Le manque d'harmonisation des niveaux d'exigence en Europe crée de vraies problématiques, que nous avons dû adresser sur le contrat Engie dont la couverture est mondiale* », précise ainsi Alexandre Jouys.

Vers le SOC 2.0

Pour Thales toutefois, si la certification PDIS est un « *must have* », elle ne suffit pas pour remporter des marchés. Et ne saurait résumer à elle seule les enjeux auxquels font face les grandes entreprises, fussent-elles classées OIV. « *La LPM n'est qu'une composante des défis qui attendent les entreprises en matière de sécurité. La transformation numérique en est une autre, car cette transformation se révèle anxiogène pour les entreprises. C'est par exemple un des facteurs clefs dans le contrat que nous avons signé avec Engie* », explique ainsi Jean-Marie Letort, vice-président stratégie et marketing de l'activité sécurité de Thales CIC.

Si le référentiel PDIS se veut très précis en matière d'exigences (avec par exemple une cinquantaine d'indicateurs réclamés par l'Anssi), la société dirigée par Patrice Caine indique aussi travailler à l'évolution technologique de ses SOC. « *Nous travaillons déjà sur le SOC 2.0, via des développements internes et des partenariats,* reprend Jean-Marie Letort. *Les investissements portent sur la détection proactive des menaces. Pour ce faire, nous nous appuyons sur le Machine Learning et le Deep Learning. L'enjeu consiste à réduire les faux positifs par l'analyse comportementale des menaces.* » Cette montée de version vers ce que Thales appelle le SOC 2.0 se fera graduellement, au cours des deux années qui viennent, sur la base de technologies dont Thales jalouse les secrets, la société se refusant par exemple à dévoiler les partenaires avec lesquels elle travaille. Outre Elancourt (78) – qui supervise une quarantaine de grands comptes -, Thales aligne deux autres centres de supervision (aux Pays-Bas et en Grande-Bretagne) et doit en ouvrir prochainement un troisième à Hong-Kong.

A lire aussi :

[La sécurité des OIV mise au pas par l'Etat… petit à petit]

[L'Etat français va certifier les Cloud de confiance]

Crédit photo : Light eX Machina