Orange Cyberdéfense entend surfer sur la législation des OIV

Faut-il y voir un hasard du calendrier ? Probablement pas. Alors que se met en place la législation encadrant la sécurité des grandes entreprises et administrations françaises, Orange Cyberdéfense, l'activité cybersécurité de l'opérateur juridiquement constituée depuis le 1er janvier, montre les muscles. Lors d'une conférence de presse à Rennes, l'opérateur, qui au cours des deux dernières années s'est renforcé sur ce créneau via deux rachats (Atheos en 2014 et Lexsi en 2016), s'est positionné comme le leader des prestataires de cybersécurité en France. Le cabinet Pierre Audoin Consultants lui attribue une part de marché de 7,9 % en 2015 (devant Atos, qui avec le renfort de Bull, atteint 7,3 %), pour un chiffre d'affaires de 125 millions d'euros (+ 11 % sur un an). « *La cybersécurité ressemble un peu à Game of Thrones* », ironise Michel Van den Berghe, le directeur d'Orange Cyberdéfense, pour parler de la course aux armements que se livrent les grands noms du secteur. Et d'insister sur l'avance prise par sa société dans la conquête du 'cyber-trône de fer'.

« *Avec le renfort de Lexsi (intégré depuis le second trimestre de 2016), notre part de marché devrait avoisiner les 10 %* », assure Michel Van den Berghe. De quoi conforter la domination d'Orange Cyberdéfense dans l'Hexagone et lui assurer une place dans le top 5 européen. Bref, la structure regroupant 1200 personnes se voit comme idéalement positionnée pour profiter du renforcement des règles de cybersécurité s'imposant aux grandes entreprises françaises, en particulier avec l'entrée en vigueur de la législation sur les Opérateurs d'importance vitale (OIV), environ 250 organisations dont la sécurité est peu à peu strictement encadrée par l'Etat.

2 millions d'euros pour une certification

C'est notamment le cas dans la détection d'incidents, un domaine où l'Anssi (Agence nationale de la sécurité des systèmes d'information), qui pilote la législation des OIV, entend imposer une habilitation aux entreprises concernées. En résumé, celles-ci devront soit faire certifier leur centre de supervision (on parle de SOC pour Security Operation Center), soit passer par un prestataire habilité. « *Nous avons investi plus de deux millions d'euros pour nous mettre en conformité avec les 400 exigences du référentiel Anssi* », détaille Rodrigue Le Bayon, le responsable de la cyber-surveillance chez Orange Cyberdéfense. Ce niveau d'investissement explique à lui seul pourquoi l'opérateur mais aussi ses concurrents nourrissent tant d'espoirs sur ce marché : le niveau d'exigence fixé par l'Anssi devrait encourager les grandes entreprises françaises concernées à se tourner vers l'externalisation. Même si quelques-unes – dans le secteur bancaire notamment – pourraient tout de même poursuivre la surveillance de leurs infrastructures en solo.

« *Et nous encourageons l'Anssi à ne pas abaisser ses exigences* », ajoute Rodrigue Le Bayon. A ce jour, Orange affirme faire partie des 3 prestataires à avoir passé le premier niveau de certification PDIS (Prestataires de détection d'incidents de sécurité), le nom donné par l'Anssi à cette habilitation. Récemment, dans nos colonnes, Thales et Atos indiquaient également être engagés dans cette certification. Orange Cyberdéfense explique avoir été récemment audité par l'Anssi et avoir basculé un premier client sous le régime PDIS.

21 milliards d'événements par jour

Chez Orange, c'est l'offre dite CyberSOC qui est concernée par cette habilitation. Cette structure, présente à Rennes (avec 80 personnes) et en Inde (40 personnes environ), compte environ 80 clients (surtout des grandes entreprises) et apparaît comme une évolution des centres de supervision traditionnels d'Orange, axés sur la gestion distante des éléments périphériques du réseau. « *Nous sommes passés à une logique de détection/traitement sur l'ensemble du système d'information*, détaille Franck Ollivier, le responsable du CyberSOC. *On s'appuie sur des sondes placées dans l'entreprise ainsi que sur la collecte et la corrélation des événements dans un SIEM (Security information and event management, console de gestion et de corrélation des logs) pour identifier, 24 heures sur 24 et 7 jours sur 7, les comportements suspects.* » Un domaine où évidemment la phase d'analyse des événements techniques collectés (21 milliards par jour pour Orange) s'avère déterminante.

Pour se distinguer de la concurrence, Orange mise sur une base de données maison, renfermant les menaces et constituée par une équipe de R&D interne. « *Cette base de 16 millions de données catégorisées est réinjectée dans le dispositif opérationnel. Et 50 % des données qui y figurent ne sont présentes dans aucune base commerciale. C'est tout l'intérêt de se tourner vers un prestataire de cybersécurité qui est également un opérateur télécoms !* », explique Rodrigue Le Bayon. Orange assure en effet être, de par son activité centrale, en mesure de détecter les prémisses de certaines attaques. C'est particulièrement le cas dans le déni de service distribué (DDoS). « *Notre base est complémentaire de celles d'acteurs comme Trend Micro ou Kaspersky. Nous travaillons sur des attaques non référencées dans ces bases* », assure Michel Van den Berghe.

Réponse aux incidents : un campus à Lille

Selon le prestataire, pour une entreprise, le coût de la supervision annuelle démarre à quelques dizaines de milliers d'euros et peut dépasser le million d'euros. Orange dit s'engager sur la réactivité de ses équipes à une attaque et être en mesure de donner des garanties à ses clients sur les risques métiers couverts par la prestation. « *On va jusqu'à des pénalités* », dit Michel Van den Berghe. L'enjeu central d'un SOC est évidemment de ne pas passer à côté des menaces ciblant l'entreprise. Selon le Gartner, 92 % des attaques ne sont tout simplement pas détectées par les entreprises. Orange assure ne pas être informé d'attaques lui ayant échappé et ayant provoqué des dommages chez un des clients de son CyberSOC.

Au-delà du volet détection, signalons qu'Orange Cyberdéfense s'est aussi lancé dans la certification de l'Anssi relative à la réponse aux incidents (PRIS , prestataires de réponse aux incidents de sécurité). Lexsi, désormais propriété d'Orange, figure d'ailleurs parmi les quatre premiers prestataires en cours de qualification. Et Orange prévoit également d'ouvrir début 2017 un campus à Lille dédié à cette activité (le positionnement de la capitale des Flandres au cœur de l'Europe expliquant ce choix). « *Dès l'inauguration, en janvier, ce centre comptera 60 personnes*, dit Michel Van den Berghe. *Et on va monter à une centaine de collaborateurs en 2018.* »

A lire aussi :

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

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

L'Etat français va certifier les Cloud de confiance