OIV : la France pousse à la normalisation des incidents de sécurité

Difficile d'organiser une défense collective, le vœu de l'Anssi (l'Agence nationale pour la sécurité des systèmes d'information) avec la législation encadrant la cybersécurité des organisations stratégiques de France, avec des outils ou des organisations qui ne dialoguent pas entre eux selon des normes partagées. Pas étonnant donc de retrouver l'agence dirigée par Guillaume Poupard parmi les soutiens d'un projet de recherche appelé Secef, emmené par CS Communication et Systèmes, et où figurent également TelecomSudParis (qui dépend de l'institut Mines-Télécom) et CentraleSupélec. Objectif de Secef : moderniser et promouvoir deux formats internationaux appelés IDMEF et IODEF.

Derrière ces acronymes un peu barbares, se cachent deux formats d'échange. Le premier (Intrusion Detection Message Exchange Format) vise à normaliser les communications sur les incidents entre les dispositifs techniques (par exemple entre les sondes et les consoles d'agrégation). Le second (Incident Object Description Exchange Format) sert à décrire des incidents de sécurité entre des équipes différentes. C'est par exemple un format que peuvent employer les SOC (Security Operation Center) pour s'échanger des informations sur les menaces. Un point qui intéresse évidemment l'Anssi, puisque cette dernière est censée recevoir, dans le cadre de la législation sur les OIV (Opérateurs d'importance vitale), les remontées d'incidents de sécurité de ces quelque 250 organisations jugées essentielles au bon fonctionnement de la nation. « *L'Anssi aimerait bien éviter d'avoir à gérer autant de standards de remontée d'incidents que d'OIV* », résume Thomas Girard, le directeur du département cyber-sécurité de CS, un intégrateur qui réalise 170 millions d'euros de chiffre d'affaires et emploie 1 800 personnes environ.

Une norme sous-utilisée

Si CS apparaît comme la cheville ouvrière de Secef, c'est avant tout parce que la société propose une console de centralisation des événements de sécurité (en jargon un SIEM, security event information management), qui équipe notamment le ministère de la Défense. « *C'est la seule solution française et même européenne du genre* », assure un porte-parole de CS. Ce produit, appelé Prélude, est compatible avec le format IDMEF depuis le début de sa commercialisation, en 1999. Mais, pour CS, la législation sur les OIV en France apparaît comme une opportunité de remettre l'importance de la standardisation des formats de description des incidents sur le devant de la scène et de bénéficier du regain d'intérêt pour la technologie française qui accompagne la mise en place de la législation. « *Nous avions déjà un standard IDMEF en version 1, normalisé par l'IETF (depuis 2007, NDLR). Avec l'Anssi et la DGA (Direction générale de l'armement), nous avons décidé de l'améliorer et de l'ouvrir pour en faire un format d'échange global* », explique Thomas Girard. Le projet vise à faciliter l'intégration des différentes technologies de sécurité.

Car, aujourd'hui, on en est loin. La plupart des matériels et logiciels des grands industriels du secteur, notamment américains, ignore le standard, explique CS. « *Par volonté politique* », tranche Thomas Girard. Et ce, même si, selon lui, le format de l'IETF présente l'intérêt d'être très complet

(avec 250 champs). « *Aujourd'hui, seule une partie du parc d'équipements dialogue en IDMEF. Dans mes rêves les plus fous, il en irait de même pour Cisco et Microsoft !* », lance le directeur du département cyber-sécurité de CS. Aujourd'hui, selon ce dernier, si 100 % des sondes de détection d'intrusion sont compatibles (sous l'influence de Snort en particulier), aucun log Windows n'est conforme au standard. D'où la nécessité de développer et de maintenir de multiples connecteurs sur les consoles de remontée d'incidents. « *Sur le marché, cette absence de normalisation provoque une course en avant permanente, avec des formats qui évoluent à chaque nouvelle version de produit* », regrette Thomas Girard.

Déjà adoubés dans le RGI

Si on retrouve l'Anssi parmi les parrains de Secef, il est peu probable que l'agence ira jusqu'à imposer des formats précis comme IDMEF aux OIV. La question pourrait en revanche se poser pour la normalisation des échanges entre l'Anssi et les équipes des OIV, autour de IODEF. Mais les négociations entre l'Agence nationale et les organisations concernées autour du déploiement pratique de la législation sur les OIV sont loin d'être terminées. Et restent tendues, car les contraintes émanant de la loi impliquent des dépenses supplémentaires que les OIV sont censés supporter… Même si les deux normes ne leur seront probablement pas imposées, elles sont en réalité déjà adoubées par l'Etat, via la seconde version du Référentiel général d'interopérabilité (RGI, en PDF ici), un référentiel de formats informatiques conseillés aux administrations françaises. Tant IODEF que IDMEF y figurent, avec le statut recommandé, le niveau le plus élevé parmi les quatre que décrit le RGI.

En parallèle, le projet Secef vient de lancer un programme partenaires, visant à aider les éditeurs de sondes ou d'autres produits de sécurité à rendre leurs produits compatibles IDMEF. Quatre sociétés y figurent déjà (Stamus, Ilex, 6cure et Teclib' avec l'antivirus Armadito) et trois autres travaillent à les rejoindre (Darktrace, Quarslabs et Sentryo). « *Notre volonté, c'est que le projet nous échappe* », assure Thomas Girard. Le consortium entend aussi soumettre les nouvelles versions des deux standards à la normalisation internationale. « *Et, en 2017, nous voulons aussi changer d'échelle sur le programme en nous appuyant sur des organismes européens* ». Logique, puisque la directive NIS (Network and Information Security), proche de la législation française sur les OIV dans ses principes, prévoit elle aussi une notification des incidents majeurs aux autorités nationale et un partage d'informations sur les menaces entre Etats membres.

A lire aussi :

Assises de la sécurité 2016 : l'urgentiste Poupard prescrit ses remèdes

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