Eau, santé et alimentation, les premiers arrêtés sur les OIV publiés

Il y a quelques semaines, Guillaume Poupard, directeur général de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) nous avait indiqué que les arrêtés concernant les opérateurs d'importance vitale (OIV) allaient bientôt paraître. Il avait précisé que ces arrêtés concerneraient d'abord certains secteurs, avec une première vague effective à partir du 1er juillet 2016. Une autre devrait intervenir à la rentrée. En réponse au propos du responsable, le *Journal Officiel* vient de publier une salve de 3 arrêtés fixant « *les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité* ». Les 3 textes visent les secteurs de la gestion de l'eau, des produits de santé et de l'alimentation. Une sortie émaillée d'un « dialogue rugueux » entre les entreprises et administrations référencées comme OIV et l'ANSSI, avait souligné Guillaume Poupard lors des Assises de la Sécurité Informatique en octobre dernier. Et les discussions ont traîné, le directeur général de l'ANSSI l'a avoué lors du dîner des savoirs sur le risque IT, tout en relativisant. « *Il y a surtout des incompréhensions qui ont finalement été résolues* », déclarait-il.

Fruit de ces échanges, les arrêtés fixent donc un ensemble de règles strictes en matière de sécurité pour les OIV sur les systèmes d'information d'importance vitale (SIIV) identifiés comme tels. Car l'ensemble du système d'information (SI) des OIV n'est pas concerné par les obligations des arrêtés. Il y a donc eu un travail en amont pour déterminer le périmètre du SI qui est concerné. Une fois le SIIV identifié, il va devoir être homologué à travers un dossier et un audit. Cet audit porte l'architecture, la configuration, l'organisationnel et le physique. Il est réalisé par un prestataire qualifié homologué par l'ANSSI. A noter que l'homologation est valable pour une durée de 3 ans.

Cartographie du SI et sondes de détection

Dans les règles pointées par les arrêtés, les OIV vont devoir fournir une cartographie des SIIV avec différents éléments : noms et fonctions des applications, plages d'adresses IP de sortie, des sous-réseaux, points d'interconnexion, topologie notamment pour l'accès à distance, la liste des comptes privilégiés, etc. L'ANSSI demande que ces éléments lui soient communiqués « *dans un format lu par les principaux logiciels bureautiques accessibles au public* ». Pas de Volapuk donc !

Les points suivant sont liés aux outils à mettre en place. Les OIV doivent en premier lieu s'assurer du maintien en condition de sécurité de leur système d'information d'importance vitale. Ils doivent donc s'assurer que les systèmes, hardware, logiciel, applications soient à jour en terme de sécurité et fonctionnent sur des versions stables et robustes. Par ailleurs, Ils devront se doter de capacité de gestion de logs et de comptes à privilèges pour faire de la journalisation. De même, cette journalisation devra être en lien avec un système de corrélation et d'analyse des journaux.

L'arrêté parle ensuite de la détection des incidents. La loi impose la mise en place de « *sonde d'analyse de fichiers et de protocoles* ». Des boîtes noires capables faire du DPI (Deep Packet Inspection) pour analyser le flux de données et détecter des évènements susceptibles d'affecter la

sécurité des SIIV. Ces sondes devront être qualifiées par l'ANSSI. L'agence a donc choisi le plus haut niveau de labellisation impliquant l'accès au code source. Un choix assumé par Guillaume Poupard lors du FIC 2016, qui poussait à la qualification plus lourde, mais peut-être plus efficace aussi.

Gestion des incidents et cloisonnement

Un *vademecum* sur la découverte des incidents, la gestion des alertes et des crises est ensuite donné par les arrêtés. On notera la mise en place d'un service de permanence en lien avec l'ANSSI. En cas d'attaques majeures, l'OIV dispose de moyens techniques pour circonscrire ou éviter la propagation de l'attaque. Il lui est conseillé de « *proscrire les supports de stockage amovibles, la connexion d'équipements nomades au SI, imposer un protocole de routage, filtrage réseau, blocage des échanges de fichiers, isolation du réseau, etc.* ».

Enfin, la liste se poursuit sur les questions d'identification, d'authentification, les droits d'accès, les comptes d'administrations. Les OIV devront créer des comptes individuels pour les utilisateurs et les processus accédant aux ressources des SIIV. L'authentification est assurée par un mécanisme automatique ou non basé sur un élément secret.

Toutes ses procédures s'entendent avec une règle de base, le cloisonnement des SIIV. Un point de discussion âpre avec les OIV, car les mentalités doivent changer. « *Il y a dans certains cas des impacts profonds sur les architectures réseaux qui ont fait peur. Pour nous, l'administration réseau doit être isolée des usages, sinon il y a des risques d'intrusion et d'élévation de privilèges. Cela demande de repenser ces architectures et il y a un héritage qui va devoir s'adapter progressivement* », admettait Guillaume Poupard à Monaco.

A lire aussi :

Cybersécurité : une législation de type OIV examinée aux États-Unis

Assises de la sécurité 2015 : L'Anssi couve les OIV

Crédit Photo : Matyas Reha-Shutterstock