Parole d'expert

LPM - OIV

ou comment faire d'une contrainte une opportunité

Les récents décrets d'application n°2015-350 et 351, du 27 mars 2015, relatifs à la Loi de Programmation Militaire (LPM 2014-2019), précisent les obligations et responsabilités des Opérateurs d'Importance Vitale (OIV) en matière de sécurité des Systèmes d'Information d'Importance Vitale (SIIV). La nature et l'ampleur des travaux qu'ils auront à réaliser pour se mettre en conformité seront très variables, mais ce peut être une occasion à saisir.

Un OIV est un opérateur public ou privé gérant des infrastructures dont l'indisponibilité, le dommage ou la destruction mettrait gravement en danger la sécurité de la nation ou de sa population. Établie par arrêtés ministériels, la liste des OIV – 218 à ce jour – est classée Confidentiel Défense. Si elle comporte à l'évidence les activités régaliennes de l'état, les grands acteurs de l'énergie, des transports, de la finance ou des télécommunications, elle est susceptible d'accueillir des associations ou des entreprises aux activités à risques, comme la chimie ou le traitement des déchets, notamment nucléaires. Malgré leur hétérogénéité en termes de secteur, de taille, de ressources, les OIV doivent se conformer – à leurs frais – aux mêmes obligations. Ces dernières sont prescrites dans une ou plusieurs Directives Nationale de Sécurité (DNS) émanant de son autorité administrative. L'OIV doit, par exemple, mettre en place un dispositif de détection des incidents de sécurité, afin de signaler tout incident à l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), avoir la capacité à isoler géographiquement ses systèmes, ou encore soumettre son SIIV à un audit annuel par l'ANSSI ou une société qualifiée Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI). De plus, les dispositifs techniques mis en œuvre dans les SIIV devront être qualifiés, tout comme les prestataires en charge des services associés, PDIS (Prestataire de Détection des Incidents de Sécurité) ou PRIS (Prestataires de Réponse aux Incidents de Sécurité).

De nouvelles exigences de sécurité

Étant donné le niveau de sécurité recherché, l'État souhaite étendre le contrôle à tous les maillons de la chaîne, y compris humains. Il en résulte un modèle contraignant, qu'il convient d'éclaircir. Pour un OIV, la première tâche sera d'élaborer un plan de mise en conformité. Ce Plan de Sécurité d'Opérateur (PSO) reflète la véritable politique de sécurité du SIIV, situé ou non dans un Point d'Importance Vitale (PIV), potentiellement inscrit dans une Zone d'Importance Vitale (ZIV). Le PSO, qui s'apparente à un schéma directeur, devra être validé par une commission ministérielle. La direction de l'entreprise s'engage alors sur les mesures techniques et organisationnelles qu'elle mettra en place ainsi que sur le calendrier associé, conforme au délai maximum fixé par l'arrêté relatif au secteur. Le PSO contient des mesures de protection internes (Plan Particulier de Protection), sous sa responsabilité, ou externes, définies par le préfet de département (Plan de Protection Externes).

Des enjeux de modernisation

L'accompagnement des OIV dans l'élaboration de leur PSO ou le respect de leurs exigences, notamment pour la détection des incidents, peut faire l'objet de prestations réalisées par Atos. Cependant, l'agrément par l'ANSSI est une condition nécessaire, mais pas suffisante. L'efficacité de ces missions passe par une maîtrise parfaite du contexte et du métier de l'entreprise : le type de menaces, les contraintes techniques ou organisationnelles, la nature et les technologies des systèmes à protéger, les mesures de sécurité déjà en place et leur adaptation par rapport aux contraintes réglementaires...
Dans une perspective d'amélioration, le PSO permet à l'entreprise non seulement de définir un ensemble de mesures pertinentes et économiquement proportionnées, mais aussi de réaligner sa politique de sécurité avec l'évolution des menaces et des attentes de ses parties prenantes. Pour les OIV, la mise en conformité est donc une contrainte, mais aussi l'opportunité de se moderniser, à condition de s'appuyer sur un partenaire disposant du niveau de maturité requis pour répondre aux défis techniques et, souvent, accompagner la nécessaire transition.

Nota : les modalités d'application de la LPM pour les OIV sont décrites dans l'Instruction Générale Interministérielle N°6600/SGDSN/PSE/PSN du 7 janvier 2014.

« LPM-OIV : des nouvelles exigences qui nécessitent l'assistance d'experts en cybersécurité. »

Claude Amiens,
Senior Manager Cybersécurité
Atos France

À propos d'Atos

Atos SE (Société Européenne), est un leader de services numériques avec un chiffre d'affaires annuel pro forma de l'ordre 12 milliards d'euros et environ 100 000 collaborateurs dans 72 pays. Atos fournit à ses clients du monde entier des services de conseil et d'intégration de systèmes, d'infogérance, de Big Data et de Sécurité, d'opérations Cloud et des services transactionnels par l'intermédiaire de Worldline, le leader européen des services de paiement. Grâce à son expertise technologique et sa connaissance sectorielle pointue, Atos sert des clients dans différents secteurs : Défense, Services financiers, Santé, Industrie, Médias, Services aux collectivités, Secteur Public, Distribution, Télécoms, et Transports.

Atos déploie les technologies qui accélèrent le développement de ses clients et les aident à réaliser leur vision de l'entreprise du futur. Atos est le partenaire informatique mondial des Jeux Olympiques et Paralympiques. Le Groupe est coté sur le marché Euronext Paris et exerce ses activités sous les marques Atos, Bull, Canopy, Worldline, Atos Consulting, Atos Worldgrid et Unify.

Pour plus d'informations
fr.atos.net
fr.directionmarketing@atos.net

Vision et innovation
ascent.atos.net

Suivez-nous !