Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité

NOR : *ECOP1825228A*

Le ministre de l'économie et des finances et le ministre de l'action et des comptes publics,

Vu le code de la défense, notamment ses articles L. 1141-1, R. 1143-1 (3°) et R. 1143-5 (8°) ;

Vu l'arrêté du 1er août 2016 portant approbation de la politique générale de sécurité des systèmes d'information pour les ministères économiques et financiers ;

Vu la circulaire n° 5725/SG du 17 juillet 2014 relative à la politique de sécurité des systèmes d'information de l'Etat,

Arrêtent :

Art. 1er. – Est approuvé le cahier des clauses simplifiées de cybersécurité annexé au présent arrêté.

Ce cahier des clauses n'est applicable qu'aux marchés qui s'y réfèrent.

Art. 2. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait le 18 septembre 2018.

Le ministre de l'économie et des finances,
Pour le ministre et par délégation :
Le fonctionnaire de la sécurité des systèmes d'information,
J.-P. PAPILLON

Le ministre de l'action et des comptes publics,
Pour le ministre et par délégation :
Le fonctionnaire de la sécurité des systèmes d'information,
J.-P. PAPILLON

ANNEXE

CAHIER DES CLAUSES SIMPLIFIÉES DE CYBERSÉCURITÉ

Article 1er

Champ d'application

1.1. Ce cahier de clauses simplifiées de cybersécurité (CCSC) n'est applicable qu'aux marchés qui s'y réfèrent.

1.2. Les clauses ont pour vocation d'assurer un premier cadre de sécurisation des systèmes d'information et des données associées via tout type de marché, aussi bien un marché à objet principal directement associé aux technologies de l'information et de la communication (ordinateurs, logiciels, développements ou hébergement d'application via le web) que des fournitures et services annexes (extranet de commande et service clients), ou même les simples échanges d'information par messageries électroniques.

1.3. Pour les marchés ayant un objet principal numérique comme l'externalisation d'une brique de système d'information, les présentes clauses simplifiées peuvent être complétées dans le cahier de clauses particulières du marché auquel fait écho la production par les candidats puis la contractualisation avec le titulaire d'un plan d'assurance sécurité (PAS).

Article 2

Politiques de sécurité

2.1. Les candidats et titulaires sont tenus de respecter les prescriptions des politiques de sécurité des systèmes d'information (PSSI) des bénéficiaires des marchés, dès lors que ces politiques ont été publiées avant la contractualisation des marchés, a fortiori si elles sont fournies au cours de l'appel d'offres.

2.2. Il en est de même pour les annexes techniques des PSSI dès lors qu'elles sont disponibles à première demande motivée.

2.3. Le référentiel général de sécurité (RGS) et la PSSI Etat s'appliquent aux marchés des entités couvertes par ces textes, sans qu'il soit besoin que le cahier des charges en fasse mention explicitement.

Article 3

Contrôles et audits

3.1. Durant la préparation ou la réalisation du marché, l'acheteur peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le candidat ou titulaire, et leurs sous-traitants.

3.2. Dans tous les cas, des audits légitimés par la sélection ou le suivi de titulaires de marchés peuvent être réalisés sans accord préalable dès lors que les tests et sondes respectent les conventions techniques d'usage permettant de les identifier (par exemple, User-Agent référençant une URL d'explication, reverse-DNS permettant de donner une origine claire à une adresse IP, etc).

Article 4

Documentations

4.1. Les politiques de sécurité prévoient généralement une revue formelle de sécurité appelée homologation, auquel les titulaires doivent apporter leur concours en matière de documentations et de réponses aux questions, permettant d'analyser les risques résiduels en matière de confidentialité, authentification, traçabilité, intégrité, disponibilité et résilience.

4.2. Par ailleurs, les règlementations applicables par exemple à la protection des données à caractère personnel (RGPD) ou aux données de santé prévoient la tenue de registres des traitements et la documentation des mesures de protection. Le candidat ou titulaire et leurs sous-traitants identifient proactivement les traitements de données personnelles ou sensibles et aident à la réalisation d'analyses d'impact relative à la protection des données et à la consultation préalable des autorités de contrôle.

4.3. Dans tous les cas, un titulaire de marché est tenu de fournir à première demande la documentation nécessaire à la sécurisation de leurs fournitures dans les systèmes d'information, la protection des données des bénéficiaires et aux démonstrations du respect de leurs obligations par les bénéficiaires du marché.

4.4. En particulier, la documentation explicite tous les flux échangés (entrants et sortants, applicatif mais aussi de maintenance, de statistiques, de mise à jour, d'administration distante, etc), et les dispositifs de contrôle d'accès et de maintien en condition de sécurité.

4.5. Si l'emploi sécurisé du produit ou du service nécessite des actions particulières de la part des bénéficiaires du marché, elles doivent être clairement identifiées dans un chapitre Sécurité du mode d'emploi (par exemple, la procédure de changement des mots de passe par défaut ou des interfaces exposées, de mise à jour de composants logiciels…).

Article 5

Maintien en condition de sécurité

5.1. Les politiques de sécurité convergent pour exiger les mises à jour des composants logiciels vers des versions supportées par l'éditeur ou la communauté Open Source qui les produisent. Dans ces conditions, une vérification d'aptitude au bon fonctionnement ou au service régulier (VABF et VSR) est refusée si des composants ne sont pas à jours des correctifs de failles de sécurité.

5.2. La responsabilité du maintien en condition de sécurité d'un titulaire comprend les composants et services développés en propre mais aussi ses composants et dépendances amont (librairies, cadriciels, environnement d'exploitation, API tierces) ou sous-traités.

5.3. Un candidat ou titulaire ne peut conditionner ses garanties de bon fonctionnement de fournitures ou prestations qu'il fournit à l'emploi de composants dans une version non supportée, sauf à démontrer une contrainte supérieure et proposer à ses frais des moyens de cantonner les risques, ou démontrer que les risques sont négligeables dans le contexte d'emploi.

5.4. Dans tous les cas, les unités d'œuvre portant le maintien en condition opérationnelle (labellisée MCO mais aussi tierce maintenance applicative (TMA) ou simplement hébergement) incluent le maintien en condition de sécurité et donc la mise en œuvre des correctifs de failles de sécurité.

Article 6

Signalements de sécurité

6.1. Pour les prestations, produits et services qu'ils fournissent dans le cadre du marché, les titulaires mettent à disposition des fils publics par abonnement (flux RSS, liste de diffusion par courriel) ou autre dispositif d'information dédié à la sécurité informatique. Ces fils, identifiés dans le chapitre Sécurité des modes d'emploi, permettent aux bénéficiaires d'être tenu informés en continu des événements et changements impactant la sécurité, par exemple annonce de correctif, attaque en cours, nouvelle configuration à appliquer, violation de données à caractère personnel…

6.2. Afin de garder leur pouvoir d'alerte, ces canaux de diffusion ne sont pas mélangés avec des flux commerciaux et marketing. Les fils peuvent être multiples dans le cas de fournitures en plusieurs composants mais sans laisser de vide d'information.

6.3. Réciproquement, les outils numériques mis à disposition permettent aux bénéficiaires et leurs experts en cybersécurité de signaler directement aux équipes appropriées du titulaire de possibles failles ou détournements de dispositifs de sécurité.

6.4. Afin que ces signalements soient effectifs et efficaces, les conventions d'usage en cybersécurité sont respectées (security.txt, abuse@). Dans tous les cas, il faut moins d'une minute pour trouver le point d'entrée approprié du signalement.

6.5. Après analyse partagée et vérification, le titulaire a obligation d'enregistrer les failles auprès des autorités compétentes (CERT nationaux pour les éditeurs, registres RGPD et CNIL ou équivalent pour la divulgation de données personnelles, ANSSI pour les opérateurs d'importance vitale ou de services essentiels, etc.) en suivant les réglementations établies. L'emploi d'un système de cotation connu (par exemple CVSS) permet de hiérarchiser l'urgence pour tous les acteurs en aval. A défaut d'action sous 3 mois, l'acheteur a la possibilité de se substituer aux titulaires dans les actions précédentes ou de pratiquer une divulgation responsable (annonce de la faille avec embargo pendant au moins 90 jours sur les détails techniques)

Article 7

Hébergement de données

7.1. A première demande, le candidat ou titulaire identifie tous les prestataires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.

Peuvent être exclus de cette déclaration les prestataires qui seraient dépositaires de copies chiffrées à condition que l'algorithme soit sans faille connue et que les prestataires ne soient pas en possession des clés cryptographiques.

Article 8

Sous-traitances

8.1. Les clauses de ce cahier s'appliquent aux marchés publics en incluant tous les sous-traitants. Comme les titulaires sont responsables de leurs sous-traitants, les contrôles et les éventuelles actions de remédiation en cas de défaut, y compris jusqu'au remplacement, sont donc à la charge des titulaires.

Article 9

Labels et certificats

9.1. Afin de démontrer de manière économique la réalité de leurs efforts pour sécuriser les composants impliqués dans le marché, candidats et titulaires sont invités à présenter des labels et certificats qui permettent à l'acheteur d'avoir un premier niveau d'assurance au cours de l'évaluation d'offres.

9.2. Ces qualifications peuvent parfois être globales (ISO27000), partielles (référentiel en « Tier » 1 à 4 pour l'hébergement), ou très ponctuelles (rapports de test de l'état de l'art sur des interfaces spécifiques, cf. clause ci-dessous).

Article 10

Défauts et règlement des différends

10.1. Tout au long des processus d'attribution et d'exécution d'un marché, l'acheteur et les bénéficiaires peuvent constater ou découvrir des non-conformités à la politique de sécurité de l'entité et des défauts de sécurisation.

10.2. L'entité apprécie l'enjeu du défaut eu égard à la sensibilité des données manipulées, de leurs volumes, et des conséquences prévisibles si le défaut persiste.

10.3. En fonction de cette analyse, ces défauts peuvent avoir comme conséquence le rejet d'une candidature, d'une offre, la non-validation d'aptitude au service régulier, pénalités de retard, l'ajournement, la suspension ou la résiliation des bons de commandes ou du marché.

10.4. Comme les différends peuvent être techniques et nécessiter un traitement confidentiel, le règlement des éventuelles contestations sur les décisions précitées passera systématiquement par un comité consultatif de règlement amiable.

10.5. Un comité consultatif est composé de membres qualifiés et habilités pour cette fonction, désignés au préalable ou choisis conjointement.

Article 11

Etats de l'art

11.1. La sécurisation des systèmes informatiques dépend de l'évolution des technologies. Il appartient à chaque titulaire de marché de s'aligner sur les standards et référentiels qui concernent les services qu'il propose, utilise ou met à disposition. Pour les interfaces web, les services de courriels, les appareils connectés, les sauvegardes de données et l'administration de systèmes d'information, les référentiels à retenir sont résumés ci-après et détaillés dans les textes techniques publiés sur www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi. Les respects de référentiels sont aussi vérifiés par les agences de notation en cybersécurité.

11.2. A première demande, le candidat ou titulaire fournit la conformité à ces référentiels pour les services et objets numériques qu'il inclut dans son offre de fournitures. Il précise alors les domaines concernés (interfaces web et courriels), les objets et bases d'information concernées (appareils connectés, sauvegardes de données, consoles d'administration).

11.3. Interfaces web

- Interfaces utilisables par des navigateurs à l'état de l'art (part de marché cumulée supérieure à 50%), sans générer d'alerte de sécurité.
  - sans module d'extension.
  - dans leur mode Grand public le plus protecteur (souvent appelé navigation Incognito).
- et en exploitant les techniques de protections associées.
  - connexion TLS (https) pour authentifier la source et chiffrer les communications.
  - marquage approprié des cookies ou jetons de session pour se protéger des vols ou exploitation de sessions déjà ouvertes.
  - politique de sécurité des contenus pour se protéger contre les injections de contenus actifs malicieux.
  - activation des protections des navigateurs par l'emploi d'entêtes de sécurité.
- Publication d'un point de contact via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des bonnes équipes techniques.

11.4. Services de courriels

- Authenticité des émetteurs garantie par l'émission de messages depuis des serveurs associés publiquement aux domaines, signature numérique par domaine et une politique publique liant le tout.
- Identification claire du statut des comptes émetteurs de courriels, par exemple en ajoutant un suffixe à ceux fournis aux personnels qui ne sont pas agents ou salariés directs.
- Intégrité des messages par leur signature numérique.
- Confidentialité des échanges de machines en machines, confidentialité compatible avec les obligations d'interceptions légales.
- Analyse des rapports d'anomalies via DMARC ou abuse@.

11.5. Appareils connectés

- Dispositif de lutte contre les logiciels malveillants (anti-virus, ou système de vérification et détection à base de signatures ou condensats des logiciels autorisés).
- Dispositif de mise à jour sécurisé.
- Limitation de l'exposition via les réseaux en réduisant les ports acceptant des connexions entrantes et en authentifiant les accès distants, sans faille connue (ceci exclut les connections non chiffrés TELNET, HTTP/SMTP sans TLS, et l'emploi de mots de passe génériques ou faciles à découvrir, par exemple du fait d'un hachage insuffisant).

11.6. Sauvegardes des données stockées

- Sauvegardes 3-2-1 (3 copies, 2 technologies, 1 exemplaire hors site principal, donc avec chiffrement) pour se protéger des rançongiciels, des erreurs de manipulations ou des défaillances de matériels.

11.7. Administration des systèmes d'information

- Consoles dédiées à l'exploitation et l'administration, et au minimum isolées des réseaux bureautiques et d'Internet, web et courriel notamment.
- Connexions aux machines administrées par des protocoles chiffrés, authentifiants et sans faille connue et bien configurés (VPN IPsec, TLS, ssh, RDP avec NLA).