Novembre 2021

COMMENTAIRES DE BSA | THE SOFTWARE ALLIANCE A L'ANSSI SUR LA REVISION DE SECNUMCLOUD

BSA | The Software Alliance[1] remercie l'ANSSI de l'opportunité de commenter la mise à jour du référentiel d'exigences SecNumCloud (version 3.2.a), important à la fois pour soutenir des normes de cybersécurité robustes et harmonisées pour l'ensemble de l'industrie, et pour la mise en œuvre de la nouvelle stratégie française en matière de cloud.

Le fait que SecNumCloud s'appuie, entre autres, sur des normes existantes adoptées par l'ensemble de l'industrie, qui sont internationalement reconnues, fondées sur la gestion des risques, et volontaires, telles que l'ISO/IEC 27001, permet d'évaluer les fournisseurs selon des critères reconnus basés sur des pratiques industrielles bien établies. L'utilisation de mises à jour spécifiques au cloud dans les normes ISO 27017 et 27018 contribuerait également à garantir l'interopérabilité et l'assurance de la conformité en matière de sécurité.

Cependant, le projet de référentiel (version 3.2.a) contient de nouvelles exigences liées aux provisions de localisation et à l'immunité à la législation extraterritoriale qui soulèvent des préoccupations importantes :

- D'un point de vue opérationnel, elles pourraient avoir un impact considérable sur la capacité des clients à sélectionner le prestataire de services d'informatique en nuage qui répond le mieux à leurs besoins opérationnels et qui offre les meilleures protections de cybersécurité.
- Au niveau commercial, elles pourraient augmenter considérablement le coût de la mise en conformité et de la supervision sans renforcer la sécurité : la manière dont les données sont protégées est plus importante pour leur sécurité que l'endroit où elles sont stockées.
- D'un point de vue juridique, certaines des exigences proposées soulèvent de sérieuses questions de compatibilité avec la législation européenne existante et les engagements commerciaux internationaux de la France et de l'Union Européenne.

Nous encourageons l'ANSSI à prendre en compte l'ensemble de ces aspects lors de la mise à jour de SecNumCloud. Nous soutenons que ces évolutions au niveau national devraient être alignées avec la mise en place d'un nouveau schéma de certification pour les services de cloud (EUCS) au sein de l'ENISA, tel que mandaté par le règlement 2019/881 relatif à la certification de cybersécurité des technologies de l'information et des communications (Cybersecurity Act), afin d'éviter toute nouvelle fragmentation du marché entre les États membres.

[1] BSA | The Software Alliance est le principal organisme de promotion de l'industrie du logiciel auprès des administrations gouvernementales et sur le marché international. Ses membres comptent parmi les entreprises les plus innovantes au monde, à l'origine de solutions logicielles qui stimulent l'économie et améliorent la vie moderne. Basée à Washington, DC et présente dans plus de 30 pays, BSA est pionnière en matière de programmes de conformité qui encouragent l'utilisation légale de logiciels et plaide en faveur de politiques publiques à même de promouvoir l'innovation technologique et de favoriser la croissance économique numérique.

Les BSA incluent: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

5.3. Appréciation des risques

[…]

c) Le prestataire doit prendre en compte dans l'appréciation des risques :

- *- les risques d'atteinte à la confidentialité des données des commanditaires par des tiers impliqués dans la fourniture du service (fournisseurs, sous-traitants, etc.).*

d) Le prestataire doit lister, dans un document spécifique, les risques résiduels liés à l'existence de lois extraterritoriales ayant pour objectif la collecte de données ou métadonnées des commanditaires sans leur consentement préalable.

e) Le prestataire doit mettre à la disposition du commanditaire, sur demande de celui-ci, les éléments d'appréciation des risques liés à la soumission des données du commanditaire au droit d'un état non-membre de l'Union Européenne.

Réponse de BSA au 5.3

La disposition 5.3.d fait référence à « l'existence de lois extraterritoriales ayant pour objectif la collecte de données ou métadonnées des commanditaires sans leur consentement préalable ». Cette définition des lois extraterritoriales pertinentes pour l'évaluation des risques est très large et pourrait englober de nombreuses lois qui sous-tendent l'action légitime des agences gouvernementales, y compris celle des autorités françaises.

Tout d'abord, en ce qui concerne les critères de collecte des données et des métadonnées, la définition inclurait les lois qui sous-tendent la coopération réglementaire entre la France et les États membres de l'UE et/ou les pays tiers dans des domaines tels que la concurrence, la lutte contre le blanchiment d'argent et la coopération en matière d'enquêtes criminelles.

Deuxièmement, le critère de l'application extraterritoriale concerne, en droit international public, une situation dans laquelle un État prétend appréhender, par son ordre juridique, des éléments situés en dehors de son territoire, et vice versa, en laissant s'exercer l'autorité d'un État étranger sur son propre territoire. Par définition et dans le contexte des dispositions relatives à l'évaluation des risques du cadre de référence SecNumCloud, cela s'applique aux lois de tout pays qui sont pertinentes au regard des paramètres de service du fournisseur. Par défaut, cela inclurait toute loi extraterritoriale de la France, ainsi que potentiellement des États membres de l'UE et de tout autre pays tiers pertinents.

Le couplage des deux critères signifie donc que l'évaluation des risques, telle qu'elle est actuellement rédigée, obligera les fournisseurs de services de cloud à inclure les lois de sécurité nationale, y compris la loi française sur le renseignement (référence : LOI n° 2015-912 du 24 juillet 2015 relative au renseignement) dont l'art. L. 811-2 est ainsi rédigé : « [Les services spécialisés de renseignement] ont pour mission, en France et à l'étranger, la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. »

De manière positive, cette approche évite toute discrimination à l'encontre d'un État membre de l'UE ou d'un pays tiers – une approche qui, autrement, serait sans doute incompatible avec les principes du droit européen et international et les exemptions d'ordre public applicables à la France. Aller au-delà de cette approche par liste créerait une charge supplémentaire significative à la fois pour le prestataire de services qui serait tenu d'établir une liste complète et précise, et pour l'ANSSI qui se devrait d'avoir une image complète et précise des législations extraterritoriales pertinentes en vigueur.

Cependant, l'approche choisie d'une liste à fournir par le fournisseur de services de cloud à son client engendrera une charge importante pour les fournisseurs, quelle que soit leur taille ou la localisation

de leur siège social. Elle soulèvera également des problèmes de mise en œuvre, car les fournisseurs n'ont pas un accès illimité aux données de leurs clients stockées dans leur infrastructure ou service de cloud qui leur permettrait de déterminer quelles lois extraterritoriales seraient pertinentes dans ce contexte. Il est aussi important de noter que cette proposition doit être mise en parallèle de la proposition de *Digital Services Act* et son article 7 qui vise à empêcher l'obligation de surveillance généralisée des informations que les fournisseurs de services intermédiaires transmettent ou stockent.

9.7. Restriction des accès à l'information

(d) Dans le cadre du support technique, si les actions nécessaires au diagnostic et à la résolution d'un problème rencontré par un commanditaire nécessitent un accès aux données du commanditaire, alors le prestataire doit :
(…)
- vérifier que la personne à qui l'accès doit être autorisé est localisée au sein de l'Union Européenne ;

12.13. Télédiagnostic et télémaintenance des composants de l'infrastructure

a) Dans le cadre du télédiagnostic ou de la télémaintenance de composants de l'infrastructure, considérant les risques d'atteinte à la confidentialité des données des commanditaires, alors le prestataire doit :
(…)
- vérifier que la personne à qui l'accès doit être autorisé est localisée au sein de l'Union Européenne

Réponse de BSA aux 9.7 et 12.13

Les actions visées au point 9.7.d reposent sur la possibilité pour les fournisseurs de services d'utiliser toutes leurs capacités de détection, d'analyse et d'investigation des menaces, de réponse et de résolution - indépendamment de l'endroit où se trouvent leurs collaborateurs et leurs ressources, et quelle que soit le jour et l'heure. L'assistance 24h/24, 7j/7 et 365 jours par an nécessite des ressources dans plusieurs fuseaux horaires. Restreindre cette possibilité aux personnes physiquement situées dans l'Union européenne, ou dans un pays particulier de l'UE, rendrait leur capacité d'action très difficile, voire impossible. Cela entraverait considérablement la capacité de nombreux fournisseurs, y compris ceux qui ont leur siège en Europe avec des capacités en dehors de l'UE, à tirer parti de leurs capacités mondiales et à fournir un service de premier ordre. Les mêmes considérations s'appliqueraient à l'assistance de deuxième ligne (correction du code, tests, etc.), car les données devront circuler entre le client en France et les équipes d'ingénieurs des fournisseurs de services concernés, qui peuvent être répartis dans le monde entier.

En outre, les règles commerciales internationales applicables aux dispositions relatives aux services de cloud exigent un respect des principes de non-discrimination et d'égalité de traitement en termes de nationalité des personnes, produits, services ou technologies. Sous réserve de limitations légitimes de politique publique, une règle ayant un impact sur la fourniture de services de cloud soulèverait des inquiétudes si elle faussait le marché ou modifiait les conditions de concurrence en fonction de l'origine nationale des personnes, des produits ou services, ou des technologies concernés. Dans certains cas, si les règles de transfert de données étaient conçues pour (ou résultaient à) fournir des avantages économiques aux transferts à l'intérieur des frontières d'un pays, et aux personnes nationales, à leurs produits ou services, ou à leurs technologies, par rapport à ceux accordés aux transferts transfrontaliers et aux personnes, produits, services ou technologies non nationaux, cela pourrait également soulever des questions de compatibilité avec les principes pré-cités.

Pour ces raisons, nous émettons des réserves quant à certaines exigences proposées dans le projet de référentiel SecNumCloud qui impacteraient la fourniture de services de cloud d'une manière qui

semble incompatible avec les engagements commerciaux internationaux de l'UE et de la France en matière de non-discrimination à l'égard des personnes, produits ou technologies étrangers.[2]

14.4. Environnement de développement sécurisé

a) Le prestataire doit mettre en œuvre un environnement sécurisé de développement permettant de gérer l'intégralité du cycle de développement du système d'information du service.

b) Le prestataire doit prendre en compte les environnements de développement dans l'appréciation des risques et en assurer la protection conformément au présent référentiel.

14.5. Développement externalisé

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de superviser et de contrôler l'activité de développement externalisé des logiciels et des systèmes. Cette procédure doit s'assurer que l'activité de développement externalisé soit conforme à la politique de développement sécurisé du prestataire et permette d'atteindre un niveau de sécurité du développement externe équivalent à celui d'un développement interne (voir exigence 14.1 a).

Réponse de BSA aux 14.4 et 14.5 :

Les normes et les recommandations sont des outils importants pour aider les développeurs de logiciels à évaluer et assurer la sécurité tout au long du cycle de vie des logiciels et pour guider la sécurité des logiciels indépendamment de l'environnement de développement ou de l'objectif du logiciel. Il est important d'aborder trois fonctions distinctes mais complémentaires : le développement sécurisé pour soutenir la sécurité dans la phase de développement du logiciel lorsqu'un projet est conçu, initié, développé et mis sur le marché ; les fonctionnalités pour identifier les caractéristiques de sécurité clés pour un produit logiciel ; le cycle de vie sécurisé pour maintenir la sécurité dans un produit logiciel depuis son développement jusqu'à la fin de sa vie. BSA s'attache à ce que les processus organisationnels et les capacités de sécurité des produits soient des éléments intrinsèques à la sécurité des logiciels.

BSA a développé et met régulièrement à jour son Cadre pour la Sécurité du Logiciel[3], qui offre un outil de gestion des risques axé sur les résultats de sécurité et basé sur des normes visant à soutenir les parties prenantes de l'industrie du logiciel (développeurs, vendeurs, clients, décideurs politiques et autres), leur permettant de communiquer et d'évaluer les résultats de sécurité de leurs produits et services logiciels spécifiques. Ce cadre peut être un outil de référence pertinent pour aider les fournisseurs de services à répondre aux exigences des articles 14.4 et 14.5.

19.2. Localisation des données

b) Le prestataire doit stocker et traiter les données du commanditaire au sein de l'Union Européenne.

c) Les opérations d'administration et de supervision du service doivent être réalisées depuis l'Union Européenne.

d) Le prestataire doit stocker et traiter les données techniques (identités des bénéficiaires et des administrateurs de l'infrastructure technique, données manipulées par le Software Defined Network, journaux de l'infrastructure technique, annuaire, certificats, configuration des accès, etc.) au sein de l'Union Européenne.

e) Le prestataire peut réaliser des opérations de support aux commanditaires depuis un État hors de l'Union Européenne. Il doit documenter la liste des opérations qui peuvent être effectuées par le support au commanditaire depuis un État hors de l'Union Européenne, et les mécanismes permettant d'en assurer le contrôle d'accès et la supervision depuis l'Union Européenne.

[2] Voir notamment l'Accord de commerce et de coopération entre l'Union européenne et le Royaume-Uni, Chapitre 2, Article DIGIT 6.

[3] *Voir "*BSA Framework for Secure Software" à https://www.bsa.org/reports/updated-bsa-framework-for-secure-software

Réponse de BSA au 19.2 :

L'exigence du point e) pourrait contribuer à accroître la transparence, ce que soutient BSA. Cependant, la localisation des données ou d'autres exigences très restrictives qui affectent le transfert transfrontalier des données ne feraient pas progresser les objectifs de cybersécurité (ou de protection des données personnelles) et pourraient engendrer des vulnérabilités et conséquences néfastes. La manière dont les données sont protégées est beaucoup plus importante pour la sécurité que l'endroit où elles sont stockées.

Les transferts transfrontaliers de données sont importants pour la cybersécurité pour plusieurs raisons. Les entreprises peuvent choisir de stocker des données dans des lieux géographiquement différents pour masquer l'emplacement des données et réduire le risque d'attaques physiques, pour permettre aux entreprises de réduire la latence du réseau et pour maintenir la redondance et la résilience des données critiques à la suite de dommages physiques à un lieu de stockage. En outre, les transferts de données transfrontaliers permettent aux outils de cybersécurité de surveiller les schémas de trafic, d'identifier les anomalies et de détourner les menaces potentielles grâce à l'accès mondial aux données en temps réel.

En outre, plusieurs législations européennes - dont le règlement sur la libre circulation des données et le règlement général sur la protection des données - consacrent la libre circulation des données (personnelles et non personnelles) au sein de l'UE et vers l'extérieur comme un principe fondamental du droit européen. La Cour de justice de l'UE a confirmé ce principe, en exigeant toutefois des garanties supplémentaires dans certains cas, notamment dans son arrêt Schrems II.[4]

Comme nous l'avons déjà indiqué dans notre réponse aux points 9.7 et 12.13, les exigences de localisation ou autres exigences très restrictives iraient également à l'encontre des engagements commerciaux internationaux de l'UE (et donc de la France). Ces engagements visent à garantir que, sauf exception limitée en matière de protection des données personnelles et de politique de confidentialité : *« Les flux transfrontaliers de données ne sont pas restreints entre les Parties par une Partie :*
(a) exigeant l'utilisation d'installations informatiques ou d'éléments de réseau sur le territoire de la Partie pour le traitement, y compris en imposant l'utilisation d'installations informatiques ou d'éléments de réseau qui sont certifiés ou agréés sur le territoire d'une Partie ;
(b) exigeant la localisation des données sur le territoire de la Partie pour leur stockage ou leur traitement ;
(c) en interdisant le stockage ou le traitement sur le territoire de l'autre Partie ; ou
(d) subordonnant le transfert transfrontalier de données à l'utilisation d'installations informatiques ou d'éléments de réseau sur le territoire des Parties ou à des exigences de localisation sur le territoire des Parties. »

19.6. Immunité au droit extracommunautaire
a) Le siège statutaire, administration centrale ou principal établissement du prestataire doit être établi au sein d'un Etat membre de l'Union européenne.
b) Le capital social et les droits de vote dans la société du prestataire ne doivent pas être, directement ou indirectement :
- individuellement détenus à plus de 24% ;
- et collectivement détenus à plus de 39% ;

[4] Cas C-311/18

par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d'un Etat non membre de l'Union européenne.
Ces entités tierces susmentionnées ne peuvent pas individuellement :
- en vertu d'un contrat ou de clauses statutaires, disposer d'un droit de véto ;
- en vertu d'un contrat ou de clauses statutaires, désigner la majorité des membres des organes d'administration, de direction ou de surveillance du prestataire.
c) En cas de recours par le prestataire, dans le cadre des services fournis au commanditaire, aux services d'une société tierce - y compris un sous-traitant - possédant son siège statutaire, administration centrale ou principal établissement au sein d'un Etat non membre de l'Union européenne ou appartenant ou étant contrôlée par une société tierce domiciliée en dehors l'Union européenne, cette susdite société tierce ne doit ni avoir la compétence pratique d'obtenir les données opérées au travers du service. Ces données visées sont celles qui sont confiées au prestataire par les commanditaires ainsi que toutes données techniques (identités des bénéficiaires et des administrateurs de l'infrastructure technique, données manipulées par le Software Defined Network, journaux de l'infrastructure technique, annuaire, certificats, configuration des accès, etc.) comprenant des informations sur les commanditaires. Pour les besoins du présent article, la notion de contrôle est entendue comme étant celle mentionnée au II de l'article L233-3 du Code de commerce.
e) […]

Réponse de BSA au 19.6 :

En tant que membre de l'Organisation Mondiale du Commerce, la France et l'Union européenne se sont engagées à respecter les principes fondamentaux de non-discrimination dans le traitement des personnes, produits, services et technologies étrangers. En vertu de l'article III de l'Accord général sur les tarifs douaniers et le commerce (GATT), la France et l'UE se sont engagées à ne pas accorder un traitement moins favorable aux produits importés par rapport aux produits nationaux. De même, en vertu de l'article 17 de l'Accord général sur le commerce des services (AGCS), la France et l'UE se sont engagées à ne pas accorder un traitement moins favorable aux services et fournisseurs de services non nationaux par rapport au traitement qu'elles accordent aux services et fournisseurs de services nationaux. Entre autres secteurs, ces dernières obligations de non-discrimination s'appliquent spécifiquement à tous les "services informatiques et services connexes ;" en d'autres termes, la France n'a pas stipulé de réserves ou d'exceptions à ses engagements de non-discrimination et d'accès au marché relatifs aux services et fournisseurs de services de cloud étrangers, ainsi qu'à tous les autres services informatiques. En conséquence, plusieurs aspects de la section 19.6 (y compris l'établissement local, les limitations du capital et des droits de vote, et les stipulations relatives au personnel de supervision) semblent contrevenir aux engagements de la France d'accorder aux prestataires de services étrangers un accès complet et sans restriction au marché du point de vue transfrontalier (Mode 1) et du point de vue de la présence commerciale (Mode 3) en ce qui concerne tous les services informatiques et connexes.[5] Dans des différends soumis à l'OMC, des panels de l'OMC ont constaté que des exigences très similaires à celles de la section 19.6 violaient les engagements de l'OMC et devaient être modifiées.[6]

Le point 19.6.b) semble également être un critère discriminatoire sans base juridique. Il violerait les règles de l'UE telles que la directive 2014/24 sur la passation des marchés publics et l'article 14 de la directive 2006/123/CE relative aux services dans le marché intérieur qui interdit expressément toute restriction fondée sur la détention du capital social. Elle violerait également les règles internationales en matière de marchés publics telles que l'Accord multilatéral sur les marchés publics, rendant

[5] *Voir* Union Européenne, Listes d'engagements spécifiques, GATS/SC/157, "Services informatiques et services connexes," p. 63-68., à : https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/SCHD/GATS-SC/SC157.pdf&Open=True
[6] *Voir notamment,* Chine — Mesures affectant les droits de commercialisation et les services de distribution pour certaines publications et certains produits de divertissement audiovisuels, DS363, AB/R (21 décembre 2009) à : https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=R:/WT/DS/363ABR.pdf&Open=True

SecNumCloud hautement contestable devant les tribunaux. Dans la pratique, les sociétés cotées en bourse ont également un contrôle et une connaissance limités de la composition de leur actionnariat, précisément en raison de la structure d'actionnariat, qui est également susceptible d'évoluer continuellement dans le temps. Le point 19.6.b crée une charge supplémentaire pour les sociétés cotées en bourse - qu'elles soient cotées en France, dans l'UE au sens large et/ou dans des pays tiers - de contrôler l'actionnariat de leurs actions. Cette exigence apparaît également en contradiction avec les lois sur la transparence des marchés de capitaux qui imposent des obligations de transparence aux actionnaires.

Pour plus information:
Isabelle Roccia, Director Policy – EMEA
isabeller@bsa.org