RÈGLEMENT D'EXÉCUTION (UE) 2018/151 DE LA COMMISSION

du 30 janvier 2018

portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union [1], et notamment son article 16, paragraphe 8,

considérant ce qui suit:

(1) Conformément à la directive (UE) 2016/1148, les fournisseurs de service numérique restent libres de prendre les mesures techniques et organisationnelles qu'ils jugent appropriées et proportionnées pour gérer les risques qui menacent la sécurité de leurs réseaux et systèmes d'information, pour autant que ces mesures garantissent un niveau de sécurité approprié et tiennent compte des éléments prévus dans ladite directive.

(2) Lors de la définition des mesures techniques et organisationnelles appropriées et proportionnées, le fournisseur de service numérique devrait aborder la sécurité de l'information de manière systématique, selon une approche fondée sur les risques.

(3) Afin d'assurer la sécurité des systèmes et des installations, les fournisseurs de service numérique devraient appliquer des procédures d'évaluation et d'analyse. Ces activités devraient concerner la gestion systématique des réseaux et des systèmes d'information, la sécurité physique et environnementale, la sécurité de l'approvisionnement et le contrôle de l'accès.

(4) Lorsqu'ils effectuent une analyse des risques dans le cadre de la gestion systématique des réseaux et des systèmes d'information, les fournisseurs de service numérique devraient être encouragés à repérer les risques spécifiques et à quantifier leur importance, par exemple en établissant quelles sont les menaces pour les actifs essentiels et comment elles pourraient affecter les activités, et en déterminant les meilleurs moyens d'atténuer ces risques en fonction des capacités existantes et des ressources nécessaires.

(5) Les stratégies en matière de ressources humaines pourraient avoir trait à la gestion des compétences, y compris aux aspects liés à la sensibilisation et au développement des compétences dans le domaine de la sécurité. Lorsqu'ils décident d'un ensemble approprié de politiques relatives à la sécurité de fonctionnement, les fournisseurs de service numérique devraient être encouragés à tenir compte des aspects de gestion du changement, de gestion de la vulnérabilité, de formalisation des pratiques opérationnelles et administratives et de cartographie du système.

(6) Les politiques sur l'architecture de la sécurité pourraient prévoir en particulier la séparation des réseaux et des systèmes ainsi que des mesures de sécurité spécifiques aux opérations critiques telles que les activités d'administration. La séparation des réseaux et des systèmes pourrait permettre à un fournisseur de service numérique de distinguer les éléments tels que les flux de données et les ressources informatiques qui appartiennent à un client, un groupe de clients, le fournisseur de service numérique ou des tiers.

(7) Les mesures prises en ce qui concerne la sécurité physique et environnementale devraient protéger la sécurité des réseaux et des systèmes d'information des organisations contre les dommages causés par des incidents tels que vol, incendie, inondation ou autres conditions météorologiques, pannes de télécommunications ou de courant.

(8) La sécurité de l'approvisionnement en électricité, en combustible ou en agents de refroidissement pourrait englober la chaîne d'approvisionnement qui comprend, en particulier, la sécurité des tiers contractants et sous-traitants et leur gestion. La traçabilité des produits indispensables a trait à la capacité du fournisseur de service numérique d'identifier et d'enregistrer les sources de ces produits.

(9) Les utilisateurs de services numériques devraient englober les personnes physiques ou morales qui sont des clients ou des abonnés d'un marché en ligne ou d'un service informatique en nuage, ou qui sont les visiteurs d'un moteur de recherche en ligne souhaitant effectuer des recherches par mots clés.

[1] JO L 194 du 19.7.2016, p. 1.

(10) Lorsqu'il s'agit de déterminer l'importance de l'impact d'un incident, les cas figurant dans le présent règlement devraient être considérés comme une liste non exhaustive des incidents significatifs. Des enseignements devraient être tirés de la mise en œuvre du présent règlement et des travaux menés par le groupe de coopération en ce qui concerne la collecte d'informations sur les bonnes pratiques en matière de risques et d'incidents et les discussions sur les modalités de signalement des incidents conformément aux points (i) et (m) de l'article 11, paragraphe 3, de la directive (UE) 2016/1148. Le résultat pourrait en être des lignes directrices globales sur des seuils quantitatifs pour les paramètres de notification, qui peuvent déclencher l'obligation de notification pour les fournisseurs de service numérique au titre de l'article 16, paragraphe 3, de la directive (UE) 2016/1148. Le cas échéant, la Commission pourrait également envisager de revoir les seuils actuellement prévus par le présent règlement.

(11) Afin de permettre aux autorités compétentes d'être informées des nouveaux risques potentiels, les fournisseurs de service numérique devraient être encouragés à signaler volontairement tout incident dont ils ignoraient précédemment les caractéristiques, tels les nouveaux exploits, vecteurs d'attaque ou auteurs de menaces, vulnérabilités et risques.

(12) Le présent règlement est applicable le jour suivant l'expiration du délai fixé pour la transposition de la directive (UE) 2016/1148.

(13) Les mesures prévues par le présent règlement sont conformes à l'avis du comité de la sécurité des réseaux et des systèmes d'information visé à l'article 22 de la directive (UE) 2016/1148,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet

Le présent règlement précise les éléments à prendre en compte par les fournisseurs de service numérique lorsqu'ils définissent et prennent des mesures visant à assurer un niveau de sécurité des réseaux et des systèmes d'information qu'ils utilisent pour proposer les services visés à l'annexe III de la directive (UE) 2016/1148. Il précise également les paramètres à prendre en compte pour déterminer si un incident a un impact significatif sur la fourniture de ces services.

Article 2

Éléments de sécurité

1. La sécurité des systèmes et des installations visés à l'article 16, paragraphe 1, point a), de la directive (UE) 2016/1148 est la sécurité des réseaux et des systèmes d'information et de leur environnement physique et comprend les éléments suivants:

a) la gestion systématique des réseaux et des systèmes d'information, c'est-à-dire une cartographie des systèmes d'information et la définition d'un ensemble de politiques appropriées sur la gestion de la sécurité de l'information, y compris l'analyse des risques, les ressources humaines, la sécurité des opérations, l'architecture de la sécurité, les données sécurisées et la gestion du cycle de vie du système et, le cas échéant, le cryptage et sa gestion;

b) la sécurité physique et environnementale, c'est-à-dire la disponibilité d'un ensemble de mesures destinées à protéger la sécurité du réseau et des systèmes d'information des fournisseurs de service numérique contre les dommages par le recours à une approche globale des risques englobant par exemple les défaillances du système, l'erreur humaine, les actes malveillants ou les phénomènes naturels;

c) la sécurité de l'approvisionnement, c'est-à-dire la mise en place et le maintien de politiques appropriées afin d'assurer l'accessibilité et, le cas échéant, la traçabilité des produits indispensables à la fourniture des services;

d) le contrôle de l'accès aux réseaux et systèmes d'information, c'est-à-dire la disponibilité d'une série de mesures visant à garantir que l'accès physique et logique aux réseaux et aux systèmes d'information, y compris la sécurité administrative de ceux-ci, est autorisé et limité en fonction d'exigences commerciales et de sécurité;

2. En ce qui concerne la gestion des incidents visée à l'article 16, paragraphe 1, point b), de la directive (UE) 2016/1148, les mesures prises par le fournisseur de service numérique comprennent:

a) des processus et procédures de détection maintenus et contrôlés afin d'assurer en temps voulu la bonne connaissance des événements anormaux;

b) des processus et politiques sur le signalement des incidents et sur les faiblesses et vulnérabilités décelées dans son système d'information;

c) une réponse conforme aux procédures établies et la communication des résultats des mesures prises;

d) une évaluation de la gravité de l'incident, documentant les connaissances issues de l'analyse de l'incident et la collecte d'informations pertinentes pouvant servir de preuves et soutenir un processus d'amélioration continue.

3. La gestion de la continuité des activités, visée à l'article 16, paragraphe 1, point c), de la directive (UE) 2016/1148 est la capacité d'une organisation à maintenir ou, le cas échéant, rétablir la prestation de services à des niveaux acceptables et préalablement définis après un incident disruptif. Elle comprend les éléments suivants:

a) la mise en place et l'utilisation de plans d'urgence, sur la base d'une analyse des répercussions sur l'activité, pour assurer la continuité des services fournis par les fournisseurs de service numérique, qui doivent être évalués et testés régulièrement, par exemple au moyen d'exercices;

b) des dispositifs de rétablissement après sinistre qui doivent être évalués et testés régulièrement, par exemple au moyen d'exercices.

4. Le suivi, l'audit et le contrôle visés à l'article 16, paragraphe 1, point d), de la directive (UE) 2016/1148 incluent la création et le maintien de politiques dans les domaines suivants:

a) la réalisation d'une séquence planifiée d'observations ou de mesures afin de vérifier si les réseaux et les systèmes d'information fonctionnent comme prévu;

b) l'inspection et la vérification afin de vérifier si une norme ou un ensemble de lignes directrices est suivi, si les rapports sont exacts, et si les objectifs d'efficacité et d'efficience sont atteints;

c) un processus destiné à révéler les failles dans les mécanismes de sécurité d'un réseau et d'un système informatique, qui protègent les données et maintiennent la fonctionnalité de la manière prévue. Ce processus inclut des procédés techniques et du personnel participant à l'exploitation.

5. Les normes internationales visées à l'article 16, paragraphe 1, point e), de la directive (UE) 2016/1148 sont les normes adoptées par un organisme international de normalisation tel que visé à l'article 2, paragraphe 1, point a), du règlement (UE) nº 1025/2012 du Parlement européen et du Conseil ([1]). Conformément à l'article 19 de la directive (UE) 2016/1148, des normes européennes ou internationalement reconnues et des spécifications pertinentes pour la sécurité des réseaux et des systèmes d'information, y compris des normes nationales existantes, peuvent également être utilisées.

6. Les fournisseurs de service numérique veillent à mettre la documentation adéquate à la disposition de l'autorité compétente afin que cette dernière puisse vérifier le respect des éléments de sécurité énumérés aux paragraphes 1, 2, 3, 4 et 5.

Article 3

Paramètres à prendre en compte pour déterminer si l'impact d'un incident est significatif

1. En ce qui concerne le nombre d'utilisateurs touchés par un incident, en particulier ceux qui recourent au service pour la fourniture de leurs propres services, visé à l'article 16, paragraphe 4, point a), de la directive (UE) 2016/1148, le fournisseur de service numérique est en mesure de procéder à une estimation de l'une des deux manières suivantes:

a) le nombre de personnes physiques et morales affectées avec lesquelles un contrat de prestation de service a été conclu; ou

b) le nombre d'utilisateurs affectés ayant utilisé le service sur la base, notamment, de précédentes données relatives au trafic.

2. La durée de l'incident visée à l'article 16, paragraphe 4, point b), est la période qui s'écoule entre la perturbation de la bonne prestation du service en termes de disponibilité, d'authenticité, d'intégrité ou de confidentialité jusqu'au moment de son rétablissement.

3. En ce qui concerne la portée géographique eu égard à la zone touchée par l'incident visée à l'article 16, paragraphe 4, point c), de la directive (UE) 2016/1148, le fournisseur de service numérique est en mesure de déterminer si l'incident affecte la fourniture de ses services dans des États membres donnés.

4. La gravité de la perturbation du fonctionnement du service visée à l'article 16, paragraphe 4, point d), de la directive (UE) 2016/1148 est mesurée en fonction d'une ou plusieurs des caractéristiques suivantes affectées par un incident: la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou des services connexes.

([1]) Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

5. En ce qui concerne l'ampleur de l'impact sur les fonctions économiques et sociétales visée à l'article 16, paragraphe 4, point e), de la directive (UE) 2016/1148, le fournisseur de service numérique est en mesure de déterminer, sur la base d'indications telles que la nature de ses relations contractuelles avec le client ou, le cas échéant, le nombre potentiel d'utilisateurs touchés, si l'incident a causé d'importants préjudices matériels ou moraux aux utilisateurs, notamment en ce qui concerne la santé, la sécurité ou les dommages causés aux biens.

6. Aux fins des paragraphes 1, 2, 3, 4 et 5, le fournisseur de service numérique ne doit pas être tenu de recueillir des informations supplémentaires auxquelles il n'a pas accès.

Article 4

Impact significatif d'un incident

1. Un incident est considéré comme ayant un impact significatif si au moins l'une des situations suivantes s'est présentée:

a) le service fourni par un fournisseur de service numérique a été indisponible pendant plus de 5 000 000 heures-utilisateur, une heure-utilisateur correspondant au nombre d'utilisateurs affectés dans l'Union pendant une durée de soixante minutes;

b) l'incident a entraîné une perte de l'intégrité, de l'authenticité ou de la confidentialité des données stockées, transmises ou transformées ou des services connexes offerts ou accessibles par l'intermédiaire d'un réseau et d'un système informatique du fournisseur de service numérique, qui a touché plus de 100 000 utilisateurs dans l'Union;

c) l'incident a engendré un risque pour la sécurité ou la sûreté publiques ou a entraîné un décès;

d) l'incident a causé un préjudice matériel à au moins un utilisateur dans l'Union dès lors que le préjudice causé à cet utilisateur dépasse 1 000 000 EUR.

2. Compte tenu des meilleures pratiques recueillies par le groupe de coopération dans l'exercice des tâches qui lui sont confiées par l'article 11, paragraphe 3, de la directive (UE) 2016/1148 et des discussions visées à l'article 11, paragraphe 3, point m), de ladite directive, la Commission peut revoir les seuils fixés au paragraphe 1.

Article 5

Entrée en vigueur

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

2. Il est applicable à compter du 10 mai 2018.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 30 janvier 2018.

Par la Commission

Le président

Jean-Claude JUNCKER