COMMISSION
EUROPÉENNE

Bruxelles, le 13.9.2017
C(2017) 6100 final

RECOMMANDATION DE LA COMMISSION

du 13.9.2017

sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs

RECOMMANDATION DE LA COMMISSION

du 13.9.2017

sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292,

considérant ce qui suit:

(1) Le recours aux technologies de l'information et de la communication et la dépendance à l'égard de ces technologies sont désormais des aspects fondamentaux dans tous les secteurs d'activité économique, eu égard à l'interconnexion et à l'interdépendance sans précédent de nos entreprises et de nos citoyens par-delà les secteurs et les frontières. La survenance d'un incident lié à la cybersécurité touchant des organismes implantés dans plusieurs États membres, voire dans toute l'Union, et risquant de perturber gravement le marché intérieur et, plus généralement, les réseaux et les systèmes d'information sur lesquels reposent l'économie, la démocratie et la société dans l'Union est un scénario auxquels les États membres et les institutions de l'UE doivent être bien préparés.

(2) Un tel incident peut se muer en crise à l'échelle de l'Union lorsque les perturbations qu'il provoque dépassent les capacités d'action du seul État membre concerné ou lorsqu'il frappe plusieurs État membres en s'accompagnant de répercussions techniques et politiques si vastes qu'il requiert une coordination et une réaction rapides à l'échelle politique dans l'Union.

(3) Étant donné que les incidents de cybersécurité peuvent déclencher une crise plus large et toucher des secteurs d'activité autres que les seuls réseaux et systèmes d'information et de communication, la réaction qui s'impose, quelle qu'elle soit, doit comprendre des mesures d'atténuation tant intérieures qu'extérieures au cyberespace.

(4) Les incidents liés à la cybersécurité sont imprévisibles et surviennent et évoluent souvent dans des délais très courts, de sorte que leurs victimes et les entités chargées d'y répondre et d'en atténuer les effets doivent coordonner rapidement leur réaction. De plus, les incidents liés à la cybersécurité ne se limitent pas à une zone géographique déterminée et peuvent survenir simultanément ou se répandre instantanément dans un grand nombre de pays.

(5) L'efficacité de la réaction aux incidents et crises de cybersécurité majeurs à l'échelle de l'UE suppose une coopération rapide et efficace entre toutes les parties concernées et dépend de l'état de préparation et des capacités des divers États membres, auxquels s'ajoute une action conjointe et coordonnée s'appuyant sur les capacités de l'Union. La rapidité et l'efficacité des réactions aux incidents sont donc tributaires de l'existence de procédures et de mécanismes de coopération préalablement établis et, dans la mesure du possible, bien éprouvés, dans le cadre desquels des responsabilités et des rôles précis sont assignés aux principaux acteurs aux niveaux national et européen.

(6) Dans ses conclusions[1] du 27 mai 2011 sur la protection des infrastructures d'information critiques, le Conseil a invité les États membres de l'Union à «renforcer la collaboration entre les États membres et contribuer, en s'appuyant sur l'expérience acquise et les résultats obtenus au niveau national en matière de gestion de crise et en coopération avec l'ENISA, à la mise au point de mécanismes de coopération européens en cas d'incident informatique, qui devront être mis à l'épreuve dans le cadre du prochain exercice "CyberEurope" en 2012».

(7) La communication de 2016 intitulée «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité»[2] encourageait les États membres à tirer le meilleur parti possible des mécanismes de coopération prévus par la directive SRI[3] et à renforcer la coopération transfrontalière en matière de préparation à un cyberincident de grande ampleur. Elle précisait, en outre, qu'une approche coordonnée de la coopération en cas de crise entre les différents éléments du cyberécosystème, qui serait définie dans un «plan d'action», améliorerait la préparation et que ce plan d'action devrait également garantir des synergies et une cohérence avec les mécanismes existants de gestion des crises.

(8) Dans les conclusions du Conseil[4] relatives à la communication précitée, les États membres ont appelé la Commission à proposer un plan aux organes prévus par la directive SRI et aux autres parties prenantes. Or la directive SRI ne prévoit pas de cadre de coopération à l'échelle de l'Union pour parer aux incidents et crises de cybersécurité majeurs.

(9) La Commission a procédé à des consultations avec les États membres à l'occasion de deux ateliers distincts qui ont eu lieu les 5 avril et 4 juillet 2017, en présence de représentants des centres de réponse aux incidents de sécurité informatique (CSIRT) des États membres, du groupe de coopération institué par la directive SRI et du groupe horizontal «Questions liées au cyberespace» du Conseil, ainsi que de représentants du Service européen pour l'action extérieure (SEAE), de l'ENISA, d'Europol/EC3 et du secrétariat général du Conseil (SGC).

(10) Le plan d'action pour une réaction coordonnée aux incidents et crises de cybersécurité majeurs au niveau de l'Union, annexé à la présente recommandation, est la résultante des consultations évoquées ci-dessus et complète la communication «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité».

(11) Il énonce et décrit les objectifs et les modalités de la coopération entre les États membres et les institutions, organes, bureaux et agences de l'UE (ci-après les «institutions de l'UE») dans les réactions aux incidents et aux crises de cybersécurité majeurs et explique comment les mécanismes de gestion de crise existants peuvent exploiter pleinement les structures existantes en matière de cybersécurité à l'échelle de l'UE.

(12) Dans un scénario de crise de cybersécurité au sens du considérant (2), la coordination de la réaction de l'Union au niveau politique s'effectuera au sein du Conseil en

---

1 Conclusions du Conseil sur la protection des infrastructures d'information critiques «Réalisations et prochaines étapes: vers une cybersécurité mondiale», document 10299/11, Bruxelles, le 27 mai 2011.

2 COM(2016) 410 final du 5 juillet 2016.

3 Directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union («directive SRI»).

4 Document 14540/16, 15 novembre 2016.

recourant au dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR)[5], tandis que la Commission fera appel au processus transsectoriel de haut niveau ARGUS[6] pour la coordination en cas de crise. Si la crise comporte d'importantes implications liées à la politique extérieure ou à la politique de sécurité et de défense commune (PSDC), le système de réponse aux crises (SRC)[7] du Service européen pour l'action extérieure (SEAE) sera activé.

(13) Dans certains domaines, des mécanismes sectoriels de gestion des crises à l'échelon de l'UE prévoient une coopération en cas d'incident ou de crise de cybersécurité. Ainsi, dans le cadre du système mondial de navigation par satellite (GNSS) européen, la décision 2014/496/PESC du Conseil du 22 juillet 2014 sur les aspects du déploiement, de l'exploitation et de l'utilisation du système mondial de navigation par satellite européen portant atteinte à la sécurité de l'Union européenne définit déjà les rôles respectifs du Conseil, du haut représentant, de la Commission, de l'Agence du GNSS européen et des États membres dans le cadre de la chaîne de responsabilités opérationnelles mise en place afin de réagir à la menace pesant sur l'Union, sur les États membres et sur le GNSS, y compris en cas de cyberattaque. Il convient, dès lors, que la présente recommandation respecte ces mécanismes.

(14) C'est aux États membres qu'il appartient au premier chef de répondre aux incidents et crises de cybersécurité majeurs qui les touchent. Un rôle important est néanmoins dévolu à la Commission, au haut représentant et aux autres institutions ou services de l'UE, qui découle du droit de l'Union ou du fait que les incidents et les crises liés à la cybersécurité peuvent avoir une incidence sur tous les pans de l'activité économique au sein du marché unique, sur la sécurité et les relations internationales de l'Union ainsi que sur les institutions elles-mêmes.

(15) Au niveau de l'Union, les acteurs clés qui interviennent dans les réactions aux crises comprennent les structures et mécanismes nouvellement créés en vertu de la directive SRI, à savoir le réseau des centres de réponse aux incidents de sécurité informatique (CSIRT), ainsi que les agences et organismes concernés, à savoir l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), le Centre européen de lutte contre la cybercriminalité au sein d'Europol (Europol/EC3), le Centre d'analyse du renseignement de l'UE (INTCEN), la direction «Renseignement» de l'État-major de l'UE (EUMS INT) et la salle de veille (SITROOM) coopérant dans le cadre de la SIAC (capacité unique d'analyse du renseignement), la cellule de fusion de l'UE contre les menaces hybrides (au sein de l'INTCEN), l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'UE (CERT-UE) et le Centre de coordination de la réaction d'urgence de la Commission européenne.

(16) La coopération entre les États membres pour répondre aux incidents de cybersécurité au niveau technique est assurée par le réseau des CSIRT institué par la directive SRI. L'ENISA assure le secrétariat du réseau et appuie activement la coopération entre les CSIRT.Les CSIRT nationaux et la CERT-UE coopèrent et échangent des informations sur une base volontaire, y compris, le cas échéant, pour répondre à des incidents de sécurité qui touchent un ou plusieurs États membres. À la demande du représentant du

---

5 Pour plus d'informations, voir le point 3.1 de l'appendice «Gestion des crises, mécanismes de coopération et acteurs au niveau de l'UE».

6 Ibid.

7 Ibid.

CSIRT d'un État membre, ils peuvent discuter et, si possible, identifier une réponse coordonnée à un incident identifié qui relève de la juridiction de ce même État membre. Les procédures applicables seront définies dans les procédures opératoires standard (POS)[8] du réseau des CSIRT.

(17) Le réseau des CSIRT est également chargé de débattre, d'étudier et d'identifier d'autres formes de coopération opérationnelle, notamment en rapport avec les catégories de risques et d'incidents, les alertes précoces, l'assistance mutuelle, les principes et modalités d'une coordination lorsque les États membres réagissent à des risques et incidents transfrontaliers.

(18) Le groupe de coopération institué par l'article 11 de la directive SRI est chargé de fournir des orientations stratégiques pour les activités du réseau des CSIRT, de discuter des capacités et de l'état de préparation des États membres et, à titre volontaire, d'évaluer les stratégies nationales en matière de sécurité des réseaux et des systèmes d'information et l'efficacité des CSIRT, ainsi que d'identifier les bonnes pratiques.

(19) Un volet spécifique des travaux du groupe de coopération consiste actuellement à élaborer des lignes directrices en matière de notification d'incidents, conformément à l'article 14, paragraphe 7, de la directive SRI, relatives aux circonstances dans lesquelles les opérateurs de services essentiels sont tenus de notifier les incidents en vertu de l'article 14, paragraphe 3, ainsi que la forme et les modalités de ces notifications[9].

(20) Pour pouvoir opérer des choix éclairés, il est indispensable d'acquérir, par des rapports, des évaluations, des recherches, des enquêtes et des analyses, une connaissance et une compréhension de la situation en temps réel, de l'état des capacités de réaction aux risques et des menaces. L'appréciation de la situation et ce, par toutes les parties concernées, est essentielle pour permettre une réaction coordonnée efficace. Cette appréciation de la situation intègre des éléments relatifs aux causes ainsi qu'aux conséquences et à l'origine de l'incident. Il est admis qu'elle dépend de l'échange et du partage d'informations entre les parties concernées effectués dans un format approprié, selon une taxonomie commune pour décrire l'incident et d'une manière suffisamment sécurisée.

(21) Les réactions aux incidents de cybersécurité peuvent prendre de nombreuses formes, comprenant la recherche de mesures techniques pouvant nécessiter la collaboration de plusieurs entités pour enquêter sur les causes techniques de l'incident (par exemple, analyse de logiciels malveillants) ou la recherche de moyens permettant aux organisations de vérifier si elles ont été touchées (par exemple, indicateurs de compromis), mais aussi des décisions pratiques sur l'application de ces mesures et, à l'échelon politique, la décision de recourir ou non à d'autres instruments, comme le cadre pour une réponse conjointe face aux actes de cybermalveillance[10] ou le protocole opérationnel de l'UE de lutte contre les menaces hybrides[11], selon l'incident.

---

8 En cours d'élaboration; adoption prévue avant la fin de 2017.

9 Les lignes directrices devraient être finalisées avant la fin de 2017.

10 Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance («boîte à outils cyberdiplomatique»), document 9916/17.

11 Document de travail conjoint des services, Protocole opérationnel de l'UE de lutte contre les menaces hybrides («EU Playbook»), SWD(2016) 227 final, 5.7.2016.

(22) La confiance des entreprises et des citoyens européens dans les services numériques est essentielle à la prospérité du marché unique numérique. Par conséquent, la communication de crise joue un rôle particulièrement important dans l'atténuation des effets négatifs des incidents et des crises de cybersécurité. La communication peut également être utilisée, dans le contexte du cadre pour une réponse diplomatique conjointe, pour influencer le comportement des agresseurs (potentiels) qui agissent depuis des pays tiers. Il est essentiel, en vue d'une réaction politique efficace, d'harmoniser la communication publique destinée à atténuer les incidents et les crises de cybersécurité et la communication publique destinée à influencer l'agresseur.

(23) La fourniture d'informations au public sur les moyens d'atténuer les effets d'un incident au niveau de l'utilisateur ou de l'organisation (par exemple, en appliquant des corrections informatiques ou en prenant des mesures supplémentaires pour éviter la menace, etc.) pourrait être une mesure efficace pour atténuer un incident ou une crise de cybersécurité majeurs.

(24) Par l'intermédiaire de l'infrastructure de services numériques pour la cybersécurité, qui relève du mécanisme pour l'interconnexion en Europe (MIE), la Commission élabore actuellement un mécanisme de coopération sous la forme d'une plateforme de services centrale, appelé MeliCERTes, entre les CSIRT des États membres participants afin d'améliorer leur niveau de préparation, de coopération et de réaction aux menaces et incidents émergents dans le cyberespace. Par des appels à propositions concurrentiels pour l'attribution de subventions au titre du MIE, la Commission cofinance les CSIRT dans les États membres en vue d'améliorer leurs capacités opérationnelles au niveau national.

(25) Les exercices de cybersécurité au niveau de l'UE sont essentiels pour stimuler et améliorer la coopération entre les États membres et le secteur privé. À cette fin, l'ENISA organise régulièrement depuis 2010 des exercices paneuropéens de simulation de cyberincidents («Cyber Europe»).

(26) Dans ses conclusions[12] sur la mise en œuvre de la déclaration commune du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du Traité de l'Atlantique Nord, le Conseil appelle à renforcer la coopération en matière de cyberexercices, par une participation réciproque des services aux exercices respectifs, notamment Cyber Coalition et Cyber Europe.

(27) L'évolution constante de la nature des menaces et les incidents de cybersécurité survenus récemment trahissent une augmentation du risque auquel l'Union est confrontée, et les États membres devraient donner suite à la présente recommandation dans les plus brefs délais et, en tout état de cause, avant la fin de 2018.

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

(1) Les États membres et les institutions de l'UE devraient créer un cadre de l'UE pour la réaction aux crises de cybersécurité qui intègre les objectifs et les modalités de la coopération présentés dans le plan d'action en suivant les principes directeurs décrits dans ce document.

(2) Le cadre de l'UE pour la réaction aux crises de cybersécurité devrait notamment désigner les acteurs, institutions de l'UE et autorités des États membres concernés, à tous les niveaux requis, à savoir technique, opérationnel, stratégique/politique, et

[12] Document ST 15283/16 du 6 décembre 2016.

élaborer, en tant que de besoin, des procédures opératoires standard décrivant la manière dont ils coopèrent dans le contexte des mécanismes de gestion de crise de l'UE. Il faut s'attacher en particulier à organiser sans retard l'échange d'informations et à coordonner les réactions lors des incidents et des crises de cybersécurité majeurs.

(3) À cette fin, il convient que les autorités compétentes des États membres travaillent ensemble au développement des protocoles de partage d'informations et de coopération. Le groupe de coopération devrait procéder à des échanges d'expériences sur ces questions avec les institutions concernées de l'UE.

(4) Les États membres devraient veiller à ce que leurs mécanismes nationaux de gestion de crise prennent en charge de manière satisfaisante la réaction aux cyberincidents et prévoient les procédures de coopération nécessaires au niveau de l'UE dans le contexte du cadre de l'UE.

(5) En ce qui concerne les mécanismes de gestion de crise existants de l'UE, conformément au plan d'action, les États membres devraient établir, avec les services de la Commission et le SEAE, des lignes directrices pratiques en ce qui concerne l'intégration de leurs entités et procédures nationales en matière de gestion de crise et de cybersécurité dans les mécanismes de gestion de crise de l'UE, à savoir l'IPCR et le CRM du SEAE. Les États membres devraient notamment veiller à ce que des structures appropriées soient mises en place pour permettre un flux d'informations efficace entre leurs autorités de gestion de crise nationales et leurs représentants au niveau de l'UE dans le contexte des mécanismes de crise de l'UE.

(6) Les États membres devraient faire pleinement usage des possibilités offertes par le programme du mécanisme pour l'interconnexion en Europe (MIE) relatif aux infrastructures de services numériques (DSI) dans le domaine de la cybersécurité et coopérer avec la Commission pour que le mécanisme de coopération sous forme de plateforme de services centrale, qui est actuellement en cours d'élaboration, présente les fonctionnalités requises et réponde à leurs besoins de coopération également lors des crises de cybersécurité.

(7) Les États membres, avec l'aide de l'ENISA et en s'appuyant sur les travaux déjà réalisés dans ce domaine, devraient coopérer pour élaborer et adopter une taxonomie et un modèle communs pour les rapports de situation devant décrire les causes techniques et les incidences des incidents liés à la cybersécurité, de manière à renforcer leur coopération technique et opérationnelle en cas de crise. À cet égard, les États membres devraient tenir compte des travaux en cours au sein du groupe de coopération en ce qui concerne les lignes directrices en matière de notification d'incidents, et notamment les aspects liés au format des notifications nationales.

(8) Les procédures définies dans le cadre devraient être testées et, au besoin, révisées en fonction des enseignements tirés de la participation des États membres aux exercices de cybersécurité aux niveaux national, régional et de l'Union, ainsi qu'aux exercices cyberdiplomatiques et de l'OTAN. Elles devraient notamment être mises à l'épreuve dans le contexte des exercices «CyberEurope» organisés par l'ENISA. CyberEurope 2018 sera la première occasion de procéder à de tels essais.

(9) Les États membres et les institutions de l'UE devraient s'exercer régulièrement pour affûter leur réaction aux incidents et aux crises de cybersécurité majeurs à l'échelon national et européen, y compris sur le plan politique, s'il y a lieu, et avec la participation d'entités du secteur privé, le cas échéant.

Fait à Bruxelles, le 13.9.2017

Par la Commission
Mariya GABRIEL
Membre de la Commission

AMPLIATION CERTIFIÉE CONFORME
Pour le Secrétaire général,

Jordi AYET PUIGARNAU
Directeur du Greffe
COMMISSION EUROPÉENNE