Commission européenne - Communiqué de presse

État de l'Union 2017 — Cybersécurité: La Commission dote l'UE de moyens supplémentaires pour répondre aux cyberattaques

Bruxelles, le 19 septembre 2017

.

Le 13 septembre, dans son discours annuel sur l'état de l'Union, le **président Jean-Claude Juncker** a déclaré: *«Au cours des trois dernières années, nous avons fait des progrès dans la sécurisation de l'internet. Mais l'Europe reste mal équipée face aux cyberattaques. C'est pourquoi la Commission propose aujourd'hui de nouveaux outils, et notamment une Agence européenne de cybersécurité, pour mieux nous défendre contre ces attaques.»*

Les Européens accordent une grande confiance aux technologies numériques. Elles offrent aux citoyens de nouvelles possibilités de connexion, facilitent la diffusion de l'information et constituent l'épine dorsale de l'économie européenne. Cependant, elles s'accompagnent aussi de nouvelles menaces et on assiste à une multiplication des tentatives, émanant d'acteurs étatiques et non étatiques, visant à voler des données, à commettre des actes frauduleux, ou même à déstabiliser des gouvernements. L'année dernière, on a enregistré plus de 4 000 attaques par rançongiciel par jour et 80 % des entreprises européennes ont connu au moins un incident lié à la cybersécurité. L'incidence économique de la cybercriminalité a été quintuplée rien qu'au cours des quatre dernières années.

Pour doter l'Europe des outils adéquats pour faire face aux cyberattaques, la Commission européenne et la Haute Représentante proposent une large panoplie de mesures destinées à renforcer la cybersécurité dans l'UE. Parmi celles-ci figurent une proposition relative à une nouvelle **Agence de cybersécurité de l'UE**, qui assistera les États membres dans la gestion des cyberattaques, ainsi qu'un nouveau **système européen de certification**, qui permettra de garantir la sécurité d'utilisation des produits et services dans l'environnement numérique.

Federica **Mogherini**, la Haute Représentante et vice-présidente de la Commission, a déclaré à ce sujet: *«En matière de cybersécurité, l'UE entend mener une politique internationale visant à promouvoir un cyberespace ouvert, libre et sûr et à soutenir les efforts entrepris pour élaborer des normes de comportement responsable des États et appliquer le droit international et les mesures destinées à renforcer la confiance dans la cybersécurité.»*

Andrus **Ansip**, vice-président pour le marché unique numérique, s'est quant à lui exprimé en ces termes: *«Aucun pays ne peut relever seul le défi que représente la cybersécurité. Nos initiatives renforcent la coopération, afin que les pays de l'UE puissent présenter un front uni. Nous proposons également de nouvelles mesures pour stimuler les investissements dans l'innovation et promouvoir la cyberhygiène.»*

Julian **King** Commissaire pour l'union de la sécurité, a indiqué pour sa part: «*Nous devons travailler ensemble pour accroître notre résilience, stimuler l'innovation technologique, renforcer la dissuasion en améliorant la traçabilité et la responsabilisation, et tirer parti de la coopération internationale pour promouvoir notre cybersécurité collective*.»

Mariya **Gabriel**, commissaire pour l'économie et la société numériques, a ajouté: *«Nous devons renforcer la confiance des citoyens et des entreprises dans l'environnement numérique, notamment dans une période où les cyberattaques de grande envergure sont de plus en plus fréquentes. Mon souhait est que des normes de cybersécurité élevées confèrent un nouvel avantage concurrentiel à nos entreprises.»*

Confrontée aux récentes attaques par rançongiciel, à la spectaculaire augmentation de la cybercriminalité, à l'utilisation croissante de cyberoutils par des acteurs étatiques pour parvenir à leurs

objectifs géopolitiques et à la diversification des incidents liés à la cybersécurité, l'UE doit devenir plus résiliente face aux cyberattaques et adopter des mesures efficaces, en matière de cyberdissuasion et de répression par le droit pénal, pour mieux protéger les citoyens, les entreprises et les institutions publiques européens. C'est là l'ambition du paquet «cybersécurité» présenté aujourd'hui.

Renforcer la résilience: une Agence de cybersécurité de l'UE renforcée

Une Agence de cybersécurité de l'UE: L'actuelle Agence européenne pour la sécurité des réseaux et de l'information (ENISA) sera transformée en une Agence dotée d'un mandat permanent, qui aidera les États membres à prévenir efficacement les cyberattaques et à y répondre. Elle améliorera la préparation de l'UE en cas d'attaques en organisant chaque année des **exercices de cybersécurité paneuropéens** et en assurant un meilleur **partage des connaissances et des informations sur les menaces** par la création de centres d'échange et d'analyse d'informations. Elle contribuera à la mise en œuvre de la **directive sur la sécurité des réseaux et des systèmes d'information**, qui impose des obligations de signalement des incidents graves aux autorités nationales.

Elle aidera aussi à créer et à appliquer le **cadre de certification à l'échelle de l'UE** proposé par la Commission pour garantir que les **produits et les services répondent à toutes les exigences de cybersécurité applicables**. Tout comme le système d'étiquetage des produits alimentaires de l'UE garantit aux consommateurs la qualité de ce qui est dans leur assiette, de nouveaux certificats européens de cybersécurité garantiront la fiabilité des milliards de dispositifs (l'«internet des objets») qui pilotent dorénavant les infrastructures critiques, telles que les réseaux d'énergie et de transport, mais aussi de nouveaux équipements grand public, tels que les voitures connectées. Les certificats de cybersécurité seront reconnus dans tous les États membres, ce qui réduira les charges administratives et les coûts pour les entreprises[1].

Doter l'UE d'une capacité accrue en matière de cybersécurité

Il est dans l'intérêt stratégique de l'UE de veiller à ce que le développement des outils technologiques de la cybersécurité permette à l'économie numérique de prospérer, tout en protégeant notre sécurité, notre société et notre démocratie. Cela passe par la protection des matériels et logiciels d'importance critique. Pour renforcer la capacité de l'UE en matière de cybersécurité, la Commission et la Haute Représentante proposent:

- un **Centre européen de recherche et de compétences en matière de cybersécurité** (l'initiative pilote sera lancée dans le courant de l'année 2018). En collaboration avec les États membres, il aidera à mettre au point et à déployer les outils et les technologies nécessaires pour nous adapter à une menace qui est en constante évolution et à faire en sorte que nos moyens de défense restent à un niveau aussi avancé que les armes employées par les cybercriminels. Il complétera aussi les efforts de renforcement des capacités dans ce domaine aux niveaux national et de l'Union;
- un **plan visant à garantir une réaction** rapide de l'UE et des États membres qui soit opérationnelle et concertée en cas de cyberattaque de grande ampleur. La procédure proposée est prévue dans une recommandation qui a été adoptée la semaine dernière. Cette recommandation demande également aux États membres et aux institutions de l'UE de créer un cadre de l'UE pour la réaction aux crises de cybersécurité afin de traduire le plan d'action en mesures concrètes. Ce plan devra ensuite être régulièrement mis à l'épreuve dans le cadre d'exercices de gestion de crise dans le domaine de la cybersécurité et d'autres domaines;
- **une solidarité accrue**: Dans l'avenir, la possibilité de créer un fonds d'intervention pour les urgences en matière de cybersécurité pourrait être envisagée pour les États membres qui ont appliqué de manière responsable l'ensemble des mesures de cybersécurité prescrites par la législation de l'UE. Ce fonds fournirait une aide d'urgence destinée à assister les États membres, comme le fait actuellement le mécanisme de protection civile de l'UE en cas d'incendie de forêt ou de catastrophe naturelle;
- **un renforcement des capacités de cyberdéfense**: Les États membres sont encouragés à intégrer la cybersécurité dans le cadre d'une «coopération structurée permanente» (CSP) et du Fonds européen de la défense afin de soutenir des projets dans le domaine de la cyberdéfense. Il serait également possible de développer davantage le Centre européen de recherche et de compétences en matière de cybersécurité en lui conférant une dimension de cyberdéfense. En 2018, l'UE mettra en place une plateforme de formation et d'enseignement en matière de cyberdéfense visant à combler le manque actuel de compétences dans le domaine de la cyberdéfense. L'UE et l'OTAN favoriseront conjointement la recherche et la coopération dans le domaine de l'innovation sur les questions de cyberdéfense. La coopération avec l'OTAN, notamment la participation à des exercices parallèles et coordonnés, sera approfondie;
- **une coopération internationale renforcée**: L'UE entend muscler sa réponse aux cyberattaques

en mettant en œuvre un cadre pour une réponse diplomatique commune de l'UE à l'égard des actes de cybermalveillance, en appui d'un cadre stratégique pour la prévention des conflits et la stabilité dans le cyberespace. Parallèlement, de nouvelles mesures en matière de renforcement des cybercapacités seront prises pour aider les pays tiers à lutter contre les cybermenaces.

Une répression plus efficace par le droit pénal

Une réponse des services répressifs plus percutante, axée sur la détection, la traçabilité et la poursuite des cybercriminels, est indispensable pour établir une dissuasion efficace. La Commission propose par conséquent de renforcer la dissuasion en adoptant de nouvelles mesures de **lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces**.

La **directive** proposée renforcera la capacité des services répressifs à lutter contre cette forme de criminalité en **élargissant le champ des infractions** liées aux systèmes d'information pour y inclure toutes les opérations de paiement, y compris celles réalisées au moyen de monnaies virtuelles. Elle introduira aussi des **règles communes relatives au niveau des peines** et précisera l'**étendue de la compétence juridictionnelle des États membres** en ce qui concerne ces infractions.

Pour accroître l'efficacité des enquêtes et des poursuites en matière de criminalité facilitée par les technologies de l'information et des communications, la Commission soumettra également, au début de l'année 2018, des propositions visant à faciliter l'accès transfrontière aux **preuves électroniques**. En outre, elle présentera, d'ici à octobre, les résultats de ses réflexions sur le rôle du **cryptage** dans les enquêtes pénales.

Historique

Il ressort de statistiques récentes que les cybermenaces évoluent rapidement et que l'opinion publique perçoit la cybercriminalité comme une menace importante: des études montrent que les attaques par rançongiciel ont augmenté de 300 % depuis 2015; l'incidence économique de la cybercriminalité a quintuplé entre 2013 et 2017, et pourrait encore quadrupler d'ici à 2019. 87 % des Européens estiment que la cybercriminalité constitue un problème considérable pour la sécurité intérieure de l'UE.

Pour guider ses travaux dans ce domaine, la Commission s'appuie sur le programme européen en matière de sécurité et sur l'examen à mi-parcours de la stratégie pour un marché unique numérique, qui exposent les grandes mesures proposées pour renforcer la cybersécurité. Les mesures proposées aujourd'hui complètent les règles existantes et comblent les lacunes dues à l'évolution de la situation en matière de menaces depuis l'adoption de la stratégie de cybersécurité de l'UE en 2013, traduisant ainsi en termes concrets l'engagement prioritaire consistant à aider les États membres à assurer la sécurité intérieure pris dans la déclaration et la feuille de route de Bratislava:

Pour en savoir plus

Questions et réponses - État de l'Union 2017 — Cybersécurité: La Commission dote l'UE de moyens supplémentaires pour répondre aux cyberattaques

Fiche d'information sur les propositions en matière de cybersécurité

Fiche d'information sur l'Agence de cybersécurité de l'UE

Fiche d'information sur la lutte contre la fraude et la contrefaçon concernant les moyens de paiement autres que les espèces

Textes adoptés

[1] À titre d'exemple, le coût de la certification de compteurs intelligents au Royaume-Uni et en France avoisine les 150 000 EUR.

IP/17/3193

Personnes de contact pour la presse:
Natasha BERTAUD (+32 2 296 74 56)
Nathalie VANDYSTADT (+32 2 296 70 83)
Tove ERNST (+32 2 298 67 64)
Maja KOCIJANCIC (+32 2 298 65 70)
Inga HOGLUND (+32 2 295 06 98)

Renseignements au public: Europe Direct par téléphone au 00 800 67 89 10 11 ou par courriel

Attachments

20170919-cybersecurity factsheet non-cash-payments-fr.pdf