Commission européenne

ÉTAT DE L'UNION 2018

Renforcer la cybersécurité en Europe

#SOTEU

12 septembre 2018

«Les cyberattaques ne connaissent pas de frontières; pourtant, nos capacités de réaction varient fortement d'un pays à l'autre, ce qui crée des failles et des vulnérabilités qui favorisent les cyberattaques. L'UE doit se doter de structures plus robustes et plus efficaces pour améliorer sa cyber-résilience et réagir aux cyberattaques. Nous ne voulons pas être le maillon faible de la lutte contre cette menace mondiale.»

Jean-Claude Juncker, sommet numérique de Tallinn, 29 septembre 2017

Pour doter l'Europe des outils adéquats pour faire face à l'évolution constante des cybermenaces, la Commission européenne et la haute représentante ont présenté, en 2017, une large panoplie de mesures destinées à renforcer la cybersécurité dans l'UE. Ces efforts sont aujourd'hui complétés par une proposition visant à aider l'UE à mettre en commun les ressources et l'expertise dans les domaines de la recherche et de l'innovation, et à se hisser au rang de chef de file dans le domaine des technologies numériques et de cybersécurité de prochaine génération.

Les cybermenaces actuelles

En 2016, on a dénombré **plus de 4 000 attaques par rançongiciel** par jour.

80 % des entreprises européennes ont connu au moins un incident lié à la cybersécurité pendant l'année écoulée.

Tous secteurs confondus, les **incidents liés à la cybersécurité ont augmenté de 38 %** – soit la plus forte hausse des 12 dernières années.

Dans certains États membres **50 % de tous les actes délictueux** relèvent de la cybercriminalité.

En mai 2017, **plus de 150 pays et de 230 000 systèmes**, dans tous les secteurs, ont été touchés par la cyberattaque WannaCry et pour certains services essentiels connectés à l'internet, tels que les hôpitaux et les ambulances, l'incidence a été significative.

Renforcer la résilience face aux cyberattaques

La Commission soutient déjà le renforcement de la résilience, de la dissuasion et de la capacité de réaction de l'UE face aux cyberattaques, y compris par les moyens suivants:

Soutien à la mise en œuvre efficace du premier acte législatif de l'UE consacré à la cybersécurité (directive relative à la sécurité des réseaux et des systèmes d'information), qui prévoit les obligations suivantes:

RENFORCEMENT DES CAPACITÉS

Les États membres doivent améliorer leurs capacités en matière de cybersécurité

COOPÉRATION

Il faut renforcer la coopération à l'échelle de l'UE

PRÉVENTION DES RISQUES

Les acteurs des secteurs clés (comme l'énergie, les transports, la santé) sont tenus de mettre en place des mesures visant à prévenir les risques et à gérer les cyberincidents

Coopération avec les États membres dans les domaines suivants:

AGENCE DE L'UE POUR LA CYBERSÉCURITÉ

Renforcement de l'Agence de l'Union européenne pour la cybersécurité afin de mieux assister les États membres

CADRE DE CERTIFICATION DE L'UE

Mise en place d'un cadre de certification à l'échelle de l'UE pour garantir la cybersécurité des produits et services

RÉACTION COORDONNÉE

Réaction rapide et coordonnée aux cyberattaques majeures

L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) aide les autorités des États membres chargées de la cybersécurité à mieux protéger l'UE contre les cyberattaques.

Mise en commun des ressources et de l'expertise dans le domaine des technologies de cybersécurité

Outre les initiatives de l'UE déjà menées dans le domaine de la cybersécurité, la Commission propose aujourd'hui de compléter ces efforts par la création d'un Réseau de centres de compétences et d'un Centre de compétences européen industriel, technologique et de recherche en matière de cybersécurité pour mettre au point et déployer des outils et des technologies nécessaires pour nous permettre de nous adapter à une menace en constante évolution.

Le Centre européen sera chargé de coordonner, avec les États membres et de la manière la plus ciblée, les fonds consacrés à la cybersécurité dans le cadre du prochain budget à long terme de l'UE. Cela permettra de développer de nouvelles capacités européennes dans le domaine de la cybersécurité.

Avec plus de **660 centres de compétences en matière de cybersécurité** répartis dans l'ensemble de l'UE, celle-ci dispose déjà d'une expertise considérable en la matière. Afin d'exploiter et d'utiliser efficacement cette expertise, la Commission propose de créer un mécanisme pour:

Mettre en commun, partager et garantir l'accès à l'expertise existante

Contribuer au déploiement de produits et solutions de cybersécurité de l'UE

Garantir la coopération stratégique à long terme entre les entreprises, la communauté de la recherche et les gouvernements

Co-investir dans les infrastructures coûteuses et les partager

Le Centre de compétences européen:

Coordonnera l'utilisation des fonds consacrés à la cybersécurité dans le cadre du prochain budget à long terme de l'UE pour la période 2021-2027 au titre du programme pour une Europe numérique et du programme «Horizon Europe». Le Centre soutiendra le Réseau et la communauté des compétences pour faire progresser la recherche et l'innovation dans le domaine de la **cybersécurité**. Il organisera aussi les **investissements conjoints** de l'UE, des États membres et de l'industrie. Par exemple, **2 milliards d'euros** seront investis, au titre du programme pour une Europe numérique, dans la protection de l'économie numérique, de la société et des démocraties de l'UE en assurant la promotion du secteur de la cybersécurité de l'Union et en finançant des équipements et infrastructures de pointe en matière de cybersécurité.

Le Réseau des centres nationaux de coordination:

Chaque État membre désignera un centre national de coordination pour piloter le Réseau, qui s'attellera au développement de nouvelles capacités et de compétences plus étendues dans le domaine de la cybersécurité. Le Réseau permettra de recenser et de soutenir les projets les plus pertinents en matière de cybersécurité dans les États membres.

La communauté des compétences:

Un groupe de grande taille, ouvert et varié d'acteurs concernés par la cybersécurité provenant du milieu de la recherche et des secteurs privé et public, y compris les autorités civiles et militaires.

Quelles sont les améliorations escomptées?

- meilleure coordination des travaux;
- accès à l'expertise;
- accès aux infrastructures d'essai et d'expérimentation;
- évaluation du niveau de cybersécurité des produits;
- accès à des produits et solutions de cybersécurité innovants;
- soutien au déploiement commercial de produits et de services;
- visibilité accrue auprès des investisseurs et des partenaires commerciaux potentiels;
- réduction des coûts grâce au co-investissement avec d'autres États membres;
- capacité de l'UE à sécuriser de manière autonome son économie et la démocratie;
- émergence de l'UE en tant que chef de file mondial dans le domaine de la cybersécurité.

Quels seront les secteurs bénéficiaires?