COMMISSION
EUROPÉENNE

Bruxelles, le 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

ANNEXES

de la

Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ANNEXE I

La base de référence en cybersécurité concerne les domaines suivants:

(1) la politique de cybersécurité, y compris les objectifs et les priorités en matière de sécurité des réseaux et des systèmes d'information, en particulier en ce qui concerne l'utilisation des services d'informatique en nuage (au sens de l'article 4, point 19, de la directive [proposition SRI 2]) et les modalités techniques permettant le télétravail;

(2) l'organisation de la cybersécurité, y compris la définition des rôles et des responsabilités;

(3) la gestion des actifs, y compris l'inventaire des actifs informatiques et la cartographie des réseaux informatiques;

(4) le contrôle des accès;

(5) la sécurité des activités;

(6) la sécurité des communications;

(7) l'acquisition, le développement et la maintenance des systèmes;

(8) les relations avec les fournisseurs;

(9) la gestion des incidents, y compris les approches visant à améliorer la préparation, la réaction et le rétablissement à la suite d'incidents et la coopération avec le CERT-UE, telles que la maintenance du suivi de la sécurité et de la journalisation;

(10) la gestion de la continuité des activités et la gestion des crises; et

(11) les programmes d'éducation, de sensibilisation et de formation en matière de cybersécurité.

ANNEXE II

Les institutions, organes et organismes de l'Union abordent au moins les mesures spécifiques de cybersécurité suivantes dans le cadre de la mise en œuvre de la base de référence en cybersécurité et dans leurs plans de cybersécurité, conformément aux documents d'orientation et aux recommandations émanant de l'IICB:

(1) des mesures concrètes pour progresser vers un modèle à vérification systématique (c'est-à-dire un modèle de sécurité, un ensemble de principes de conception du système et une stratégie coordonnée de cybersécurité et de gestion des systèmes fondée sur la reconnaissance de l'existence de menaces tant à l'intérieur qu'à l'extérieur des frontières traditionnelles du réseau);

(2) l'adoption de l'authentification à facteurs multiples comme norme dans l'ensemble des réseaux et des systèmes d'information;

(3) la sécurisation de la chaîne d'approvisionnement des logiciels au moyen de critères pour le développement et l'évaluation sécurisés des logiciels;

(4) le renforcement des règles de passation des marchés publics afin de faciliter un niveau élevé commun de cybersécurité par:

   (a) la suppression des obstacles contractuels qui limitent le partage d'informations sur les incidents, les vulnérabilités et les cybermenaces entre les fournisseurs de services informatiques et le CERT-UE;

   (b) l'obligation contractuelle de signaler les incidents, les vulnérabilités et les cybermenaces ainsi que de veiller à ce que des mesures appropriées de réaction et de suivi en cas d'incidents soient en place.