Directive SRI

La directive SRI est le premier texte législatif à l'échelle de l'UE en matière de cybersécurité. Il prévoit des mesures juridiques visant à renforcer le niveau global de cybersécurité dans l'UE.

© iStock by Getty Images -1169999045 aismagilov

La directive sur la sécurité des réseaux et des systèmes d'information (directive SRI) prévoit des mesures juridiques visant à renforcer le niveau global de cybersécurité dans l'UE en garantissant:

- La préparation des États membres, en exigeant qu'ils soient équipés de manière appropriée. Par exemple, avec une équipe d'intervention en cas d'incident de sécurité informatique (CSIRT) et une autorité nationale compétente en matière de SRI,
- la coopération entre tous les États membres, par la création d'un groupe de coopération chargé de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres.
- une culture de la sécurité dans tous les secteurs qui sont vitales pour notre économie et notre société et qui dépendent fortement des TIC, telles que l'énergie, les transports, l'eau, les banques, les infrastructures des marchés financiers, les soins de santé et les infrastructures numériques.

Les entreprises identifiées par les États membres comme des opérateurs de services essentiels dans les secteurs susmentionnés devront prendre les mesures de sécurité appropriées et notifier aux autorités nationales compétentes les incidents graves. Les principaux fournisseurs de services numériques, tels que les moteurs de recherche, les services d'informatique en nuage et les places de marché en ligne, devront se conformer aux exigences en matière de sécurité et de notification

prévues par la nouvelle directive.

Une «boîte à outils NIS»

Étant donné que le paysage des menaces en matière de cybersécurité évolue à un rythme rapide, il a été nécessaire de mettre en œuvre rapidement la directive SRI. La Commission a adopté une communication visant à soutenir les États membres dans leurs efforts de mise en œuvre de la directive.

La communication, surnommée la «boîte à outils SRI», fournit aux États membres des informations pratiques sur la directive. Par exemple, il présente les meilleures pratiques en matière de mise en œuvre de la directive par d'autres États membres, avec des explications et une interprétation de dispositions spécifiques visant à clarifier la manière dont la directive SRI devrait fonctionner dans la pratique.

Rapport évaluant la cohérence des approches dans l'identification des opérateurs de services essentiels

Les opérateurs de services essentiels sont responsables de la notification aux autorités nationales des cyberincidents graves. Le présent rapport donne un aperçu de la manière dont les États membres ont identifié les opérateurs de services essentiels. Il évalue si les méthodes d'identification de ces opérateurs sont cohérentes entre les États membres.

Révision de la directive

L'article 23 de la directive impose à la Commission européenne de réexaminer périodiquement le fonctionnement de la présente directive. Dans le cadre de son principal objectif politique visant à rendre l'Europe adaptée à l'ère numérique ainsi qu'aux objectifs de l'union de la sécurité, la Commission a annoncé, dans son programme de travail 2020, qu'elle procéderait à l'examen d'ici la fin de 2020.

Dans le cadre de ce processus, une consultation a été ouverte le 7 juillet 2020, la date limite étant fixée au 2 octobre 2020. Les résultats de cette consultation ont été utilisés pour l'évaluation et l'analyse d'impact de la directive SRI.

Proposition de directive SRI révisée (SRI2)

À l'issue du processus de réexamen, la nouvelle proposition législative a été présentée le 16 décembre 2020.

La proposition fait partie d'un ensemble de mesures visant à améliorer encore les capacités de résilience et de réaction aux incidents des entités publiques et privées, des autorités compétentes et de l'UE dans son ensemble. Il couvre le domaine de la cybersécurité et de la protection des infrastructures critiques. La proposition est conforme aux priorités de la Commission visant à rendre l'Europe adaptée à l'ère numérique et à construire une économie prête pour un avenir qui fonctionne pour les citoyens.

La proposition s'appuie sur la directive SRI actuelle et l'abroge. Il modernise le cadre juridique existant en tenant compte de la numérisation accrue du marché intérieur ces dernières années et de l'évolution du paysage des menaces en matière de cybersécurité.

La proposition de directive révisée sur la sécurité des réseaux et des systèmes d'information a été accompagnée d'une analyse d'impact, qui a été soumise au comité d'examen de la réglementation le 23 octobre 2020 et a reçu un avis positif assorti d'observations par le comité d'examen de la réglementation le 20 novembre 2020.

Un accord politique a été conclu le 13 mai 2022.

Révision de la directive SRI: Questions et réponses

Dernières nouvelles

COMMUNIQUÉ DE PRESSE | 28 novembre 2022
Déclaration commune de la présidente von der Leyen et du président Yoon sur le partenariat numérique UE-République de Corée

Nous nous félicitons du lancement aujourd'hui d'un nouveau partenariat numérique entre l'UE et la République de Corée. Dans un monde de plus en plus instable, la nécessité de travailler avec des partenaires partageant des valeurs démocratiques est plus importante que jamais pour relever les défis communs.

COMMUNIQUÉ DE PRESSE | 24 novembre 2022
Cybersécurité: L'UE lance la première phase de déploiement de l'infrastructure européenne des centres d'opérations de sécurité transfrontalière

La Commission, en coordination avec le Centre européen de compétences en matière de cybersécurité (ECCC), lance un appel à manifestation d'intérêt pour sélectionner, dans les États membres, des entités qui hébergeront et exploiteront des plateformes transfrontières de détection des cybermenaces, chacune réunissant des entités publiques pertinentes de plusieurs États membres, ainsi que des entités privées.

COMMUNIQUÉ DE PRESSE | 17 novembre 2022
La Commission se félicite de l'accord politique sur le lancement des hôpitaux IRIS, le programme de l'Union pour une connectivité sécurisée

La Commission s'est félicitée de l'accord politique intervenu le 17 novembre entre le Parlement européen et les États membres de l'UE sur le programme de l'Union pour une connectivité sécurisée 2023-2027, doté d'un budget de 2.4 milliards d'euros.

COMMUNIQUÉ DE PRESSE | 17 novembre 2022
Nouveaux appels de financement au titre du programme pour une Europe numérique pour renforcer la cyber-résilience

La Commission a lancé une invitation aux entreprises, aux administrations publiques et à d'autres organisations à soumettre des propositions de solutions innovantes en matière de

cybersécurité et à demander un financement de l’UE au titre du programme pour une Europe numérique.

Parcourir Cybersécurité

Contenu associé

Vue d’ensemble

Politiques de cybersécurité

L’Union européenne travaille sur différents fronts pour promouvoir la cyberrésilience, préserver nos communications et nos données et assurer la sécurité de la société et de l’économie en ligne.

Aller plus loin

État d’avancement de la transposition de la directive SRI

La Commission, en collaboration avec l’Agence de l’Union européenne chargée de la sécurité des réseaux et de l’information, travaille en étroite collaboration avec les États membres pour assurer la transposition de la directive SRI dans la législation nationale.

Groupe de coopération SRI

Le groupe de coopération en matière de réseaux et de systèmes d’information a été créé par la directive SRI pour assurer la coopération et l’échange d’informations entre les États membres.

À lire également

Réseau et centre européen de compétences en matière de cybersécurité

Le réseau européen de cybersécurité et le Centre de compétences en cybersécurité aident l’UE à conserver et à développer les capacités technologiques et industrielles en matière de cybersécurité.

Groupe de certification de la cybersécurité des parties prenantes

Le groupe des parties prenantes pour la certification de cybersécurité a été créé pour fournir des conseils sur les questions stratégiques relatives à la certification de cybersécurité.

La loi sur la cybersécurité de l’UE

La loi sur la cybersécurité renforce l’Agence de l’UE pour la cybersécurité (ENISA) et établit un cadre de certification de cybersécurité pour les produits et services.

Le cadre de certification de cybersécurité de l’UE

Le cadre de certification de cybersécurité de l’UE pour les produits TIC permet la création de systèmes de certification européens adaptés et fondés sur les risques.
