



Directive SRI et sécurité de la chaîne logistique : en quoi cela vous concerne-t-il ?

09 septembre 2022, 15:33

Tatiana Galibus

Avez-vous déjà entendu parler de la directive SRI ? La majorité des entreprises manufacturières ne sont pas encore conscientes de l'importance de cette réglementation dans l'UE. Chez Sirris, nous suivons la mise en œuvre de cette directive en Belgique. Les règles qu'elle établit vous touchent en effet directement si vous travaillez dans l'une des 3.000 PME manufacturières de Belgique, et même si vous travaillez pour une entreprise prestataire, un constructeur de machines ou un fournisseur de services numériques..

De quoi s'agit-il ?



(ec.europa.eu)

La directive SRI(-1) a été adoptée par l'UE en 2016. Il s'agissait de la première réglementation en matière de cybersécurité au niveau européen. En Belgique, elle a été appliquée sous la forme de la loi SRI en 2019. Quelles sont les obligations en vertu de la SRI actuelle ?

Les États membres	• élaborent des stratégies nationales en matière de cybersécurité; • adoptent une collaboration transfrontalière; • identifient les opérateurs de services essentiels (OSE) dans les domaines suivants : énergie, transports, banques, infrastructures des marchés financiers, soins de santé, eau potable et infrastructures numériques.
Les opérateurs OSE	• prennent des mesures de sécurité minimales; • signalent les incidents significatifs.
Les fournisseurs de services numériques clés	• se conforment à ces exigences de sécurité et de notification.

La réglementation SRI-2 a été proposée par l'UE en décembre 2020 en raison de l'augmentation des cyberattaques et de leur impact dévastateur. Elle comprend, entre autres, les améliorations suivantes :

- davantage de secteurs et d'entités dans le champ de la cybersécurité
- exigences de sécurité étendues
- implication personnelle et responsabilité des dirigeants et des conseils d'administration
- sanctions strictes et montants plus élevés
- obligations détaillées en matière de rapport d'incidents
- focalisation sur le renforcement de la sécurité de la chaîne logistique.

Vous n'en avez probablement pas encore entendu parler, car ces règles ne sont pas encore largement adoptées. Toutefois, on s'attend à ce que la situation change d'ici 2025 avec l'adoption de la loi SRI belge.

Pourquoi est-ce important ?

En résumé, l'UE propose de renforcer les exigences imposées aux fournisseurs, d'alourdir les sanctions et d'imposer une responsabilité personnelle aux CEO et aux conseils d'administration. Des réglementations renforcées et personnalisées toucheront toutes les entreprises impliquées dans les interactions de votre chaîne logistique. Elles changeront inévitablement la façon dont vous collaborez avec les fournisseurs et fournissez les produits aux clients. La sécurité deviendra bien plus essentielle pour la continuité des activités.

Pour certains, cela peut sembler effrayant, mais pour d'autres, qui préparent déjà l'avenir, ce n'est pas une surprise. La cybersécurité prend sa place comme valeur ajoutée à votre produit et, tôt ou tard, vous ne pourrez plus vendre sans cette « fonctionnalité ».

Et si vous choisissez d'ignorer ces changements réglementaires ? Qu'est-ce que cela signifie pour une PME ? Cela signifie perdre définitivement des clients si votre sécurité n'est pas suffisante. La majorité des entreprises sont impliquées, dans la chaîne logistique, dans des interactions de plus en plus complexes qui ne sont souvent pas encore sécurisées. Par exemple, si vous répondez « oui » à l'une des questions suivantes, cela signifie que vous n'êtes pas sûr en termes de SRI :

- Donnez-vous des droits d'administration à des collaborateurs externes sans spécifier les machines et la politique de contrôle d'accès ?
- Évitez-vous de surveiller régulièrement les connexions externes ?
- Vous arrive-t-il d'oublier de passer en revue les ports et les outils utilisés pour la télémaintenance ?

Suis-je en sécurité ?

Malheureusement, il n'existe pas de questionnaire uniforme relatif à la sécurité de votre chaîne logistique et à la directive SRI-2. Nous travaillons sur un tel outil automatique chez Sirris dans le cadre du projet Cornet Cybersecurity 4.0.

À l'heure actuelle, Sirris propose aux entreprises manufacturières des séances d'information gratuites d'une heure sur la cybersécurité, axées sur la chaîne d'approvisionnement. À cette occasion, nous vous poserons quelques questions et nous proposerons des solutions aux éventuelles vulnérabilités critiques découvertes. Un tel processus vous intéresse ? [Contactez-nous](#) !

Et que faire ensuite ?

Soyez bien préparé. Prenez de l'avance sur les pirates. Le paysage de la cybersécurité évolue de jour en jour et il est essentiel de garder le cap. Les attaques étant de plus en plus organisées, la sécurité doit être plus collaborative et agile, ce qui implique de garantir la sécurité de l'ensemble de la chaîne logistique.

Sirris propose un programme de formation de deux mois, axé sur la pratique, pour aider les entreprises manufacturières en matière de cybersécurité. Nous proposons des sessions de

coaching individuel et des masterclasses dans vos locaux, afin de vous aider à concevoir votre propre stratégie de cybersécurité et à éliminer les risques spécifiques.

Découvrez nos offres collectives et individuelles [ici](#)!

Pour en savoir plus :

ENISA: <https://digital-strategy.ec.europa.eu/en/policies/nis-directive>

CCA Belgium: <https://www.cybersecuritycoalition.be/nis-2-where-are-you/>

Auteurs



Tatiana Galibus