Information Presse

AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 vloquet@alx-communication.com

NIS2 :
Il est urgent pour les entreprises de ne plus attendre

Le CESIN appelle à une transposition stratégique et rapide de la directive NIS2

Paris, le 5 novembre 2024 – Dans un monde où le numérique devient le pilier central de notre économie et de notre société, la cybersécurité n'est plus une option mais une nécessité absolue. La directive NIS2, qui succède à la directive NIS1, représente une avancée majeure dans l'Union Européenne pour renforcer la cybersécurité et en harmoniser l'approche.

Le CESIN, en tant que porte-voix des experts en sécurité de l'information, appelle les entreprises, les administrations et les collectivités locales à entamer les travaux dès maintenant, en se basant sur les textes existants en dépit d'une transposition retardée de cette directive dans notre législation nationale.

Pourquoi la directive NIS2 ?

Afin de répondre à l'évolution de la menace cyber qui, en devenant systémique, cible désormais l'ensemble du tissu social et économique de manière indifférenciée, la directive NIS2 élargit le périmètre des entités concernées, incluant désormais des secteurs essentiels de notre économie qui jusqu'ici n'étaient pas soumis à des exigences de sécurité aussi strictes. Cela inclut des entreprises et administrations de toutes les tailles, notamment les fournisseurs de services de confiance, les opérateurs de réseaux de communications électroniques, et même certains acteurs de la santé et des transports ainsi que certaines collectivités territoriales dès lors qu'elles présentent une sensibilité particulière du fait de leur taille (régions, départements ou communautés de communes) ou du secteur dans lequel s'inscrivent leurs activités. Cette extension est cruciale, car la chaîne de sécurité est aussi forte que son maillon le plus faible.

Les avantages de la directive

- Une **cybersécurité renforcée et proportionnée** : NIS2 impose des mesures de sécurité plus robustes, une gestion proactive des risques, et des obligations de reporting qui permettront de mieux prévenir et répondre aux cyberattaques.
- Afin d'**adapter le niveau d'exigences** à la menace, aux capacités et à la criticité des entités concernées, la directive NIS2 identifie deux catégories d'entités régulées, « essentielles » et « importantes », en fonction des services qu'elles fournissent et de leur taille, et avec des mesures de sécurité différentes.
- **Harmonisation européenne** : grâce aux règles minimales de cybersécurité communes à tous les Etats membres (ce qui fait du sens dans un marché unique) et la coopération cyber entre Etats membres pour répondre de manière plus coordonnée et cohérente aux attaques cyber.
- **Protection des données et renforcement de la confiance** : avec l'augmentation des cyberattaques, la confiance des citoyens et des entreprises dans les infrastructures numériques est en jeu. NIS2 aide à restaurer et maintenir cette confiance.
- **Compétitivité économique** : les entreprises soumises à des standards de cybersécurité élevés seront plus compétitives sur le marché international, où la sécurité est désormais un critère de choix de partenaires et de prestataires.
- **Sensibilisation des directions générales** : NIS2 permettra de sensibiliser et surtout responsabiliser les dirigeants sur la prise en compte du risque cyber de leur entreprise.
- **Sécurisation de la chaine de valeur** : NIS2 permettra un maillage cohérent du niveau cyber de toute la chaine de valeur et de production de l'entreprise, étendue à ses fournisseurs.

L'Appel du CESIN

« Le Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité » a fait l'objet d'un examen en Conseil des ministres le 15 octobre dernier.

Le CESIN exhorte le gouvernement à considérer la transposition de NIS2 comme une opportunité stratégique. Une transposition rapide et efficace qui :

- Renforcera notre posture de sécurité nationale face aux cybermenaces qui ne cessent de croître en sophistication et en fréquence.
- Stimulera l'innovation dans le secteur de la cybersécurité, poussant les entreprises à développer de nouvelles solutions pour répondre aux exigences de la directive.
- Sensibilisera les dirigeants et les employés à l'importance de la cybersécurité, un aspect souvent sous-estimé jusqu'à ce qu'une crise survienne.

Le CESIN encourage les dirigeants à ne pas retarder les travaux de renforcement de cybersécurité et de :

- Identifier si la directive NIS 2 s'applique à leur entité (l'ANSSI met notamment à disposition des entités un espace numérique MonEspaceNIS2 permettant de déterminer si l'entité relève de la règlementation).
- Réaliser dès lors une analyse d'écart avec la NIS2.
- Supporter les équipes cyber pour la prise en compte des mesures.
- Valider le budget pluriannuel nécessaire à sa mise en œuvre.

Le CESIN vise à conscientiser et encourager une action rapide tant sur le plan législatif, pour ne pas retarder davantage la transposition, que sur le plan opérationnel afin que les entités concernées s'engagent dès à présent dans leurs travaux internes de sécurisation, sans attendre le délai de 3 ans annoncé par l'ANSSI pendant lequel elle ne prévoit pas de sanctions relatives à la mise en place des mesures de sécurité. Cependant l'ANSSI souligne à juste titre qu'elle n'attendra pas trois ans pour exiger certaines choses simples comme l'enregistrement auprès de l'ANSSI des entités régulées ou encore la notification des incidents.

Depuis 2017, de nombreuses actions concrètes ont été entreprises en matière de cybersécurité :

- Création du Commandement de la cyberdéfense (COMCYBER) en 2017, centralisant les efforts de défense cyber des armées françaises.
- Plan de lutte contre les cyberattaques annoncé en 2021, doté d'un budget d'un milliard d'euros, visant à tripler le chiffre d'affaires de la filière cyber d'ici 2025, doubler le nombre d'emplois dans le secteur, et renforcer la recherche et l'innovation en cybersécurité.
- Développement de l'innovation de nos fournisseurs de sécurité (services et produits) au travers des différents plans de France 2030.
- Impulsion des Cyber Campus à La Défense puis dans les régions pour réunir les compétences et développer la recherche en France.
- Sensibilisation et formation, avec des initiatives pour doubler le nombre d'emplois dans le secteur et promouvoir une culture de la cybersécurité à travers des campagnes de sensibilisation, comme le mois d'octobre dédié à la cybersécurité.

Ces initiatives montrent une stratégie globale et proactive, allant de la protection des infrastructures critiques à l'éducation et la coopération internationale. Ne laissons pas la cybersécurité être notre talon d'Achille. Transposons la directive NIS2, non pas parce que nous le devons, mais parce que nous le pouvons, et devons le faire, pour la sécurité et la compétitivité de la France.

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la cybersécurité.

Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.

Le CESIN compte plus de 1 000 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120. Pour en savoir plus www.cesin.fr