VERS LA DIRECTIVE NIS 2

Vincent Ceriani – Head of CyberRisk Services

vincent.ceriani@nrb.be

NRB

DARING TO COMMIT

Agenda

- Introduction
- CyberSécurité : la nouvelle normalité
- NIS vers NIS2
- Qui doit se conformer à NIS2 ?
- Le signalement d'incident
- La transition vers NIS2 ?

Introduction

VERS LA DIRECTIVE NIS2

NRB

DARING TO COMMIT

Introduction

Directive NIS2

Depuis le 16 janvier 2023, la directive européenne dénommée ci-après NIS2 est en vigueur.

Il s'agit de la Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (modifiant le règlement (UE) n°910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148).

Cette directive succède à la directive NIS1 (transposée en droit belge principalement par la loi du 7 avril 2019) et a été proposée par la Commission européenne en décembre 2020.

Après un processus de négociation, elle a été adoptée par le Conseil et le Parlement européen le 14 décembre 2022 pour être publiée officiellement le 27 décembre 2022.

Désormais, chaque Etat membre de l'Union européenne aura jusqu'au 17 octobre 2024 pour transposer la directive NIS2 dans sa législation nationale.

CyberSécurité : la nouvelle normalité

VERS LA DIRECTIVE NIS 2

NRB

DARING TO COMMIT

CyberSécurité : la nouvelle normalité

- La directive NIS initiale a imposé un changement significatif vers l'amélioration de la cybersécurité, mais le cadre nécessite une révision constante pour refléter l'évolution du paysage des menaces. C'est pourquoi la directive NIS2 a été publiée afin d'aligner ses attentes et ses recommandations.
- L'intention de la Commission européenne avec la mise à jour de la législation est de :
  - Renforcer le cadre réglementaire en matière de cybersécurité
  - Obliger les autorités nationales à consacrer l'attention nécessaire à la cybersécurité
  - Assurer une application uniforme dans les États membres
  - Mettre en place une gouvernance efficace au niveau européen
  - Renforcer la coopération européenne entre les autorités de cybersécurité
  - Imposer aux principaux opérateurs des secteurs clés de notre société la prise de mesures de sécurité et la notification d'incidents

NRB DARING TO COMMIT vincent.ceriani@nrb.be

CyberSécurité : la nouvelle normalité

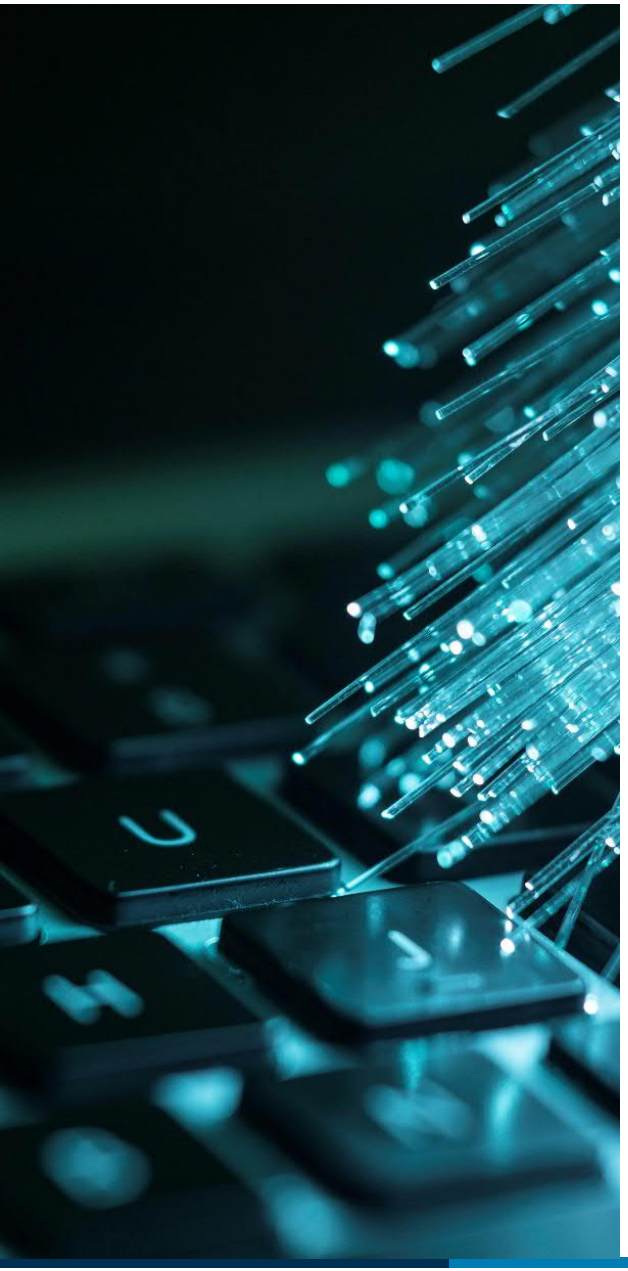
- Les principaux changements concernent :
  - Redéfinition et extension du champ d'application
  - Renforcement des mesures de gestion des risques en matière de cybersécurité
  - Rationalisation et simplification des exigences minimales de sécurité et de l'obligation de signaler les cyberattaques
  - Renforcement des activités de surveillance au niveau européen avec l'introduction de nouveaux organes de surveillance
  - Nouvelles obligations visant à assurer une plus grande sécurité des chaînes d'approvisionnement en étendant la gestion des risques et l'évaluation de la vulnérabilité aux fournisseurs de services couverts par la directive NIS2
  - Un régime de sanctions harmonisé et plus sévère

NIS vers NIS2

VERS LA DIRECTIVE NIS 2

NRB

DARING TO COMMIT



NIS vers NIS2

Exigences minimales

- Analyser et évaluer les risques de sécurité pour les systèmes informatiques
  - Gestion des cyberattaques : prévention, détection, identification, confinement, atténuation et réponse
  - Assurer la continuité des activités et la gestion des crises
  - Assurer la sécurité de la chaîne d'approvisionnement en vérifiant les exigences de sécurité des fournisseurs et en empêchant qu'une attaque sur le réseau principal ne se propage à ces fournisseurs
  - Assurer la sécurité dans le développement et la maintenance des systèmes d'information
  - Assurer la sécurité des réseaux et des systèmes d'information par l'évaluation des vulnérabilités, les tests de pénétration, les simulations d'attaques et d'autres activités similaires
  - Tester et évaluer l'efficacité des mesures de gestion des risques liés à la sécurité informatique

Qui doit se conformer à NIS2 ?

VERS LA DIRECTIVE NIS 2

NRB

DARING TO COMMIT

Qui doit se conformer à NIS2 ?

SECTEURS CRITIQUES DANS LE CADRE DE LA DIRECTIVE

NIS

- Infrastructure numérique et fournisseurs de services numériques
- Énergie, pétrole et gaz
- Réseaux d'approvisionnement en eau
- Santé
- Transport
- Finances

NIS2

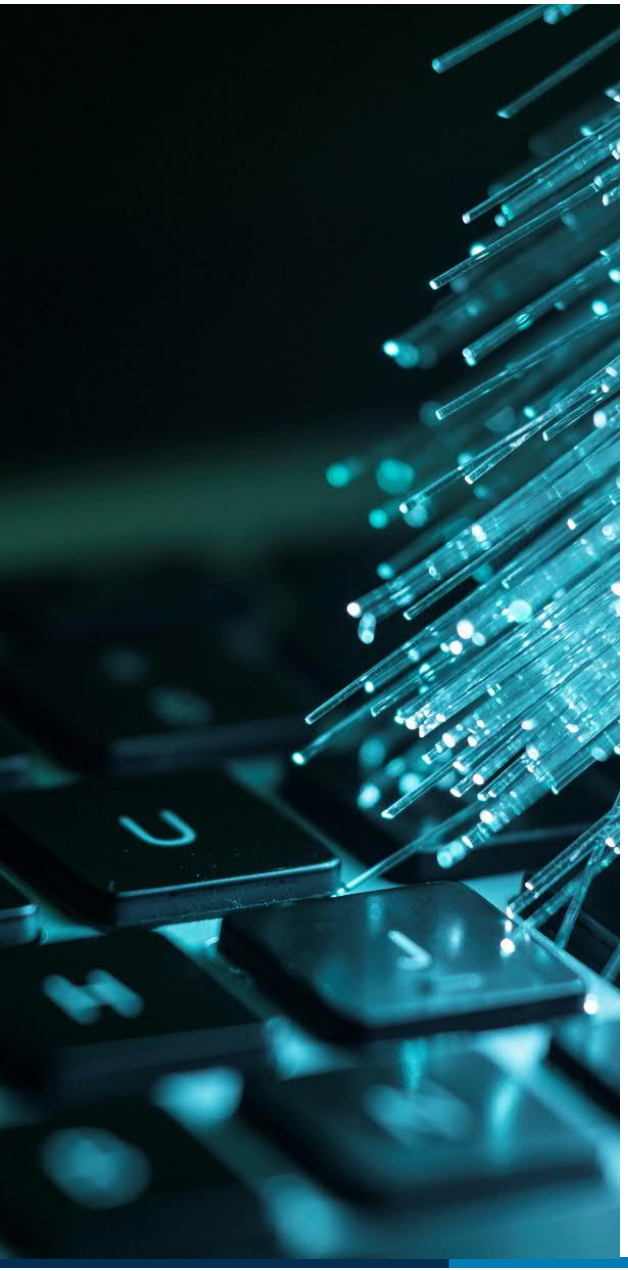
- Administration publique
- Fournisseurs de services publics de communications électroniques
- Gestion des déchets
- Aérospatiale
- Produits critiques (médicaments, dispositifs médicaux, produits chimiques, etc.)
- Services postaux
- Chaîne d'approvisionnement agroalimentaire
- Autres plateformes de services numériques (par exemple, centres de données et médias sociaux)

Qui doit se conformer à NIS2 ?

Entités essentielles et importantes

La directive NIS2 défini deux types d'entités : "essentielles" et "importantes".

- Les entités essentielles pourraient coïncider avec les domaines de l'énergie, des transports, de la banque et de la finance, de l'eau potable, des eaux usées, de l'infrastructure numérique, de la santé, de l'aérospatiale et de l'administration publique.
- Les entités importantes pourraient être des organisations dans les services postaux, la gestion des déchets, l'industrie chimique, l'industrie agroalimentaire et les fournitures numériques non classées comme entités essentielles.



NIS2 : les sanctions

Les violations en matière de mesures de gestion des risques ou de notification d'incident pourront être punies:

- pour les entités essentielles à des amendes administratives d'un montant maximal s'élevant à au moins 10 millions EUR ou à au moins 2% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu;

- pour les entités importantes à des amendes administratives d'un montant maximal s'élevant à au moins 7 millions EUR ou à au moins 1,4% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu.

Le signalement d’incident

VERS LA DIRECTIVE NIS 2

NRB

DARING TO COMMIT

Le signalement d'incident

Obligations d'information et de notification d'incident

Les entités essentielles et importantes devront notifier, sans retard injustifié, aux autorités nationales compétentes (notamment le CSIRT national – en Belgique le CCB) tout incident ayant un impact significatif sur la fourniture des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la directive.

Les entités doivent déclarer les incidents dans les 72 heures afin de faciliter la réaction des CSIRT pour contenir la cybermenace (alignement avec les règles RGPD).

Un incident significatif est un incident qui :

1° soit a causé ou est susceptible de causer une perturbation opérationnelle grave des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la directive ou des pertes financières pour l'entité concernée; ou

2° a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

« Les entreprises qui fournissent des services considérés comme essentiels pour le bien-être du système économique et social du pays sont tenues de signaler tout incident majeur ou cybermenace significative (NIS 2), même s'ils découlent de vulnérabilités de fournisseurs tiers »

Le scénario NIS2 n'a pas encore été défini, mais l'objectif du législateur semble clairement être de susciter un plus grand engagement général dans les activités de notification par rapport à la directive NIS initiale. À tout moment, les autorités compétentes ou le Computer Security Incident Response Team (CSIRT) peuvent demander des rapports plus spécifiques aux organisations participantes.

Le signalement d'incident

Le rapport

- Les rapports d'incident doivent contenir suffisamment de détails sur l'attaque elle-même. À l'aide d'outils et de technologies appropriés, l'équipe doit retracer les événements sur le réseau, les points finaux et les journaux des systèmes afin d'identifier toutes les données et métadonnées pertinentes pour aider à reconstituer la chaîne d'attaque, le scénario, l'entité et toute autre information pertinente.

- Le délai de soumission des rapports est généralement de quelques heures et dépend du type d'attaque et des spécifications de la législation nationale de chaque pays.

- Après l'incident, l'entreprise concernée doit envoyer un rapport final contenant une description détaillée et complète de ce qui s'est passé, ainsi que des dommages directs et indirects causés à l'entreprise ou à des tiers.

- Le rapport doit également contenir une description technique de l'attaque, les causes possibles, les mesures mises en œuvre pour en atténuer les effets et le plan d'amélioration à mettre en place pour réduire le risque de récurrence.

La transition vers NIS2

VERS LA DIRECTIVE NIS 2

NRB

DARING TO COMMIT

Transition vers NIS2

ISO 27001

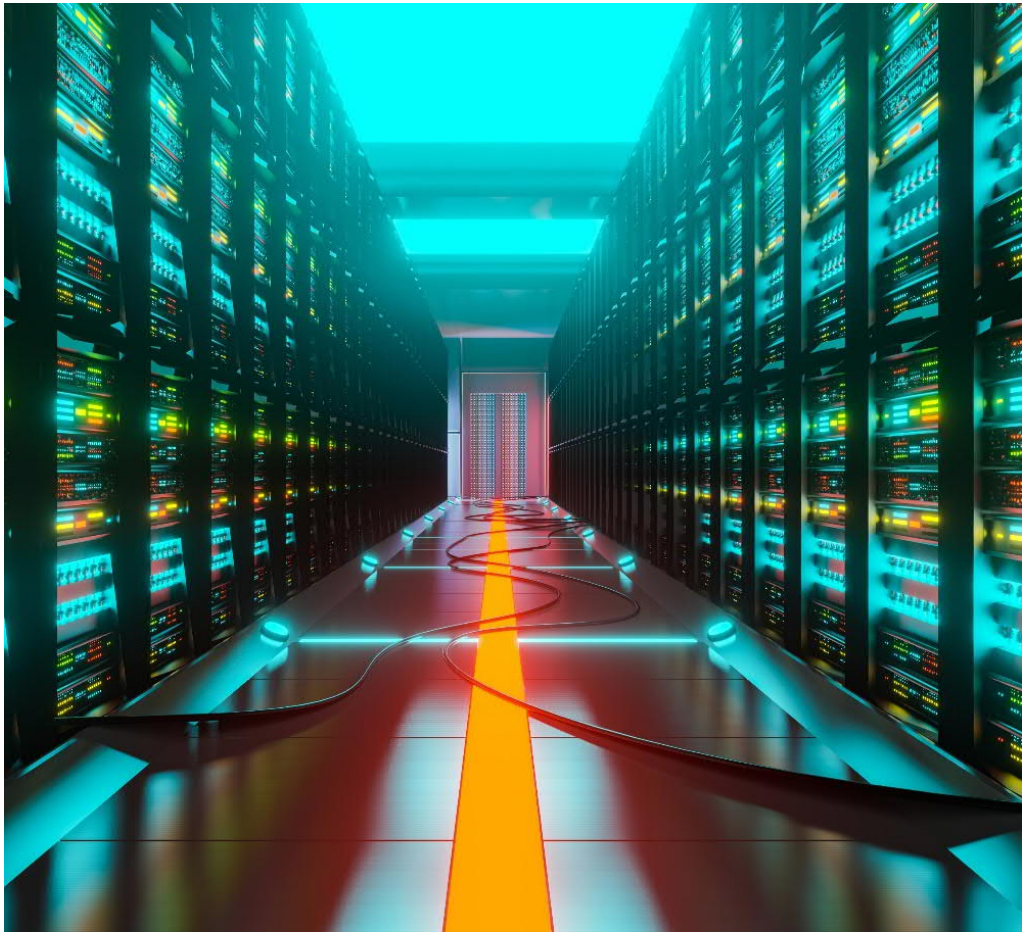
Gestion des cyberattaques	• prévention, détection, identification, confinement, atténuation et réponse – SOC/SIEM - CSIRT
Continuité des activités	• Plan de continuité des activités (BCP / ISO22301)
Sécurité développement et la maintenance	•DevSecOps - OWASP
Sécurité des réseaux et des systèmes d'information	• Evaluation des vulnérabilités, les tests de pénétration, les simulations d'attaques et d'autres activités similaires
Tester et évaluer l'efficacité des mesures de gestion des risques liés à la sécurité informatique	•Analyse de risques, plans de mitigation, tableTop, Audit interne

La transition vers NIS2

Synthèse

- La Belgique devra adopter et publier de nouvelles dispositions remplaçant la loi NIS existante au plus tard pour le 17 octobre 2024 sur la base de la nouvelle directive.
- En tout état de cause, les nouvelles obligations pour les entités concernées ne devraient entrer en vigueur qu'à l'échéance du délai de transposition (octobre 2024).
- Il est toutefois utile pour les entreprises de se préparer dès à présent aux obligations générales découlant de la directive, sans attendre la loi de transposition, en tenant compte des menaces et des risques croissants.
- Par conséquent, nous ne pouvons que recommander aux entités qui seront manifestement soumises à ces nouvelles obligations d'entamer (ou de poursuivre) leurs efforts pour augmenter leur niveau de cybersécurité .
- Plus d'informations :

https://ccb.belgium.be/fr/la-directive-nis2-que-cela-signifie-il-pour-mon-organisation




NRB
DARING TO COMMIT