rubrik

GUIDE CONSACRÉ À LA NIS2

Réglementations sur la sécurité des réseaux et systèmes d'information

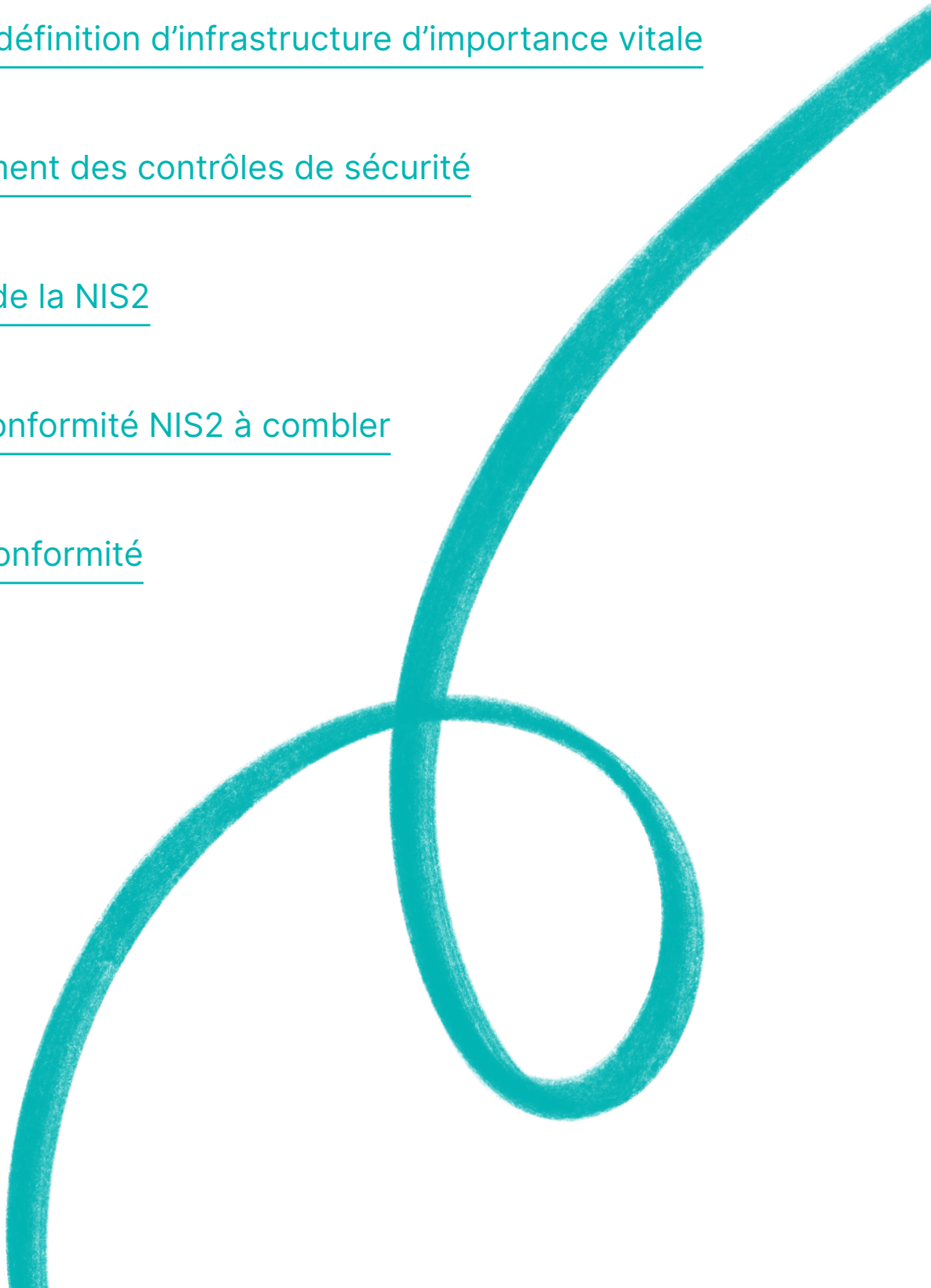
rubrik

Explosion des cybermenaces, développements technologiques, pandémies, catastrophes naturelles… nos infrastructures d'importance vitale sont sans cesse mises à rude épreuve.

La deuxième mouture de la directive sur la sécurité des réseaux et systèmes d'information, ou NIS2, est la dernière d'une longue liste de réglementations sur la protection des données. Elle s'applique en particulier aux entités traitant avec toute structure de l'Union européenne (UE) et du Royaume-Uni considérée comme opérateur d'importance vitale (OIV) dans son pays d'implantation.

Ce guide consacré à la NIS2 vous aidera à faire de ce nouveau cadre réglementaire un levier de cyber-résilience.

Sommaire



Remplacement de la NIS par la NIS2

La directive sur la sécurité des réseaux et de l'information (NIS) fut le premier texte législatif sur la cybersécurité au niveau de l'Union européenne. Son objectif était d'harmoniser les pratiques pour atteindre un haut niveau de cybersécurité dans toute l'UE. Bien que la directive ait renforcé les capacités des organisations dans ce domaine, sa mise en œuvre s'est avérée difficile, ce qui a entraîné une fragmentation à différents niveaux parmi les organisations basées dans l'UE.

La Commission européenne a alors identifié certaines failles dans la directive NIS, notamment :

- Une cyber-résilience insuffisante des entreprises de l'UE
- Une résilience inégale au sein des États membres et des secteurs d'activité
- Un manque de compréhension commune des menaces
- Une absence de réponse commune en cas de crise

Pour répondre aux menaces qu'engendrent la transformation numérique et l'augmentation des cyberattaques, l'UE a substitué la directive NIS par la directive NIS2 dans le but de resserrer les exigences en matière de sécurité, d'assurer la sécurité des chaînes d'approvisionnement (supply chains), de rationaliser les obligations de déclaration, et d'introduire des mesures de surveillance et des exigences de mise en application plus strictes, y compris par une harmonisation des sanctions à l'encontre d'organisations contrevenantes exerçant dans l'UE. [Source]

« La directive NIS2 est à la cybersécurité européenne ce que le RGPD est à la protection des données européennes. »

RICHARD CASSIDY, RSSI

Extension de la définition d'infrastructure d'importance vitale

La directive NIS2 impose des obligations plus strictes en matière de cybersécurité pour la gestion des risques, les obligations de déclaration et le partage d'informations. Les exigences couvrent entre autres la réponse à incident, la sécurité des chaînes d'approvisionnement, le chiffrement et la divulgation des vulnérabilités. La directive NIS2 élargit également le nombre de secteurs couverts, qui passe de 7 à 15, et introduit les catégories « entités essentielles » et « entités importantes ».

« La directive NIS2 élargit également le périmètre d'application à un plus grand nombre d'entités opérant dans des infrastructures d'importance vitale. »

RICHARD CASSIDY, RSSI

	Entités essentielles	Importantes
Taille de l'organisation	• Plus de 250 employés OU • Chiffre d'affaires annuel de 50 millions d'euros ou bilan comptable de 43 millions d'euros	• Plus de 50 employés OU • Chiffre d'affaires annuel de 10 millions d'euros ou bilan comptable de 10 millions d'euros
Secteur	• Énergie • Transport • Banque • Infrastructures des marchés financiers • Santé • Eau potable • Eaux usées • Infrastructure numérique • Gestion des services TIC • Entités de l'administration publique (à l'exception du pouvoir judiciaire, du parlement et des banques centrales)	• Services postaux et de messagerie • Gestion des déchets • Fabrication, production et distribution de produits chimiques • Production, transformation et distribution de denrées alimentaires • Fabrication d'appareils médicaux, de produits électroniques et de moyens de transport • Fournisseurs de services numériques • Recherche

Chaque réglementation s'accompagne d'un risque de sanctions en cas d'infraction. Au vu du montant des amendes qu'elles encourent, les organisations doivent s'interroger sur le coût et les implications respectifs de la conformité et de la non-conformité NIS2. Pour chacune des catégories, le montant de l'amende varie :

	Entités essentielles	Importantes
Montant de l'amende	• Une amende maximale de 10 000 000 € ou à hauteur de 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.	• Une amende maximale de 7 000 000 € ou à hauteur d'au moins 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

NIS2 : renforcement des contrôles de sécurité

Un grand nombre de réglementations et de cadres législatifs peuvent être considérés comme laborieux et contraignants, dans la mesure où ils mobilisent beaucoup de ressources pour cocher les cases, sans pour autant apporter une réelle valeur ajoutée aux organisations. La directive NIS2 aide réellement les organisations à renforcer leurs contrôles de sécurité.

> « Cette directive européenne aidera environ 160 000 entités à renforcer leurs contrôles en matière de sécurité. »

BART GROOTHUIS, MEMBRE DU PARLEMENT EUROPÉEN

Outre le fait qu'elle améliore la directive NIS existante, l'idée principale de la NIS2 est de recentrer la focale sur certains éléments qui méritent une attention particulière. Prenons l'exemple de la gestion des menaces et des incidents. En cas de compromission, plus vite vous partagez des informations avec vos homologues et autres organisations pour permettre une réponse collective à l'incident, meilleure sera la cyber-résilience. C'est une amélioration considérable en matière de partage d'informations à travers de multiples secteurs. Beaucoup des législations précédentes étaient axées sur la FinTech et la finance en général, ou avaient une portée trop vaste et étaient trop difficiles à définir. Avec la NIS2, l'accent est mis sur les domaines clés qui apporteront des avantages tangibles aux organisations. [Source]

La directive NIS2 constitue un ensemble de contrôles réels, concis et convergents. Elle permet aux entreprises de gérer leurs données de façon exhaustive dans des domaines clés, le but étant d'établir une défense beaucoup plus efficace contre les cybermenaces et de favoriser la reprise des opérations après un cyberincident majeur.

Les cinq piliers de la NIS2

La NIS2 subdivise les secteurs en plusieurs catégories : les entités essentielles et les entités importantes. Si cette catégorisation ne change pas les points sur lesquels vous devez vous aligner pour vous conformer à la NIS2, il existe néanmoins des domaines sur lesquels vous devez porter une attention particulière, en fonction de la catégorie à laquelle vous appartenez.

La NIS2 se compose de 46 articles que vous pouvez retrouver ici. En prenant un peu de hauteur, nous constatons qu'ils reposent sur cinq piliers :

NIS2				
Exigences en matière de sécurité	Traitement des incidents	Continuité de service	Surveillance, audit et tests	Conformité aux normes internationales

C'est sur les piliers suivants que nous constatons les plus grands changements du point de vue des technologies et des processus : traitement des incidents, surveillance, audit et test, et continuité de service. Un grand nombre de nouvelles fonctions et caractéristiques parmi ces trois piliers obligeront les entreprises à repenser leurs stratégies de cybersécurité et de cyber-résilience, ainsi que la manière dont elles partagent les données à l'extérieur de l'organisation.

En matière de cybersécurité, les organisations sont souvent à la tête d'écosystèmes de sécurité certes très complets, mais également complexes, cloisonnés et conçus pour agir au service de fonctions opérationnelles spécifiques. Avec la directive NIS2, les organisations doivent considérablement améliorer leurs pratiques de partage des données avec les autorités de surveillance européennes et les autres organisations entrant dans le dispositif NIS2. Ce niveau d'échange d'informations permettra d'accroître l'efficacité de la résilience opérationnelle et de la reprise des activités.

« Les ransomwares et autres cybermenaces frappent les organisations européennes depuis bien trop longtemps. Nous devons agir pour renforcer la résilience de nos entreprises, nos administrations et notre société tout entière face aux opérations cybernétiques hostiles. »

BART GROOTHUIS,
MEMBRE DU
PARLEMENT EUROPÉEN

Les écarts de conformité NIS2 à combler

Où les organisations ont-elles le plus grand écart à combler pour se préparer à l'entrée en vigueur de la directive NIS2 ?

Si on examine les cinq piliers de la directive NIS2, on constate que la plupart des organisations, si ce n'est toutes, ont un écosystème très cloisonné en termes de gestion des exigences de sécurité. Ceci va de la notification initiale d'un incident jusqu'à son traitement, en passant par le partage d'informations entre organisations d'une même branche.

Pilier n°1 : les exigences de sécurité sont un domaine dans lequel la plupart des organisations ont atteint un haut degré de maturité.

Pilier n°2 : à l'instar des exigences de sécurité, la gestion des incidents est également un domaine dans lequel de nombreuses organisations auront des pratiques bien établies. Elles sont habituées à gérer les incidents depuis déjà longtemps, que ce soit en interne ou via un prestataire externe. Dans ce domaine, vous devrez certainement adapter et modifier vos outils et politiques de traitement des incidents par rapport aux exigences de la directive NIS2. Toutefois, dans la plupart des organisations, les dispositifs devraient déjà être en place.

Pilier n°3 : la continuité de service est un domaine où vous constaterez probablement d'importantes lacunes et où vous devrez consacrer du temps et des ressources pour vous mettre à jour. Beaucoup d'organisations ne sont pas prêtes ou n'ont pas les capacités de cyber-résilience en place, principalement parce qu'elles confondent souvent sauvegardes de données et cyber-résilience, ou parce qu'elles sont convaincues que leur fournisseur de services cloud (CSP) offre une sécurité suffisante. La véritable cyber-résilience consiste à élaborer et à tester son propre plan de résilience opérationnelle et de reprise d'activité.

Pilier n°4 : surveillance, audit et tests.

Pilier n°5 : conformité aux normes internationales. Pour ces deux piliers, les organisations devront se concentrer sur la manière dont les données sont acquises, sur leur origine et sur le cadre juridique de leur partage en vertu de la NIS2.

« Nous devons renforcer la résilience collective des systèmes critiques qui sous-tendent nos modes de vie. »

MICHAEL ŠIMEČKA, MEMBRE DU PARLEMENT EUROPÉEN

La course à la conformité

Les organisations ont jusqu'au 17 octobre 2024 pour se conformer à la directive NIS2. Mais ne vous y trompez pas : c'est maintenant qu'il faut mettre vos affaires en ordre ! Cela étant dit, la directive NIS2 implique-t-elle une refonte totale de l'ensemble de votre structure de cybersécurité ? Pas nécessairement.

> « Faut-il se dépêcher ? Oui. Vous avez jusqu'à octobre 2024 pour vous y conformer. »
>
> **RICHARD CASSIDY,** RSSI DE RUBRIK

Le plus grand défi de la NIS2 ? Elle est obligatoire pour les OIV. Nul ne peut y échapper. Et l'élan doit venir d'en haut, du conseil d'administration. Celui-ci devra examiner attentivement les projets prévus pour les 12 à 18 prochains mois et les aligner sur la directive NIS2. La mise en œuvre de la NIS2 peut être considérée comme tout autre projet, à la différence près qu'il s'agit d'un grand chantier stratégique à lancer au plus vite. Amendes administratives, sanction non pécuniaires, condamnations pénales… tout défaut de conformité peut avoir de graves conséquences. Sans compter une éventuelle interdiction de transacter avec d'autres entités soumises à la NIS2 au sein de l'Union européenne.

La bonne nouvelle ? Un grand nombre de projets IT en cours ou à l'étude prévoient déjà un dispositif de redémarrage à zéro de l'ensemble des opérations métiers en cas de défaillance majeure ou de scénario de reprise après sinistre. Vous constaterez donc que les capacités en place répondent à de nombreuses exigences de la NIS2. Pour vous aider à déterminer votre état de conformité actuelle à la directive NIS2, nous vous recommandons de suivre les trois étapes suivantes :

1. **Périmètre NIS2 applicable :** déterminez le périmètre et la catégorie NIS2 dont relève votre organisation, ainsi que les départements concernés de votre entreprise.
2. **Couverture NIS2 :** évaluez les mesures et les politiques de sécurité déjà en place et recadrez-les, si nécessaire, sur les exigences de la directive NIS2.
3. **Analyse des écarts :** analysez et identifiez les mesures et politiques de sécurité à mettre en place pour se conformer à la NIS2. Dans le domaine de la chaîne d'approvisionnement, les obligations de déclaration d'incidents sont le point à résoudre rapidement afin d'éviter tout retard dans votre mise en conformité.

Conseil : concentrez-vous sur les fournisseurs et sous-traitants de la chaîne, un domaine facilement négligé et souvent ciblé par les cyberattaquants.

Conclusion

Ce qu'il faut retenir, c'est que vous avez peut-être déjà mis en place une grande partie des exigences de conformité à la directive NIS2. Pour ceux qui partiraient de plus loin, vous vous simplifierez la tâche en effectuant une bonne analyse des écarts et en collaborant avec des fournisseurs de technologies et de services. Souvenez-vous : la directive NIS2 a été créée pour vous aider, alors utilisez-la à votre avantage !

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com