LIVRE BLANC

La mise en conformité à la directive NIS2 – le Zero Trust doit être un élément essentiel de cette démarche

Sommaire

Note de synthèse

Directive NIS2 et rôle du Zero Trust pour renforcer la cyber-résilience

L'adoption de la Network and Information Security Directive 2 (Directive NIS2) marque une évolution importante dans l'engagement de l'Union européenne (UE) à renforcer la cybersécurité dans ses États membres. NIS2 remplace la directive NIS précédente et étend son champ d'application à un éventail plus large de secteurs et de sous-secteurs d'activité, tout en renforçant les exigences de sécurité, notamment en élevant la cybersécurité au rang d'impératif de gestion et de gouvernance. Bien que la directive NIS2 soit entrée en vigueur en 2023 c'est à l'horizon d'octobre 2024, que les États membres de l'UE doivent l'avoir retranscrite et appliquée au plus tard dans leur législation nationale. Étant donné que l'application de la directive NIS2 peut varier légèrement entre chaque État membre, ce livre blanc se concentre sur les exigences et les principes généraux de la directive elle-même.

Aucun fournisseur/éditeur de solution ou de logiciel ne peut garantir la conformité à la NIS2. Cependant, l'adhésion aux principes du Zero Trust (une bonne pratique d'ailleurs suggérée par la directive elle-même) répond à un certain nombre de critères imposés par NIS2. Le déploiement d'une architecture Zero Trust au sein de l'environnement d'une entreprise, des composantes de son réseau distribué et des réseaux de tiers peut radicalement réduire les surfaces d'attaque et lever une série de freins techniques susceptibles d'entraver les efforts de mise en conformité avec la directive NIS2. Le Zero Trust devrait être l'un des principaux leviers utilisés par les entreprises pour améliorer leur résilience. C'est précisément le rôle d'un partenaire fournisseur du Zero Trust d'accompagner les entreprises dans leur démarche de mise en conformité.

Le processus de mise en conformité doit être structuré et communiqué au sein de toutes les entreprises concernées par la nouvelle directive. De récentes enquêtes menées par Zscaler auprès d'équipes informatiques européennes ont évalué l'état de préparation des entreprises à l'entrée en vigueur de la directive.
71 % des responsables informatiques interrogés estiment que la modernisation de la sécurité exige un changement majeur d'état d'esprit, bien plus qu'un simple exercice de mise en conformité.

Cependant, les attitudes des différentes parties prenantes impliquées dans la mise en conformité varient considérablement. Alors que 80 % des responsables informatiques interrogés sont convaincus que leur entreprise sera conforme à la date limite, seuls 53 % pensent que leurs équipes comprennent pleinement la portée des obligations prévues par NIS2. Lorsqu'on leur demande si les dirigeants de leur entreprise comprennent les exigences de conformité, ce chiffre tombe à 49 %. Plus de 60 % des personnes interrogées estiment que NIS2 impliquera un changement important par rapport à leur stratégie de sécurité actuelle.

Expert de la sécurité du cloud, Zscaler est idéalement positionné pour aider les entreprises à s'y retrouver parmi les changements induits par NIS2. En adoptant l'architecture Zero Trust de Zscaler, les entreprises, quelle que soit leur envergure, peuvent se conformer aux exigences fondamentales de la directive, pour ainsi améliorer leurs mécanismes de défense, réduire leur exposition aux risques cyber et simplifier leurs tâches de mise en conformité. Les principes du Zero Trust sont dans le droit fil des objectifs de NIS2 : les droits d'accès superflus sont éliminés, toutes les connexions sont rigoureusement vérifiées tandis que l'impact potentiel des incidents de sécurité est minimisé. Zscaler fournit une palette de fonctionnalités et d'outils qui accompagnent les efforts de mise en conformité avec les dispositions spécifiques de NIS2, notamment l'application des politiques, la détection des incidents et les processus de réponse.

Directive NIS2 et périmètre d'application

NIS2 est entrée en vigueur en 2023 et la date limite de sa transposition et de son application pour les États membres de l'UE est fixée à octobre 2024. Les responsables politiques de l'UE ont adopté cette nouvelle législation essentielle en réponse au besoin de l'UE d'améliorer sa cyber-résilience à une époque où les cyber-attaques contre les citoyens, les entreprises et les économies européennes se multiplient. NIS2 souligne la responsabilité des entités d'assurer la sécurité des réseaux et des systèmes d'information, en les appelant à adopter une culture de gouvernance et de framework complet de gestion des risques. NIS2 s'inscrit dans une tendance croissante au sein de l'UE à réglementer directement les efforts de cyber-résilience. (Par exemple, la loi sur la résilience opérationnelle numérique (DORA), qui entrera en vigueur en janvier 2025, est un framework distinct pour la gestion et la maîtrise des risques liés aux TIC dans le secteur financier.)

La directive NIS2 s'adresse à de nouveaux secteurs d'activité, ainsi que de nouveaux profils d'entités au sein des secteurs concernés par la première version de NIS. Cet élargissement répond à la prise de conscience croissante qu'un large éventail d'activités économiques et sociétales dépendent de manière critique de l'infrastructure informatique, que les cybermenaces pesant sur ces secteurs se multiplient et que les perturbations peuvent avoir un effet domino dans toute l'UE.

Les secteurs d'activité sont catégorisés dans NIS2 comme « essentiels » ou « importants », pour refléter leur criticité ou le service qu'ils fournissent. Bien que les exigences de cybersécurité et de déclaration des incidents soient les mêmes pour les deux profils de secteurs, les deux catégories d'entités seront soumises à des régimes de surveillance et de mise en oeuvre légèrement différents, notamment en ce qui concerne le montant des amendes potentielles en cas de non-conformité (plus de détails ci-dessous).

> « À l'approche de la date formelle d'entrée en vigueur, les entreprises doivent accélérer leurs efforts de mise en conformité, ce qui peut se faire au détriment d'autres aspects essentiels de la cybersécurité. 60 % des participants à l'enquête craignent que les efforts majeurs investis dans la mise en conformité avec NIS2 ne conduisent à négliger d'autres volets essentiels de la sécurité. Il est par conséquent impératif que les dirigeants d'entreprise apportent un soutien solide aux services informatiques, pour assurer une approche globale à la conformité qui maîtrise les risques de vulnérabilités et de perturbations opérationnelles. »
>
> **James Tucker,** Responsable des RSSI EMEA en résidence chez Zscaler

Secteurs et sous-secteurs concernés par NIS2[1]

Entités essentielles (« secteurs très critiques »)	
Énergies	Électricité, pétrole, gaz, chauffage urbain et refroidissement, hydrogène...
Transport	Transports aériens, ferroviaires, maritimes et routiers.
Banques (établissements de crédit)	
Infrastructures des marchés financiers	
Santé	Soins de santé et produits pharmaceutiques.
Traitement de l'eau potable	
Traitement des eaux usées	
Infrastructures numériques	Fournisseurs de points d'échange Internet (IXP), fournisseurs de services DNS, registres de noms de domaine de premier niveau, fournisseurs de services de cloud computing, fournisseurs de services de data center, fournisseurs de réseaux de diffusion de contenu, fournisseurs de services de confiance, fournisseurs de réseaux de communications électroniques publics et fournisseurs de services de communications électroniques accessibles au public.
Gestion des services TIC (B2B)	Fournisseurs de services managés et fournisseurs de services de sécurité managés.
Administrations publiques	Administrations publiques d'état et territoriales telles que définies par les législations nationales des États membres.
Espace (opérateurs d'infrastructures terrestres)	
Entités importantes (« Autres secteurs critiques »)	
Services postaux et de livraison	
Gestion des déchets	
Fabrication, production et distribution de produits chimiques	
Production, transformation et distribution de produits alimentaires	
Production industrielle	Produits manufacturés tels que les appareils médicaux, les produits informatiques et électroniques, les équipements électriques, les machines et équipements, les véhicules à moteur, les équipements de transport...
Fournisseurs de services numériques	Opérateurs de places de marché en ligne, fournisseurs de moteurs de recherche en ligne et fournisseurs de plateformes de services de réseaux sociaux.
Organismes de recherche	

1. Il existe quelques exceptions à ces catégories ; consultez les annexes I et II de la directive pour plus de détails. Les administrations d'état dont les activités sont principalement liées à la sécurité nationale, à la sécurité publique, à la défense ou aux forces de l'ordre sont également exclues. En outre, la directive s'applique uniquement aux entités qualifiées de « moyennes entreprises » dans l'UE (entreprises comptant plus de 250 personnes et réalisant un chiffre d'affaires annuel supérieur à 50 millions EUR). Par ailleurs, certaines exceptions appliquent la NIS2 à certaines entités plus petites.

Directive NIS2 : Approche Zero Trust de Zscaler

La plateforme Zero Trust Exchange™ de Zscaler simplifie la sécurité réseau traditionnelle, ce qui permet aux entreprises de répondre plus facilement aux exigences de la directive NIS2. Zero Trust Exchange™ est une architecture cloud native, basée sur le SASE, qui a été conçue spécialement pour les environnements business mondiaux qui présentent une diversité des besoins technologiques et opérationnels. La mise en œuvre d'une segmentation granulaire pour cloisonner un réseau, des accès sur la base du moindre privilège (restrictions des autorisations des utilisateurs) et un monitoring continu du trafic sont autant de mesures proactives qui aident à identifier et contrer les acteurs malveillants, minimisant ainsi les dommages potentiels et l'impact des attaques.

Zero Trust Exchange™ permet également aux entreprises de réduire leur surface d'attaque, de prévenir tout déplacement latéral de menaces et de réduire les risques d'intrusion, ceci étant possible grâce à une dissociation de la sécurité et de l'infrastructure réseau. Les utilisateurs se connectent ainsi en toute sécurité aux applications sans rendre leur réseau visible depuis Internet, ce qui réduit considérablement le risque d'attaques. Les capacités de la plateforme accompagnent les efforts de conformité requis dans le cadre de NIS2 pour le traitement sécurisé des données, le contrôle d'accès et la gestion des incidents.

La plateforme renforce la sécurité selon différents axes : protection de l'ensemble du trafic, des utilisateurs et des appareils, neutralisation des menaces en temps réel et inspection complète du trafic. Zscaler améliore également la productivité des administrateurs grâce à une gestion globale et à une administration des politiques unifiée, ce qui élimine le besoin de maintenance matérielle et permet de se recentrer sur des projets à plus forte valeur ajoutée. La plateforme Zscaler améliore les performances Internet pour les utilisateurs finaux et les connexions directes à Internet, ainsi que la conformité aux principaux frameworks de sécurité tels qu'ISO 27001 et SOC2 Type II. Il en résulte une meilleure expérience utilisateur et une posture de sécurité renforcée. De plus amples détails concernant le Zero Trust et l'approche de Zscaler en matière d'architecture Zero Trust sont disponibles sur la page Zpedia de Zscaler.

Directive NIS2 : L'approche de Zscaler

L'approche globale de Zscaler en matière de sécurité et de conformité nous permet de réagir rapidement et de nous aligner sur les réglementations existantes, nouvelles et émergentes telles que NIS2. Le programme interne de gestion des risques de cybersécurité de Zscaler garantit le respect de normes internationalement reconnues telles qu'ISO 27001 et SOC 2. Le respect de ces normes fondamentales permet à Zscaler d'intégrer de manière efficace un ensemble diversifié de fonctions de sécurité destinées à identifier, prévenir et détecter les menaces, à partir de nos produits et services. La réponse aux menaces et la restauration sont également assurées. Zscaler tire parti d'un panel commun et structuré de fonctionnalités et de compétences fondamentales en cybersécurité telles que la mise en place d'un programme de gestion des risques liés à la sécurité de l'information, des pratiques de sécurisation de la supply chain, la gestion des risques liés à des tiers, les évaluations continues des risques, la déclaration des incidents, la divulgation des vulnérabilités, etc. Une liste à jour des normes de sécurité et de conformité sur lesquelles intervient Zscaler est disponible sur la **page dédiée à la conformité de Zscaler**.

En outre, Zscaler gère le **portail** Zscaler Trust pour fournir aux clients des perspectives en temps réel sur les opérations de Zscaler. Ce portail est aussi un forum de communication sur les **incidents** et les **recommandations de Zscaler**.

Principaux domaines de conformité à la directive NIS2 et comment Zscaler vous aide

La directive NIS2 définit la responsabilité des entités pour assurer la sécurité des réseaux et des systèmes d'information, en les appelant à adopter une culture de gouvernance et des frameworks de gestion des risques éprouvés, complets et bien intégrés. Pour tenir ces objectifs, NIS2 exige des mesures de gestion des risques de cybersécurité, des mesures de gouvernance, une déclaration des incidents, ainsi que des mesures de monitoring et d'application de règles, toutes décrites ci-dessous.

Dans l'enquête mentionnée ci-dessus, menée auprès de professionnels européens de l'informatique, 56 % des personnes interrogées déclarent que leurs équipes ont le sentiment de manquer de soutien de la part de leurs dirigeants pour respecter la date limite de mise en conformité avec NIS2. Pour accompagner la conformité, les responsables informatiques interrogés déclarent que les changements les plus importants à apporter dans leurs entreprises dont les suivants :

- Actualiser le panel de solutions technologiques et de cybersécurité : 34 %
- Former les collaborateurs : 20 %
- Former les dirigeants : 17 %

Mesures de NIS 2 en matière de gestion des risques de cybersécurité

Les entités relevant du champ d'application de la directive doivent adopter des mesures techniques, opérationnelles et organisationnelles proactives pour gérer les risques de sécurité des réseaux et systèmes d'information utilisés par ces entités dans le cadre de leurs opérations ou de la fourniture de leurs services. Ces entités doivent également prévenir et minimiser l'impact des incidents sur les bénéficiaires de leurs services et sur les autres services qu'elles sont susceptibles de fournir.

L'article 21 de la directive énumère les mesures à minima de gestion des risques de cybersécurité que les entreprises doivent prendre, tandis que les sections 78 et 89 fournissent plus d'informations sur les attentes des auteurs de ce règlement.

- **L'article 21 (mesures à minima de gestion des risques de cybersécurité)** précise que les entités doivent mettre en œuvre des politiques sur différentes domaines : analyse des risques et de la sécurité des systèmes d'information, continuité des activités et de gestion des crises, sécurité de la supply chain (notamment la qualité et les procédures de conception sécurisée des produits et les pratiques de cybersécurité de leurs fournisseurs et prestataires de services), des pratiques de base en matière d'hygiène informatique et de formation en cybersécurité, des politiques et procédures sur l'utilisation de la cryptographie/du chiffrement, la sécurité des ressources humaines, des politiques de contrôle d'accès et de gestion des ressources, ainsi que l'utilisation de solutions d'authentification multifacteur ou d'authentification en continu.
- **Conformément au considérant 78**, les mesures de gestion des risques de cybersécurité mises en œuvre par les entités relevant du champ d'application de la directive doivent tenir compte du degré de dépendance de l'entité vis-à-vis des réseaux et des systèmes d'information. Ces mesures doivent permettre d'identifier les risques d'incidents, de prévenir, détecter er répondre aux incidents, d'assurer la restauration post-incident et des impacts, de protéger les données stockées, transmises et traitées, ainsi que d'assurer une analyse systémique, en tenant compte du facteur humain.
- **Le considérant 89** exhorte les entités à déployer une série de pratiques de cyber-hygiène sur les domaines suivants : principes du Zero Trust, mises à jour logicielles, configuration des dispositifs, segmentation du réseau, gestion des identités et des accès, ainsi que la formation des collaborateurs et la sensibilisation aux cybermenaces, au phishing ou aux techniques d'ingénierie sociale. Le considérant 89 exhorte également les entités à rechercher des technologies améliorant la cybersécurité, telles que les systèmes d'intelligence artificielle (IA) ou d'apprentissage automatique (AA), pour améliorer leurs capacités et la sécurité des réseaux et des systèmes d'information.

Comment Zscaler peut vous aider : nous décrivons ci-dessous de manière générale l'accompagnement proposé par Zscaler à l'intention des entités souhaitant respecter certains aspects particuliers des dispositions de NIS2. Pour des informations détaillées sur les solutions et outils Zscaler qui facilitent la mise en conformité, veuillez contacter votre représentant Zscaler local. Le contenu général et les livres blancs sur les solutions Zscaler sont disponibles à l'adresse https://www.zscaler.com/fr/resources?type=white-papers.

Gouvernance et gestion des risques selon NIS2

La directive NIS2 fait des dirigeants d'une entité les responsables en dernier ressort de la conformité. Ces dirigeants sont tenus de valider et superviser la mise en œuvre des mesures de gestion des risques de cybersécurité pour leur entité. La direction doit également suivre une formation en cybersécurité et proposer régulièrement des formations similaires aux collaborateurs, afin d'acquérir des connaissances et des compétences suffisantes pour identifier les risques et évaluer les pratiques de gestion des risques de cybersécurité et de leur impact sur les services de l'entité.

Zscaler peut vous aider : Zscaler fournit, avec sa gamme de services, des fonctionnalités de sécurité conçues pour aider les entreprises à minimiser leur surface d'attaque et à garantir l'efficacité des fonctionnalités de sécurité appliquées via le programme de gouvernance et de gestion des risques d'un client.

Zscaler Resilience™ est un panel complet de fonctionnalités qui assure une continuité des activités sans aucune interruption pendant les pannes électriques, les baisses de tension ou les événements catastrophiques imprévisibles.

Zscaler Internet Access (ZIA) et Zscaler Private Access (ZPA) sécurisent les flux de trafic et fournissent des journaux d'événements et de transactions à des fins de corrélation et de gestion, ce qui permet aux entreprises de surveiller et de déjouer efficacement les menaces potentielles.

Zero Trust Exchange™ de Zscaler garantit qu'aucun utilisateur n'est positionné sur le réseau d'entreprise et que les applications ne sont jamais exposées à Internet, ce qui réduit considérablement la surface d'attaque. La solution permet également aux entreprises de créer et d'appliquer des politiques réglementant les sites d'IA générative avec lesquels les utilisateurs peuvent interagir afin de garantir la protection des données sensibles.

Les capacités d'inspection du trafic SSL de Zscaler améliorent davantage la sécurité en déchiffrant le trafic HTTPS pour détecter et neutraliser tout contenu malveillant.

Les offres Risk360™ et Zscaler Posture Control (ZPC) de Zscaler assurent une surveillance continue et une détection des vulnérabilités, ce qui permet aux entreprises de traiter de manière proactive les risques de sécurité.

Zscaler Digital Experience (ZDX) assure le suivi de l'inventaire des appareils, garantissant que les composants de service sont correctement identifiés et désactivés en toute sécurité lorsque cela est nécessaire, ce qui contribue à minimiser la surface d'attaque.

La solution Nanolog Streaming Service (NSS) de Zscaler facilite la communication transparente entre Zscaler Cloud et les dispositifs des solutions de sécurité tierces, permettant la diffusion en temps réel des logs vers les systèmes SIEM des clients via un service NSS basé sur une VM ou dans le cloud.

Le service de prévention des intrusions, Zscaler Cloud Intrusion Prevention Service (IPS), intégré avec des technologies telles que les pare-feu et le sandboxing, offre une protection complète contre les attaques, en s'appuyant sur une analyse personnalisée et efficace des signatures qui assure une surveillance en temps réel et l'application des politiques. Par ailleurs, les entreprises peuvent identifier et corriger de manière proactive les vulnérabilités à l'aide des fonctionnalités de Zscaler telles que les politiques de ZIA en matière de protection contre les menaces avancées et de protection contre les malwares pour dispositifs mobiles. De son côté, Risk360 offre une visibilité sur la surface d'attaque externe et sur les risques de déplacement latéral, ce qui permet de prendre des décisions éclairées pour améliorer la posture de sécurité d'une entreprise et accélérer son délai moyen de réponse (MTTR).

Enfin, tous les clients peuvent s'inscrire au portail Zscaler Trust Portal pour signaler des incidents ou des suspicions d'incidents.

Exigences de NIS2 en matière de déclaration des incidents (Article 23)

Les entités doivent notifier aux autorités tout incident ayant un impact majeur sur la fourniture de leurs services. Le cas échéant, les entités doivent également informer les utilisateurs de leurs services des incidents importants susceptibles d'impacter la prestation de ces services. NIS2 définit un incident majeur comme un incident qui a causé ou est susceptible de causer une grave perturbation opérationnelle des services ou une perte financière pour l'entité concernée, ou qui a affecté ou est susceptible d'affecter des personnes physiques ou morales tierces, en leur infligeant des dommages matériels ou immatériels.

Le calendrier de déclaration des incidents est le suivant :

- Une « alerte précoce » dans les 24 heures suivant la prise de connaissance de l'incident majeur ;
- Une notification officielle de l'incident dans les 72 heures suivant la prise de connaissance de l'incident majeur. Une évaluation initiale de l'incident doit être fournie, avec notamment mention de sa gravité et de son impact, ainsi que (le cas échéant) des indicateurs de compromission ;
- Un rapport final dans un délai d'un mois détaillant l'incident, notamment sa gravité et son impact, le type de menace ou la cause susceptible d'avoir déclenché l'incident, les mesures de remédiation appliquées et en cours, et, le cas échéant, les impacts transfrontaliers.
- Au cours de ce processus, les autorités peuvent demander un rapport intermédiaire sur l'état d'avancement.

Zscaler peut vous aider : les solutions de sécurité basées dans le cloud de Zscaler offrent des capacités de détection et de maîtrise des menaces en temps réel, garantissant que les entreprises peuvent rapidement identifier et contrer les menaces. En outre, en délaissant les défenses traditionnelles basées sur le périmètre au profit d'une vérification et d'une autorisation permanentes des identités, l'architecture Zero Trust de Zscaler contribue à prévenir tout déplacement latéral susceptible d'aggraver la situation en cas d'intrusion. La validation de chaque demande d'accès en fonction de l'identité, de l'autorisation et du contexte assure une meilleure protection de l'ensemble de l'environnement contre les cyber–incidents.

Surveillance et mise en œuvre de NIS2 (Articles 32 et 33)

Les États membres de l'UE peuvent utiliser leurs pouvoirs de surveillance et de contrainte à l'encontre des entités qui enfreignent les mesures de gestion des risques de cybersécurité et les obligations de déclaration de NIS2. Les processus de surveillance et d'application pour les entités essentielles et importantes sont sensiblement différents : pour les entités essentielles, la surveillance s'effectue ex ante tandis que pour les entités importantes, elle est ex post (lorsqu'il existe des preuves, des indications ou des informations prouvant qu'une entité ne respecte pas NIS2).
En général, les autorités peuvent contraindre les entités de l'une ou l'autre catégorie sur les domaines suivants :

- Inspections sur site et surveillance hors site
- Audits de sécurité ciblés réalisés par un organisme indépendant ou une autorité compétente
- Analyses de sécurité
- Demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques de cybersécurité adoptées, notamment les politiques de cybersécurité documentées
- Demandes d'accès aux données, documents et informations nécessaires à la surveillance
- Demandes de preuves de la mise en œuvre de politiques de cybersécurité

NIS2 stipule également que la direction peut être tenue personnellement responsable des infractions à NIS2, avec notamment d'éventuelles interdictions temporaires d'occuper des postes de direction. En dernier recours, les autorités ont le pouvoir de suspendre temporairement une certification ou une autorisation liée aux services fournis par l'entité ou aux activités qu'elle mène.

Les États membres de l'UE peuvent également imposer des amendes administratives en cas de non-conformité à la directive NIS2. Pour les entités essentielles, les amendes administratives peuvent atteindre 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Pour les entités importantes, les amendes peuvent atteindre 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Zscaler peut vous aider : Zscaler est aux côtés des entreprises qui préparent et répondent aux audits et aux contrôles réglementaires. Ces entreprises disposent de logs complets, d'une application cohérente des politiques et d'un reporting détaillé.

Pour plus d'informations sur NIS2 et sur l'accompagnement proposé par Zscaler, veuillez contacter votre représentant Zscaler local.

+1 408 533 0288 Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134 zscaler.fr