Digital Security
Progress. Protected.

EVERSHEDS SUTHERLAND

NIS2

Tout ce qu'il faut savoir sur la nouvelle législation de l'UE sur la cyber-sécurité

Co-auteurs :
Saranda Walgaard
Andre Lamerias

TABLE DES MATIÈRES

Qu'est-ce que NIS2 ?

NIS2 crée un nouveau champ d'application pour renforcer le niveau de cybersécurité dans l'ensemble de l'UE. Cette version actualisée de la première directive sur les réseaux et les systèmes d'information est entrée en vigueur le 16 janvier 2023, obligeant les entités opérant dans des secteurs critiques tels que l'énergie, les transports, la santé, les services numériques et les services de sécurité managés à mettre en œuvre une meilleure gestion des risques. NIS2 introduit également de nouvelles règles de notification et de nouvelles amendes.

NIS versus NIS2 : L'évolution de la réglementation de l'UE sur la cybersécurité

La directive NIS adoptée en 2016 a été la première législation sur la cybersécurité concernant tous les États membres de l'Union européenne. Elle se concentrait principalement sur des organisations appartenant à deux groupes : les opérateurs de services essentiels (OSE), tels que la santé, les transports, l'énergie, etc., et les fournisseurs de services numériques (FSN), notamment les moteurs de recherche en ligne, les places de marché sur Internet et les services dans le Cloud. La directive NIS exigeait de ces organisations qu'elles se conforment aux mesures de sécurité appropriées et qu'elles signalent tout incident majeur de cybersécurité subi. Elle permettait également aux États de tenir compte de leur situation nationale.

NIS2 crée un nouveau champ d'application pour renforcer le niveau de cybersécurité dans l'ensemble de l'UE. Cette version actualisée de la première directive sur les réseaux et les systèmes d'information est entrée en vigueur le 16 janvier 2023 et s'applique non seulement aux États membres de l'UE, mais également aux organisations extérieures à l'UE qui sont essentielles à son marché. Les entreprises classées dans la catégorie « haute criticité » devront prendre des mesures techniques et opérationnelles pour se conformer à NIS2, notamment **la réponse aux incidents, la sécurité des chaînes d'approvisionnement, le chiffrement et la communication des vulnérabilités, l'analyse des risques, le test et l'audit des stratégies de cybersécurité, et la planification de la gestion de crise afin d'assurer la continuité des activités**. En cas de cyberincident, ces entités devront également soumettre une notification initiale dans les 24 heures et des informations plus détaillées dans les 72 heures. NIS2 prévoit des amendes en cas de non-respect, y compris la suspension de la certification et la responsabilité personnelle pour les postes de direction, conformément aux législations nationales.

Quels secteurs étaient inclus dans la directive NIS ?

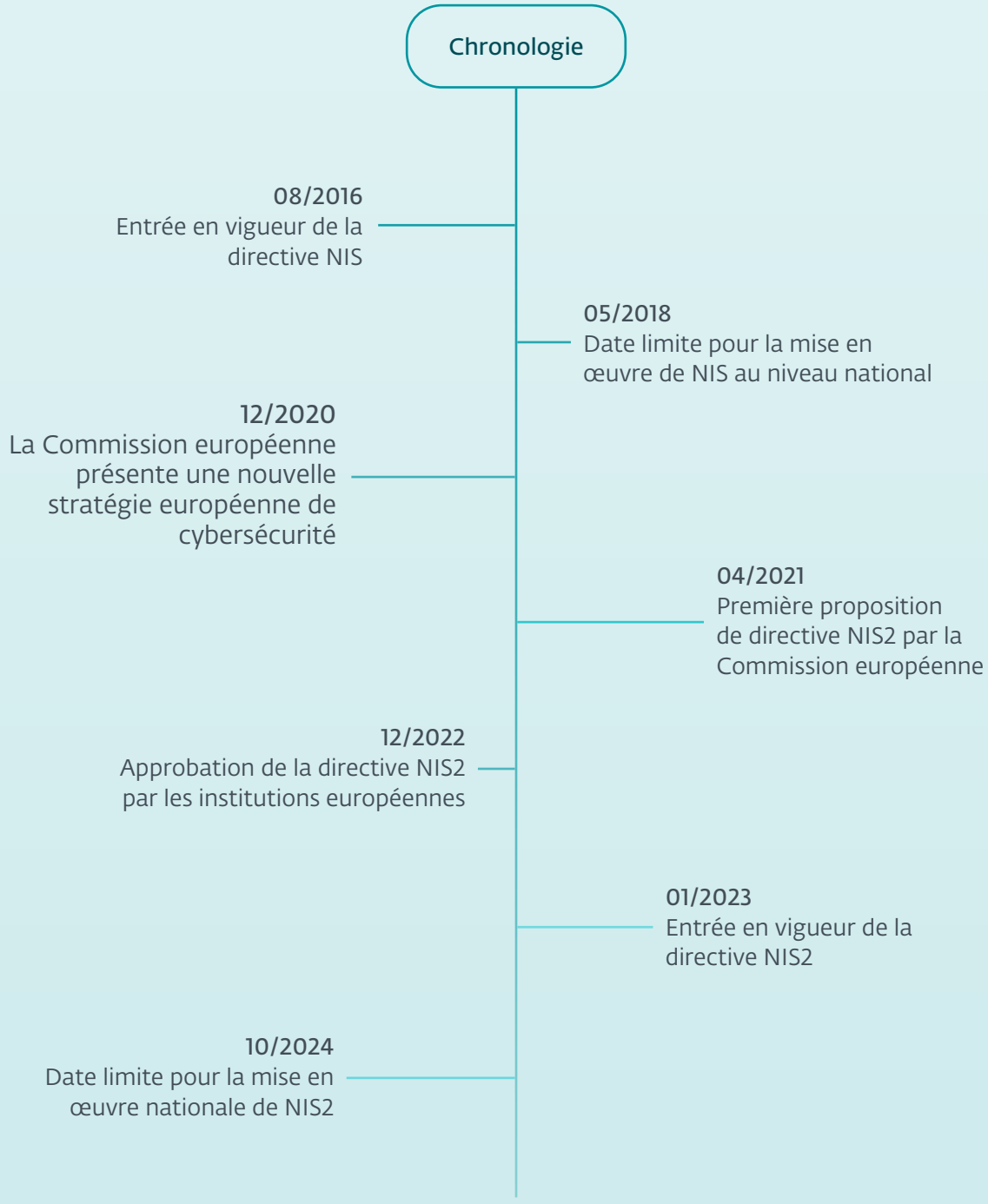
- Santé
- Infrastructure numérique
- Transports
- Approvisionnement en eau
- Fournisseurs de services numériques
- Infrastructure des banques et des marchés financiers
- Énergie

Quels secteurs ont été ajoutés par la directive NIS 2 ?

- Fournisseurs de réseaux ou de services publics de communication électronique
- Gestion des eaux usées et des déchets
- Fabrication de certains produits critiques (par ex. produits pharmaceutiques, dispositifs médicaux et produits chimiques)
- Nourriture
- Services numériques (par ex. plateformes de réseaux sociaux et services de centres de données)
- Espace (par ex. aérospatiale)
- Services postaux et de messagerie
- Administration publique

La directive établit également **le Réseau européen d'organisations de liaison en cas de cybercrise**, EU-CyCLONe, afin de permettre la coopération entre les agences et les autorités nationales chargées de la cybersécurité, et chaque État membre sera également tenu d'identifier clairement un point de contact unique pour le signalement des cyberincidents.

NIS2 deviendra applicable lorsque les États membres de l'UE auront transposé la directive dans leur droit national, d'ici septembre 2024. Néanmoins, les organisations devraient s'y préparer le plus tôt possible, non seulement pour être à temps dans le processus de mise en œuvre, mais également pour tester différentes bonnes pratiques de traitement des incidents, de politiques de contrôle et de mythologies en matière de signalement.



Qui doit s'y conformer ?

Par rapport à sa version précédente, la nouvelle directive NIS supprime la distinction entre les opérateurs de services essentiels et les fournisseurs de services numériques. Les entités seront classées en fonction de leur importance et divisées en deux catégories, les entités essentielles et les entités importantes, qui seront soumises à des régimes de surveillance différents.

Cela signifie que **tous les secteurs et toutes les organisations relevant de NIS2 sont d'une grande importance pour les communautés de l'Union européenne. Il est entendu que leur perturbation causerait un préjudice grave à la société s'ils n'étaient plus en mesure d'exercer leurs fonctions.** En fin de compte, les deux catégories ont été créées pour distinguer le fait que tous les secteurs n'ont pas le même impact sur la société en cas d'incident.

Quels sont les secteurs concernés ?

Entités essentielles (EE)

Grands opérateurs des secteurs de **haute criticité** et cas particuliers

Seuil pour les grandes organisations

> 250 collaborateurs
> 50 M€ de chiffre d'affaires
> 43 M€ de solde

Secteurs de haute criticité

- Énergie
- Transports
- Banque
- Gestion des services de TIC
- Eau potable
- Eaux usées
- Fournisseurs de soins de santé
- Infrastructure numérique
- Administration publique
- Infrastructure des marchés financiers
- Espace

Entités importantes (EI)

Grands opérateurs d'autres secteurs critiques et **opérateurs de taille moyenne**

Seuil pour les organisations de taille moyenne

50 - 250 collaborateurs
10 - 50 M€ de chiffre d'affaires
< 43 M€ de solde

Autres secteurs critiques

- Poste et messagerie
- Gestion des déchets
- Fabrication, production et distribution de produits chimiques
- Fabrication, production et distribution de denrées alimentaires
- Fabrication (électronique et autres)
- Fournisseurs numériques
- Recherche

Les deux types d'entités ont les mêmes devoirs et obligations, par exemple, les membres des organes de direction des entités essentielles et importantes sont tenus de suivre une formation et doivent prendre des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques liés à la sécurité des réseaux et des systèmes d'information. Les entités utilisent ces mesures pour leurs opérations ou la prestation de services afin de prévenir ou de minimiser l'impact des incidents sur les bénéficiaires de leurs services ou d'autres services.

Les organisations essentielles devront également disposer d'un cadre de préparation proactive pour évaluer l'impact d'une mauvaise gestion, même en l'absence d'incident.
Pour les entités importantes, la conformité est attendue de manière réactive, ce qui signifie que la conformité de ces organisations avec les lois et les exigences ne sera vérifiée qu'après un incident. S'il s'avère que des mesures insuffisantes ont été prises et que les exigences n'ont pas été respectées, des sanctions s'appliqueront aux deux types d'entités.

Il est important de noter qu'au plus tard le 17 avril 2025, et ensuite tous les deux ans, les autorités compétentes indiqueront à la Commission et au groupe de coopération le nombre d'entités essentielles et importantes pour chaque secteur.

Devoir de diligence et devoir de signalement

Toutes les organisations couvertes par NIS2, qu'elles soient essentielles ou importantes, devront commencer à se conformer à leur devoir de diligence. La directive contient une liste de types de mesures que les fournisseurs de services doivent respecter au minimum. Il s'agit notamment d'évaluer les risques pour vérifier si une organisation accorde suffisamment d'attention à la sécurité des systèmes d'information, la gestion de crise et la continuité opérationnelle en cas de cyberincident majeur, et si elle peut garantir la sécurité de sa chaîne d'approvisionnement. Le devoir de diligence consiste par ailleurs à assurer la sécurité des réseaux et des systèmes d'information, utiliser la cryptographie et le chiffrement, et disposer de politiques et de procédures permettant d'évaluer l'efficacité des mesures de gestion des risques. Le devoir de signalement s'appliquera également à toutes les organisations couvertes par NIS2. Cette obligation de notification exigera des organisations concernées qu'elles informent leurs autorités nationales dans les 24 heures suivant la découverte d'un incident, qu'elles fassent ensuite un compte rendu dans les 72 heures, et qu'elles procèdent à une évaluation finale un mois plus tard.

Le devoir de diligence

En vertu de l'ancienne directive NIS, le devoir de diligence s'applique à la fois aux fournisseurs de services essentiels et aux fournisseurs de services numériques. Il s'agit de prendre des mesures techniques et organisationnelles appropriées et proportionnées pour gérer les risques liés à la sécurité des réseaux et des systèmes d'information.

La nouvelle directive NIS2 établit une distinction différente : les entités essentielles et importantes, qui reflètent le degré de criticité de leur secteur ou du type de service qu'elles fournissent, ainsi que leur taille. Les deux types d'entités devront se conformer au devoir de diligence. Il appartient aux États membres d'établir une liste d'entités essentielles et importantes sur la base des mécanismes nationaux les plus appropriés, en permettant aux entités de s'inscrire elles-mêmes. Les entités sont soumises à des mesures de gestion du risque pour la cybersécurité lorsqu'elles sont inscrites dans l'une des deux catégories. Ces mesures doivent être proportionnées au degré d'exposition de l'entité essentielle ou importante aux risques et à l'impact sociétal et économique qu'aurait un incident. Il convient également de tenir dûment compte de la criticité de l'entité, de sa taille et de la probabilité que des incidents se produisent.

Dans ce contexte, la sécurité désigne la capacité des réseaux et des systèmes d'information à résister aux actions qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité. Le règlement de mise en œuvre de la Commission (Règlement (UE) 2018/151) précise les éléments de sécurité à respecter : sécurité des systèmes et des installations, traitement des incidents, gestion de la continuité des activités, surveillance, contrôle et tests, et normes internationales.

La directive NIS2 énumère un ensemble minimum de mesures, notamment la réalisation d'une analyse des risques et la mise en place de politiques relatives à la sécurité des systèmes d'information, à l'intervention en cas d'incident, à la continuité des activités et la gestion des crises, à la sécurité des chaînes d'approvisionnement et à la sécurité dans l'acquisition, le développement et la maintenance des réseaux et des systèmes d'information. Sont également incluses les politiques et les procédures visant à évaluer l'efficacité des mesures de gestion des risques, et l'utilisation de la cryptographie et du chiffrement.

Les entités essentielles et importantes **devraient également adopter un large éventail de pratiques de cyber-hygiène de base, telles que les principes zero-trust, les mises à jour de logiciels, la configuration des appareils, la segmentation du réseau, la gestion des identités et des accès ou la sensibilisation des utilisateurs ; organiser des formations pour leur personnel ; et sensibiliser aux cybermenaces, à l'hameçonnage ou aux techniques d'ingénierie sociale**. Ces entités devraient en outre réévaluer leurs moyens de cybersécurité et, le cas échéant, poursuivre l'intégration de technologies renforçant la cybersécurité, telles que l'intelligence artificielle ou les systèmes de machine learning, afin d'améliorer leurs capacités et la sécurité des réseaux et des systèmes d'information.

Pour démontrer la conformité avec ces mesures, **les États membres peuvent exiger des entités essentielles et importantes qu'elles utilisent des produits, des services ou des processus spécifiques de TIC qui seront certifiés dans le cadre des systèmes européens de certification de la cybersécurité** adoptés en vertu de la loi sur la cybersécurité (Règlement (UE) 2019/881).

La Commission européenne est habilitée à adopter des actes de mise en œuvre et des actes délégués pour préciser les mesures de gestion des risques. Ainsi, les obligations peuvent être mieux définies pour tenir compte des nouvelles cybermenaces, des évolutions technologiques ou des spécificités sectorielles.

Le devoir de signalement

Avec l'avènement de la directive NIS2, outre le devoir de diligence, le devoir de signalement, qui existait déjà dans la directive NIS initiale, sera étoffé.

La première directive NIS a introduit le devoir de signaler les incidents ayant un impact significatif sur la continuité des services. Selon la directive, un incident correspond à « tout événement ayant un effet préjudiciable réel sur la sécurité des réseaux et des systèmes d'information ». La sécurité désigne « la capacité des réseaux et des systèmes d'information à résister à des actions qui affectent la disponibilité, l'intégrité, la confidentialité et l'authenticité des réseaux et des systèmes d'information avec un certain degré de fiabilité ».
Pour déterminer si un incident a un impact significatif, la directive décrit plusieurs paramètres à prendre en considération, notamment le nombre d'utilisateurs touchés, la durée de l'incident et la taille de la zone géographique touchée par l'incident. Si un incident semble avoir un impact significatif sur la continuité du service fourni par un fournisseur, l'incident **doit être signalé sans délai à l'équipe locale de réponse aux incidents de sécurité informatique (CSIRT) ou à l'autorité compétente désignée par l'État membre**. Le rapport doit contenir suffisamment d'informations pour permettre à l'autorité compétente ou au CSIRT de déterminer l'impact transfrontalier de l'incident.

La directive NIS2 prévoit une « approche en deux étapes » pour le signalement des incidents. La première notification vise à limiter la propagation potentielle des incidents et à permettre aux entités de demander de l'aide. Le second compte rendu doit être approfondi, de manière à ce que des leçons puissent être tirées des incidents précédents. Il est toutefois important de noter que des éclaircissements supplémentaires peuvent être nécessaires pour évaluer clairement l'incident et ses conséquences. L'objectif est d'améliorer progressivement la résilience des entreprises et des secteurs entiers face aux cybermenaces.

Étapes de déclaration d'incidence selon NIS2

Dans les 24 heures suivant la prise de connaissance de l'incident (et sans retard injustifié), une première notification devrait être adressée à l'autorité compétente ou au CSIRT national compétent. Elle devrait indiquer si possible si un acte illégal ou malveillant est à l'origine de l'incident. Cette disposition satisfait aux informations strictement nécessaires.

Dans les 72 heures suivant la première alerte, l'entité concernée est tenue de présenter une évaluation initiale plus détaillée de l'attaque et des mesures mises en place. À la demande de l'entité, il est possible de recevoir des conseils sur la mise en œuvre de mesures d'atténuation potentielles et, le cas échéant, une assistance technique supplémentaire. Dans le cas d'un incident criminel, l'entité concernée reçoit également des conseils sur la manière de signaler l'incident aux autorités chargées de l'application de la loi.

Au plus tard un mois après la première notification, un rapport final doit être présenté, comprenant :

- une description détaillée de l'incident, de sa gravité et de ses conséquences
- le type de menace ou de cause susceptible d'avoir conduit à l'incident
- les mesures d'atténuation appliquées et en cours

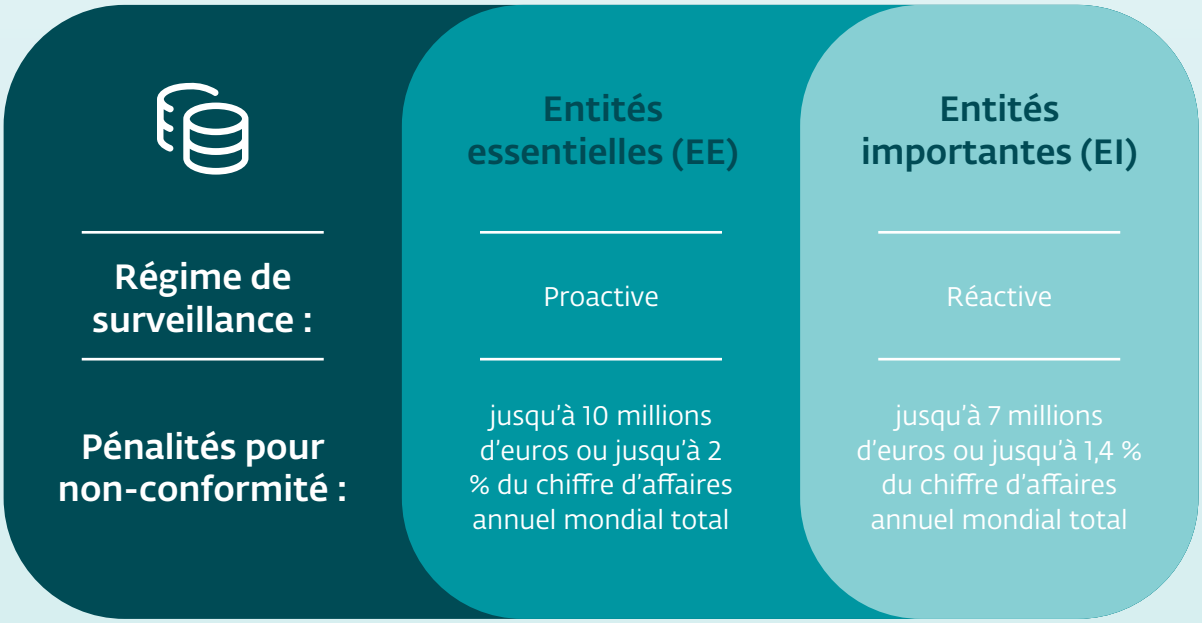
La disposition relative au signalement des incidents ayant des conséquences importantes a été adoptée dans la directive NIS2, qui ajoute que **les entités devront également signaler toute cybermenace majeure qu'elles ont identifiée et qui pourrait conduire à un incident significatif**. Le terme « cybersécurité » est défini dans le règlement relatif à l'ENISA (l'Agence de l'Union européenne pour la cybersécurité) et à la certification de la cybersécurité des technologies de l'information et de la communication ; la loi sur la cybersécurité. Ce règlement définit la cybersécurité comme « les activités nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes concernées par les cybermenaces ». Un incident est considéré comme significatif s'il entraîne ou peut entraîner une perturbation opérationnelle significative ou des pertes financières pour l'entité concernée, ou si l'incident a affecté ou peut affecter des personnes physiques ou morales en causant des dommages matériels ou immatériels significatifs.

Les entités n'entrant pas dans le champ d'application de la directive NIS2 peuvent volontairement signaler les incidents significatifs, les cybermenaces ou les incidents évités de justesse. L'autorité compétente ou le CSIRT suit la procédure décrite dans la « notification en deux étapes ». Les signalements soumis volontairement ne peuvent faire l'objet d'aucune obligation supplémentaire. Ainsi, si une entité fait une notification volontaire, elle ne devrait pas être soumise à des obligations plus onéreuses que si elle ne l'avait pas faite.

Comment va-t-elle être appliquée ?

Il incombe aux États membres d'exercer une surveillance efficace afin de garantir le respect des exigences de NIS2 une fois qu'ils l'auront transposée dans leur législation nationale.

En ce qui concerne les entités essentielles, cela implique une surveillance proactive. En revanche, les entités importantes sont soumises à une surveillance réactive, qui peut être déclenchée par des preuves, des indications ou des informations selon lesquelles l'entité ne se conformerait pas à la directive. En effet, dans ce dernier cas, des mesures ne devraient être prises que lorsque, pour un État membre, il apparaît qu'une entité importante ne respecte pas les obligations prévues par la directive.



Pour la définition des EE et des EI, voir le tableau de la page 5.

Les mesures prises par les autorités compétentes doivent être efficaces, proportionnées et dissuasives. Pour les deux types d'entités, **les organismes compétents auront le pouvoir de les soumettre à des inspections sur site et une supervision ex-post hors site menées par des professionnels qualifiés, à des audits de sécurité ciblés, à des analyses de sécurité, à des demandes d'accès aux données, documents et informations, et à des demandes de preuves de la mise en œuvre des politiques de cybersécurité, telles que les résultats des audits de sécurité réalisés par un auditeur qualifié et les preuves sous-jacentes correspondantes**. Des contrôles aléatoires viennent compléter la liste, ainsi que des audits ad hoc dans le cas d'entités essentielles. Sauf dans des cas dûment justifiés, les entités auditées devront supporter les coûts des audits de sécurité.

Si une infraction est découverte, les autorités compétentes peuvent exercer d'autres pouvoirs de mise en conformité, tels que l'émission d'avertissements, l'adoption d'instructions, l'injonction aux entités de cesser de mener des activités contraires à la directive, l'injonction aux entités d'informer les personnes physiques ou morales susceptibles d'être affectées par le comportement fautif, ou même de rendre l'information publique. Si ces mesures ne permettent pas de remédier à la situation, les autorités compétentes peuvent suspendre temporairement les activités de l'entité et le dirigeant de l'organisme qui exerce des responsabilités à un niveau de directeur général ou de représentant légal.

La directive NIS2 établit un cadre cohérent pour les sanctions dans l'ensemble de l'Union, en dressant une liste minimale de sanctions administratives en cas de manquement aux obligations de gestion et de déclaration des risques de cybersécurité. Ces sanctions comprennent des instructions contraignantes, la mise en œuvre des recommandations d'un audit de sécurité, la mise en conformité des mesures de sécurité avec les exigences de NIS2 et des amendes administratives.

Les États membres doivent donner aux autorités compétentes la possibilité d'imposer des amendes considérables. Pour les entités essentielles, il s'agit d'un maximum d'au moins 10 000 000 € ou de 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Pour les entités importantes, l'amende maximale est fixée à 7 000 000 € ou à au moins 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Les organes de direction des entités essentielles et importantes peuvent également être tenus pour responsables du non-respect des dispositions de la directive NIS2. Si votre organisation est une entité couverte et qu'elle ne parvient pas à créer et maintenir une cybercompétence, des amendes et des sanctions seront infligées pour non-respect des mesures de gestion des risques ou des obligations de signalement.

Pour renforcer la surveillance qui contribue à assurer une conformité effective, la directive NIS2 fournit une liste minimale de moyens de surveillance par lesquels les autorités compétentes peuvent surveiller les entités essentielles et importantes. Il s'agit notamment d'audits réguliers et ciblés, de contrôles sur site et hors site, de demandes d'informations et d'accès à des documents ou à des preuves.

Dans l'exercice de leurs pouvoirs de mise en application, les autorités compétentes doivent tenir dûment compte des circonstances particulières de chaque cas, telles que la nature, la gravité et la durée de l'infraction, les dommages causés ou les pertes subies, et le caractère intentionnel ou négligent de l'infraction.

Pour assurer la responsabilité des mesures de cybersécurité au niveau organisationnel, **NIS2 introduit des dispositions sur la responsabilité des personnes physiques occupant des postes de direction** dans les entités relevant du champ d'application de la nouvelle directive NIS2.

Que signifie-t-elle pour les petites et moyennes entreprises ?

NIS2 établit l'application de la règle du plafond de taille, telle que définie dans le tableau de la page 5. Bien qu'elle exclue la majorité des petites et moyennes entreprises de l'obligation de se conformer aux nouvelles règles, certaines exceptions s'appliquent, par exemple, pour **les PME des secteurs des réseaux de communication électronique ou des services de communication électronique accessibles au public, des fournisseurs de services de confiance ou des administrateurs de registres de noms de domaines de premier niveau (TLD)**.

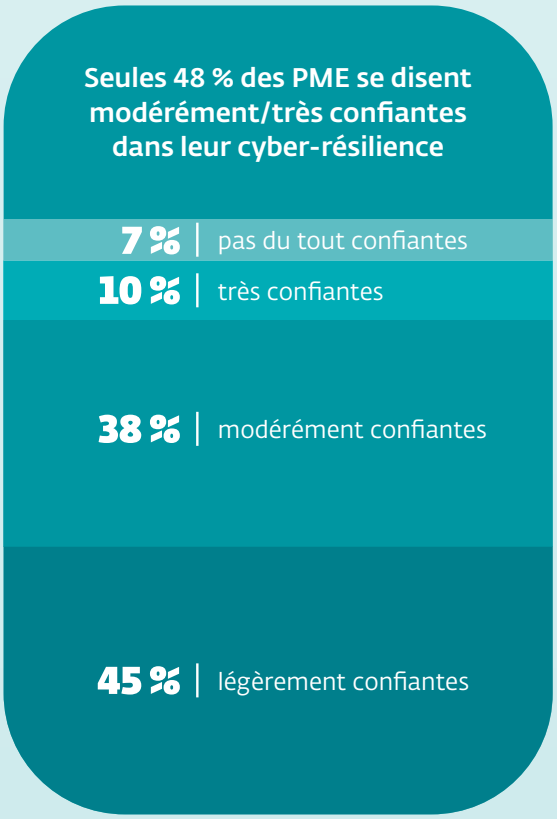
Les PME sont de plus en plus souvent la cible d'attaques contre leur chaîne d'approvisionnement en raison de leurs ressources de sécurité limitées. Ces attaques contre les chaînes d'approvisionnement peuvent avoir un effet en cascade sur les entités qu'elles servent. **Les États membres devraient, via leurs stratégies nationales de cybersécurité, aider les PME à relever les défis auxquels elles sont confrontées dans leurs chaînes d'approvisionnement**. Ils devraient mettre en place un point de contact pour les PME au niveau national ou régional fournissant des conseils et une assistance aux PME, ou les orientant vers les organismes appropriés, pour obtenir des conseils et une assistance en ce qui concerne les questions de cybersécurité.

En mars de l'année dernière, l'Alliance DIGITAL SME, le plus grand réseau de PME de l'UE dans le domaine des TIC, a publié une prise de position en réaction à la consultation sur la proposition de NIS2, saluant la nouvelle directive, mais alertant également sur l'impact indirect de NIS2 sur les PME.

Selon James Philpot, chef de projet chez DIGITAL SME, **la première chose que les PME devraient faire pour comprendre leurs besoins spécifiques afin de renforcer leurs pratiques de cybersécurité serait de consulter leur centre national de cybersécurité ainsi que les guides et recommandations de l'ENISA**. Il peut cependant être plus ou moins facile d'obtenir les bonnes informations, car les États membres fournissent des ressources différentes. Néanmoins, NIS2 prévoit que les États devraient fournir un soutien et des ressources, principalement pour aider les organisations à obtenir une compréhension détaillée du champ d'application de cette législation et de savoir si leurs clients y seront soumis, ce qui permettra de planifier à l'avance.

« Les fournisseurs en aval risquent d'être les plus perturbés, et il peut être difficile pour certaines entreprises de disposer des moyens techniques nécessaires, mais surtout de comprendre les exigences de signalement et la manière dont NIS2 interagit avec d'autres législations, » explique M. Philpot.

Confiance des PME dans la cyber-résilience



74 % des PME estiment que les entreprises de leur taille sont plus vulnérables aux cyberattaques que les grandes entreprises

Source : Rapport ESET sur le sentiment de cybersécurité des PME en 2022

D'une manière générale, tout effort visant à améliorer le niveau de cybersécurité des entreprises européennes devrait être accueilli. DIGITAL SME ainsi qu'ESET sont convaincus que ce nouveau cadre pourrait être une opportunité. La seule mise en garde, alerte M. Philpot, concerne le niveau de mise en œuvre et de soutien, et la manière dont cela sera géré. En fin de compte, cela fera la différence entre une législation qui aide les PME et une législation qui constitue un fardeau réglementaire.

Des solutions techniques sont disponibles en Europe pour assurer le niveau de cybersécurité requis, mais les entreprises doivent éviter de rechercher le nom le plus connu ou l'offre la moins chère, qui tend à provenir de l'extérieur de l'Europe. C'est pourquoi il est si important d'associer soutien et ressources pour tirer parti de cette législation et renforcer l'innovation européenne.

Les PME peuvent également s'adresser à leur CSIRT local pour pallier certaines des lacunes d'autres organismes nationaux, ou tirer parti de ressources telles que le site web DIGITAL SME/guide SBS, le DIGITAL SME Guide on Information Security Controls ou les certificats de cybersécurité.

Les PME sont les plus préoccupées par les conséquences d'une cyberattaque sur leur activité

Source : Rapport ESET sur le sentiment de cybersécurité des PME en 2022

Comme le note également M. Philpot dans sa conversation avec ESET, les conséquences des cyberincidents sont bien connues des PME : fuites de données, impact financier considérable et perte de confiance des clients. Tout au moins, elles peuvent profiter de la directive NIS2 pour se sensibiliser davantage et renforcer leur cyber-résilience.

Suivez Digital Security Guide d'ESET pour obtenir des conseils de cybersécurité pour les petites et moyennes entreprises

Digital Security
Progress. Protected.

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour protéger les entreprises, les infrastructures critiques et les consommateurs du monde entier contre des menaces digitales de plus en plus sophistiquées. Protection des terminaux et des mobiles, détection et traitement des incidents, chiffrement et authentification multifacteur... les solutions performantes et faciles à utiliser d'ESET protègent et supervisent discrètement 24 heures sur 24, 7 jours sur 7, en mettant à jour les défenses en temps réel pour assurer sans aucune interruption la sécurité des utilisateurs et le bon fonctionnement des entreprises. L'évolution des menaces exige d'une entreprise de sécurité informatique qu'elle évolue également. C'est le cas d'ESET grâce à ses centres de R&D dans le monde entier travaillant à la protection de notre avenir commun. Pour plus d'informations, consultez le site www.eset.com/fr/ ou suivez-nous sur LinkedIn, Facebook et Instagram.

EVERSHEDS
SUTHERLAND

Eversheds Sutherland est un cabinet international d'avocats et de notaires qui compte 74 bureaux dans 35 pays et emploie plus de 3 000 juristes. Grâce à notre caractère international, nous sommes en mesure de fournir des conseils transfrontaliers comme personne d'autre. Eversheds Sutherland possède 44 succursales en Europe.

Ce manuel a été créé avec le soutien des affaires gouvernementales d'ESET.