Digital Security Magazine

NIS 2
en un coup d’œil

Ce qu’il est important de connaitre pour être en conformité

EVIDEN

> Les cybermenaces causant de plus en plus de problèmes aux entreprises d'année en année, l'Union européenne a décidé de mettre en œuvre un nouvel ensemble de normes de cybersécurité à respecter afin de s'assurer que les entreprises au sein du marché de l'UE soient plus résistantes.
>
> Dans cette optique, nous avons pensé revenir sur **l'essence de la directive NIS 2** afin que vous sachiez en quoi consiste cette nouvelle directive, qui est concerné et comment s'y conformer. »

Maxime Karcenty

Avant-vente IAM et spécialiste Marketing – France, Evidian

EVIDEN

Qu’est-ce que NIS ?

La Directive NIS (Network and Information Security) a été pour la première fois introduite en 2016 **pour renforcer la cybersécurité en Europe**, en mettant l'accent sur les entreprises et les secteurs axés sur les technologies de l'information et de la communication.

Qu’est ce qui est nouveau avec NIS 2 ?

La NIS2 vise à élargir considérablement les entreprises concernées, les secteurs (18) et les exigences à respecter pour être en conformité et réduire le risque de dommages aux systèmes informatiques et aux données.

1

Poursuite de la couverture des secteurs NIS existants (soins de santé, banques, transports) et extension à de **nouveaux domaines.**

2

Extension de la directive aux **entreprises privées**, affectant des milliers d'entreprises, des PME aux grandes sociétés.

3

Introduction d'un mécanisme de proportionnalité, établissant une distinction entre les entités **essentielles** et les **entités importantes**.

EVIDEN

Qui est concerné ?

Toute entité essentielle ou importante qui fournit des services à l'économie ou à la société européenne sera soumise à la NIS2, y compris les entités situées en dehors de l'UE mais qui fournissent des services au sein de l'UE :

Entités essentielles (EE)

Entités de taille moyenne ou grande (qui emploient **au moins 250 personnes** ou dont le chiffre d'affaires est égal ou supérieur à **50 millions d'euros** ou dont le bilan annuel est égal ou supérieur à 43 millions d'euros) dans les secteurs de l'Annexe 1.

Entités importantes (EI)

Les moyennes et **grandes** entreprises des secteurs de l'annexe 2 et les moyennes entreprises des secteurs de l'Annexe 1 et de l'Annexe 2.

Quelles sont les principales exigences en matière de conformité ?

Analyse des cyber-risques
encourus et des politiques de
sécurité en place

Sécuriser les réseaux et les systèmes d'information avec :

- l'utilisation de techniques de cryptographie et de chiffrement des données
- le contrôle des accès au système
- l'intégration de solutions d'authentification multifactorielle

Mise en œuvre de mesures visant à garantir la
continuité des activités en cas d'incident.

Former les employés aux cyber-risques et aux
meilleures pratiques à adopter pour s'en protéger

L'obligation de disposer d'une **équipe de gestion des incidents cyber** avec l'obligation de :

- signaler un incident de sécurité dans les 24 heures
- présenter une évaluation de l'impact de l'incident dans les 72 heures
- fournir un rapport complet dans un délai d'un mois.

Tests et audits de sécurité
La NIS2 exigera des entités qu'elles effectuent régulièrement des tests et des audits techniques, y compris des tests d'intrusion et des analyses de vulnérabilité, afin d'évaluer l'efficacité des mesures de sécurité déployées.

Sécurité de la chaîne d'approvisionnement
Les entreprises seront tenues d'exercer un audit préalable sur la chaîne d'approvisionnement, notamment en étudiant les pratiques de cybersécurité en vigueur chez leurs fournisseurs et prestataires de services.

EVIDEN

Quand ?

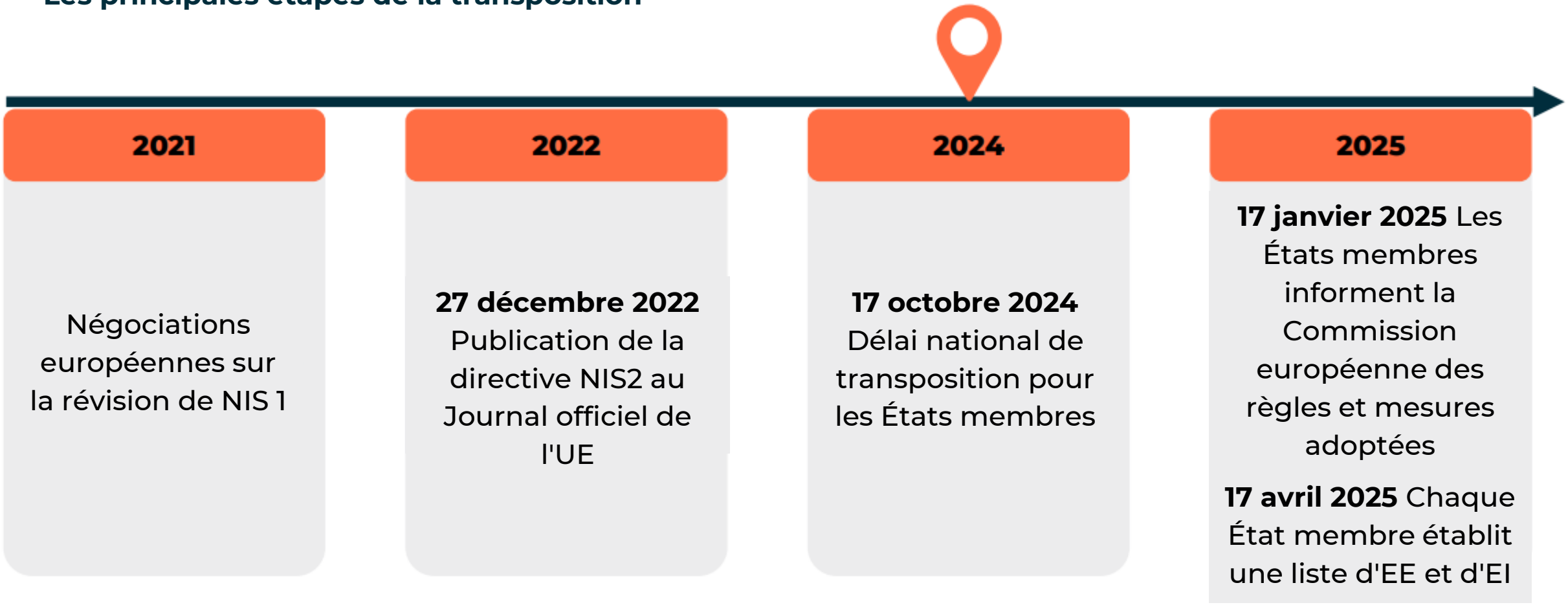
Dès le **17 octobre 2024**, les États membres doivent transposer les mesures de la directive NIS2 dans leur droit national. Les États de l'Union européenne (UE) auront alors quelques mois pour s'en imprégner, adopter la directive et publier leurs recommandations pour que les entreprises se mettent en conformité.

D'ici là, les **opérateurs de services essentiels** (OSE) et les **fournisseurs de services numériques** doivent continuer à se conformer aux exigences de la directive NIS et des autres réglementations relatives à la sécurité des systèmes d'information.

En outre, les entités qui **relevaient déjà du champ d'application de la NIS** doivent poursuivre leurs efforts pour se conformer à la **première version de la directive**. Les efforts déployés jusqu'à présent ne seront bien sûr pas perdus, puisque la nouvelle version de la directive s'appuie sur les acquis de la précédente.

EVIDEN

Les principales étapes de la transposition



Plus d'information sur MonEspaceNIS2

EVIDEN

Sanctions financières

Le niveau d'exigence des mesures de sécurité à mettre en œuvre peut être différent d'un pays à l'autre et pour des entités essentielles ou importantes. Les amendes mentionnées ci-dessous ne sont donc données qu'à titre indicatif

Pour les entités essentielles

Jusqu'à **2 %** du chiffre d'affaires mondial et jusqu'à **10 millions d'euros** d'amende

Pour les entités importantes

Jusqu'à **1,4 %** des ventes mondiales et jusqu'à **7 millions d'euros** d'amende

Annexe 1 Secteurs

Energie
(électricité, chauffage et refroidissement urbains, pétrole, gaz naturel, hydrogène)

Transport
(air, rail, eau, route)

Banque

Infrastructure des marchés financiers

Santé
(incluant désormais les laboratoires de référence, les fabricants de dispositifs médicaux, les fabricants de produits pharmaceutiques et autres)

Eau potable

Eaux usées

Infrastructure numérique

Gestion des services TIC

Administration publique
« centrale>et>régionale »

Espace

EVIDEN

Annexe 2 Secteurs

Services postaux et de messagerie

Gestion des déchets

Fabrication, production et distribution de produits chimiques

Production, transformation et distribution de denrées alimentaires

Industrie
(dispositifs médicaux et dispositifs médicaux de diagnostic in vitro ; produits informatiques, électroniques et optiques ; matériel électrique ; machines et équipements n.c.a., véhicules automobiles, remorques et semi-remorques ; autres matériels de transport)

EVIDEN

EVIDEN

Merci

Pour en savoir plus, consultez notre publication trimestrielle sur les dernières tendances et innovations en matière de cybersécurité :