arcserve®

NIS 2 :
To be, or not to be ?

La cyber-résilience Européenne s'organise, serez-vous impactés ?

MINI-QUIZZ

- ◯ Vous connaissez mal les implications de la directives NIS2 pour votre entreprise,
- ◯ Vous manquez de ressources en interne pour appliquer les nombreuses mesures de sécurité édictées et s'assurer de leur pleine conformité,
- ◯ Vous craignez les coûts potentiellement élevés à mettre en œuvre pour se conformer,

… bref, **êtes-vous prêts pour être en conformité d'ici le mois d'Octobre 2024 ?**

La suite devrait vous intéresser ⟶

TEST : Êtes-vous directement concernés par la directive NIS 2 ?

Q.1 Vous exercez dans :

A. Le secteur public ◯ **B.** Le secteur privé ◯

Q.2 Votre niveau de criticité :

A. Votre entité fournit un service de réseau de communications électroniques publics, un service de communication électronique accessible au public, un service de confiance, un service de registre de noms de domaine de premier niveau, un service de système de noms de domaine, un service d'enregistrement de noms de domaine. ◯

B. Votre entité est une entité de l'administration publique des pouvoirs publics centraux ou une entité publique au niveau régional qui fournit des services dont la perturbation pourrait avoir un impact important sur les activités sociétales ou économiques critiques. ◯

C. Aucun de ces 2 critères de criticité. ◯

Q.3 La taille de votre organisation :

A. Micro ou petite entité (<50 employés – CA <10M€) ◯

B. Moyenne entité (entre 50 et 250 employés – CA entre 10 et 50M€) ◯

C. Intermédiaire ou grande entité (>250 employés – CA >50M€) ◯

Q.4 Votre secteur d'activité :

- Production, transformation et distribution de denrées alimentaires ◯
- Banque ◯
- Assurance ◯
- Bois -Papier -Carton- Imprimerie ◯
- BTP - Matériaux de construction ◯
- Fourniture de services numériques (infrastructures informatiques et sécurité, fournisseurs de services cloud) ◯
- Édition - Communication - Multimédia ◯
- Chimie - Parachimie ◯
- Énergie ◯
- Études et conseils ◯
- Industrie pharmaceutique ◯
- Transports ◯
- Logistique ◯
- Santé et dispositifs médicaux ◯
- Spatial ◯
- Recherche* ◯
- Services des eaux ◯
- Informatique - Télécoms ◯
- Électronique - Électricité ◯
- Machines et équipements Automobile ◯
- Métallurgie - Travail du métal ◯
- Plastique - Caoutchouc ◯
- Services postaux et des services de courrier ◯
- Gestion des déchets ◯
- Textile - Habillement Chaussure ◯

* soit les organismes de recherche au sens de "une entité dont l'objectif premier est de mener des activités de recherche appliquée ou de développement expérimental en vue d'exploiter les résultats de cette recherche à des fins commerciales, à l'exclusion des établissements d'enseignement." (Article 6(41)

Comptabilisez vos symboles. Vous avez une majorité de ▲ ■ ou ★

Résultats page suivante

RÉSULTATS DU TEST*:

Vous n'êtes pas concernés pour le moment

La directive NIS 2 ne vous concerne pas encore, toutefois les bonnes pratiques de sécurité édictées par cette directive sont des lignes directrices qu'il convient de suivre dès à présent pour anticiper les risques de cybersécurité qui ciblent tous types d'entreprises. N'attendez pas le prochain élargissement de la directive pour vous mettre à niveau !

Vous êtes potentiellement concerné par la directive NIS 2

La taille de votre organisation et votre secteur d'activité vous identifie comme potentiellement concernés par les obligations légales européennes édictées par la directive NIS 2. Les critères pouvant être subtils, nous vous conseillons de tester votre éligibilité sur le site créé spécialement à cet effet par l'ANSSI et de lire la suite de cet ebook.

TESTER VOTRE ÉLIGIBILITÉ

Vous êtes automatiquement concerné par la directive NIS 2

Votre entité est considérée comme une entité importante (EI) ou une entité essentielle (EE) et doit, de fait, se conformer aux normes édictées par la directive européenne.

Le décret de transposition de NIS2 au niveau national devra être effectif au plus tard le 17 octobre 2024 et vous n'aurez pas plus d'un an de délais pour votre mise en conformité. Vous devrez rendre compte de la résilience de votre organisation sous peine de sanctions.

**Ce quizz est à titre indicatif et ne constitue pas un cadre juridique. La directive du parlement européen et du conseil du 14 décembre 2022 est le document de référence légal.*

Une nouvelle règlementation européenne basée sur la gestion des risques

La directive NIS 2 est un texte législatif de l'Union européenne sur la cybersécurité. Elle remplace et complète la directive NIS première du nom (Network and Information Security), adoptée en juillet 2016. La directive NIS 2 dresse une liste de mesures a minima devant être prises par toutes les entités.

Votre conformité en 10 thématiques

01	Les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information
02	La gestion et le traitement des incidents
03	**La continuité des activités, comme la gestion des sauvegardes et la reprise des activités** *(Art. 21.2.c)*
04	La sécurité de la chaine d'approvisionnement
05	La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
06	Évaluation des mesures de gestion des risques liés à la cybersécurité
07	Formation à la cybersécurité et cyberhygiène
08	Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
09	La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
10	L'utilisation de solutions d'authentification à plusieurs facteurs

Pour la France

La directive NIS 2 devra être transposée par chaque état membre de l'UE en droit national, **au plus tard en octobre 2024.**

Alternative pour l'Europe :

Cette transposition en droit national implique que les états devront déléguer un rôle de régulation à l'autorité nationale désignée en matière de cybersécurité et de cyberdéfense. Cette autorité veillera à l'application stricte de la législation nationale, se réservant le droit d'imposer **des sanctions administratives sévères et de prendre des mesures correctives en cas de non-conformité.**

Les principaux objectifs de la directive NIS 2 :

- Faire coopérer les Etats membres de l'UE pour améliorer la cybersécurité.
- Couvrir un plus grand nombre d'entités et de secteurs pour une protection plus complète.
- Mettre en place un système unifié pour signaler les incidents de cybersécurité et gérer les cybercrises.
- Renforcer la sécurité de la chaîne d'approvisionnement et s'attaquer aux nouvelles menaces cybernétiques.

Source : DIRECTIVE (UE) 2022/2555 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 décembre 2022

La cyberhygiène des sauvegardes à la base de votre capacité de résilience

Les récentes catastrophes informatiques, qu'elles soient dues à des cyberattaques, des erreurs humaines ou des catastrophes naturelles, rappellent l**a vulnérabilité de nos infrastructures numériques.**
La sauvegarde des données occupe une place importante dans la stratégie de cyberhygiène demandée par NIS 2.

NIS 2 confirme à toute l'Europe que la continuité des opérations est essentielle à la cyberhygiène.

Elle apparaît comme une **assurance vitale** contre la perte d'informations cruciales, **garantissant la résilience et la pérennité des activités économiques.**
Dans ce cadre, l'élaboration de plans de continuité d'activité (PCA), incluant des stratégies de sauvegarde et de récupération des données, devient une priorité pour les entreprises de toutes tailles.

LES RÈGLES D'OR :

1 Plannifier et intégrer une stratégie de sauvegarde robuste

- **Identifier** les données et systèmes critiques à sauvegarder :
  - Établir une **hiérachie** pour s'assurer que les éléments essentiels sont sauvegardés plus fréquemment.
  - Une procédure de restauration du SI doit être rédigée et régulièrement mise en œuvre.
- **Ne pas négliger la sauvegarde des environnements SaaS,** qui appliquent un modèle de responsabilité partagée.

  En savoir plus
- Effectuer des sauvegardes **en production, comme en préproduction :**
  - En cas d'échec de tests ou de modifications indésirables, elles offrent la possibilité de restaurer l'environnement à un état antérieur pour reprendre les tests entamés.
  - Documenter la stratégie de sauvegarde et s'assurer de son intégration au sein de l'organisation.

2 Respecter la règle de sauvegarde 3-2-1-1

Conservez trois copies de vos données

Un original et au moins deux copies

Stockez vos sauvegardes sur deux différents types de support

Dispositif NAS, bande ou lecteur local, par exemple

Conservez une copie hors site

Air-Gap - Dans le cloud ou dans un stockage sécurisé hors site et hors ligne

Assurez-vous qu'une copie de vos données est immuable

3 Sécuriser les données sauvegardées

- **Systématiser et tester régulièrement votre PRA** (Plan de Reprise d'activité)
- **La sauvegarde est régulière et automatisée** dans la mesure du possible
- **La capacité de restauration** des données à partir des sauvegardes **est régulièrement testée.** La planification et l'exécution de ces tests périodiques garantit le fait que les sauvegardes sont complètes et fonctionnelles.
- Ces tests doivent être systématisés et **appartenir à un plan de reprise ou continuité d'activité.**

4 Sécuriser les données sauvegardées

- **Les sauvegardes sont cryptées,** tout particulièrement si elles doivent être déplacées d'un endroit à l'autre.
- **Chaque instance de sauvegarde doit disposer de comptes dédiés** et facilement identifiables, tout comme **les comptes d'administrateurs pour la sauvegarde qui doivent être nominatifs et dédiés** pour chaque opérateur.
- L'immuabilité (deuxième 1 de la stratégie) correspond à **un format qui ne peut être ni être modifié ni supprimé.** Ainsi, vous n'aurez pas à payer de rançon pour récupérer vos données en cas d'attaque.
- **La surveillance continue** s'avère indispensable. Elle passe par l'implémentation de solutions de détection permettant de surveiller toute activité suspecte ou toute tentative d'accès non autorisé aux sauvegardes.
- **Une solution déconnectée (air-gapping)** limite la propagation des ransomwares et optimise la résilience des données.

POUR ALLER PLUS LOIN :
ANSSI Sauvegarde des systèmes d'Information les fondamentaux

Quand conformité rime avec simplicité

Pour **répondre aux exigences de conformité NIS 2 de manière pragmatique et rentable,** il faut savoir compter sur **des solutions efficaces et ciblées** pouvant faciliter **l'alignement entre cybersécurité et objectifs de l'entreprise.**

Arcserve en tant que plateforme de résilience des données unifiées vous fournit les outils pour simplifier votre conformité :

Une vision unifiée de la situation des sauvegardes en quelques clics

une plateforme de gestion des sauvegardes unifiée pour simplifier les tests de restauration, les reporting, les ajustements en fonction des risques et du PRA. Eliminer les couches d'outils disparates sans nuire à la facilité d'utilisation est la première étape de mise en conformité.

Des couches de sécurité à tous les étages

un système de cybersécurité et un stockage immuable qui vous protègent contre les attaques par ransomware. Vos données sont chiffrées et protégées contre tout accès non autorisé. L'intégration avec Sophos X bloque proactivement les attaques notamment grâce aux technologies de deep learning.

Une flexibilité à toute épreuve pour s'adapter en continue aux normes en vigueur

Parce que vous n'aurez pas tous les mêmes exigences de mise en conformité et les mêmes ressources, il est indispensable de pouvoir compter sur la polyvalence nécessaire pour mettre à niveau rapidement et efficacement votre stratégie de sauvegarde et de reprise après sinistre tout en utilisant le matériel de votre choix.

Réduire les coûts tout en éliminant les risques de perte de données

Ajuster la protection et sa couverture en fonction des objectifs de RTO et RPO et accords de niveau de service sans vous ruiner : une évolutivité quasi illimitée afin d'adapter le stockage à moindre coût au fur et à mesure de la croissance des données.

Un PRA économique et tout-en-un en seulement 15 minutes

Des appliances qui permettent une sauvegarde complète et économique de vos environnements et qui intègrent nativement le Disaster Recovery (DR). Bénéficiez ainsi d'un PRA (Plan de Repise d'Activité / PCA (Plan de Continuité d'Activité) embarqué pour une simplicité d'utilisation sans précédent en consolidant votre matériel et vos logiciels au sein d'une seule plate-forme.

Une fiabilité du système éprouvée

Les centres de données Arcserve figurent parmi les installations les plus sécurisées et les plus impénétrables au monde : système de sécurité biométrique, sas de sécurité, système de chiffrement multiniveau, stockage autoréparable, contrôle d'accès basé sur les rôles, anonymat des données…

Grâce à des solutions de sauvegarde, de restauration, de réplication, de haute disponibilité et de déduplication sur une plateforme unifiée vous pouvez **tester facilement la restauration de vos applications et données sans perturber vos activités.**

Arcserve protège et sécurise tous les environnements de données en éliminant les intégrations complexes pour une gestion unifiée de la résilience de vos données avec une supervision puissante, simple et intuitive, au plus bas coût de possession total.

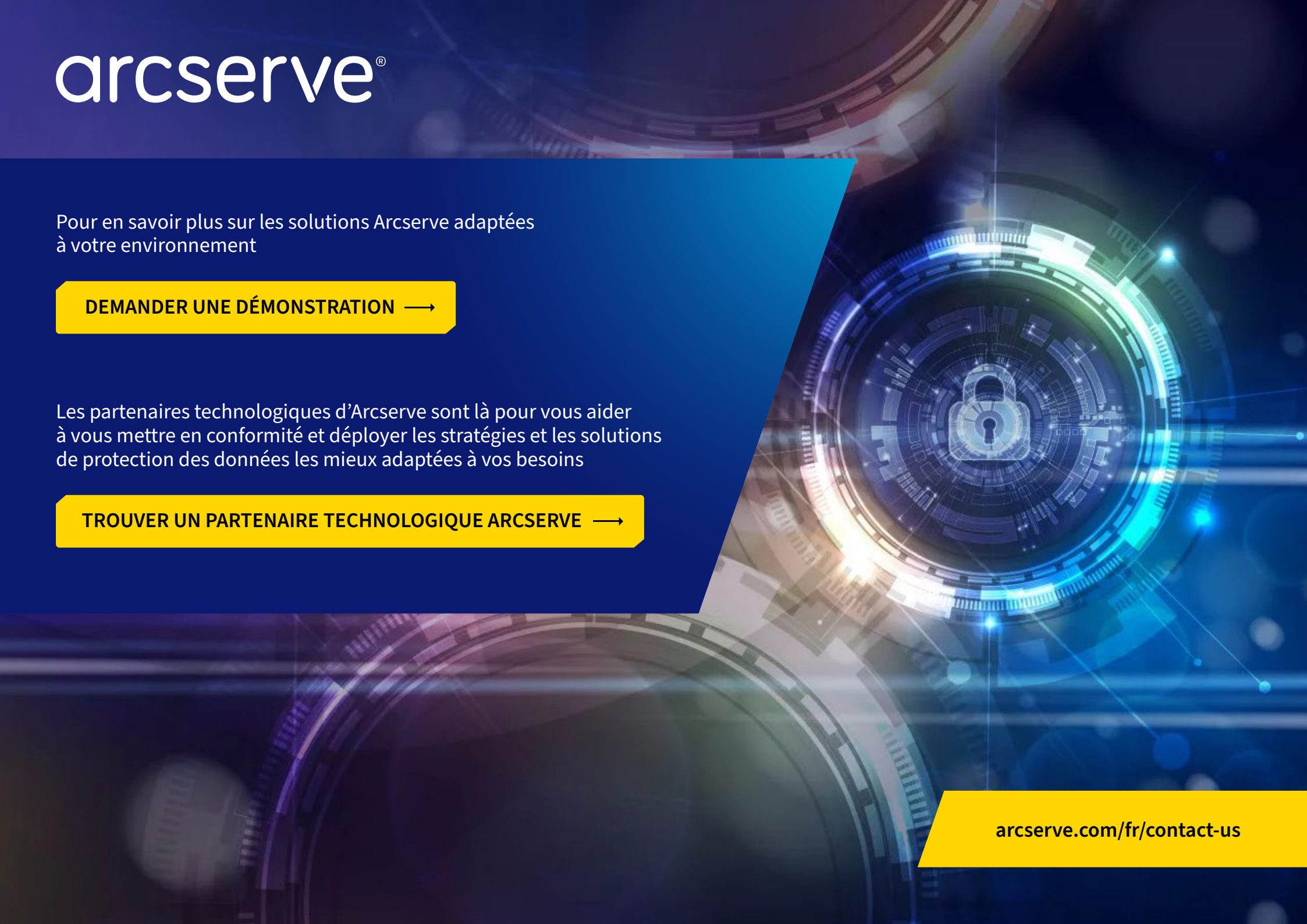
arcserve®

Pour en savoir plus sur les solutions Arcserve adaptées à votre environnement

DEMANDER UNE DÉMONSTRATION ⟶

Les partenaires technologiques d'Arcserve sont là pour vous aider à vous mettre en conformité et déployer les stratégies et les solutions de protection des données les mieux adaptées à vos besoins

TROUVER UN PARTENAIRE TECHNOLOGIQUE ARCSERVE ⟶



arcserve.com/fr/contact-us