NumSpot

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.

Ce qu'il faut retenir de NIS2

Qu'est-ce que **NIS2 ?**

La directive **Network and Information System** (NIS 2) est un texte législatif adopté par le Parlement et le Conseil de l'Union européenne le 14 décembre 2022,. Elle remplace et abroge la directive NIS 1, et a pour but de renforcer la cybersécurité des réseaux et des systèmes d'information au sein de l'Union européenne.

La directive NIS2 amène les Etats membres à renforcer leur **coopération en matière de gestion de crise cyber**, en donnant notamment un cadre formel au réseau CyCLONe (Cyber Crisis Liaison Organisation Network) qui rassemble l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et ses homologues européens.

Elle impose des **obligations minimales** en matière de cybersécurité et de **déclaration d'incidents** aux opérateurs de services essentiels (OSE) ainsi qu'aux fournisseurs de services numériques (FSD). Ces obligations devront être mises en œuvre avant janvier 2024 sous peine d'amendes sévères.

Quelles sont les obligations ?

L'élargissement du type d'organisations concernées

De **19 à 35 secteurs**. (Services postaux, gestion des déchets, production et distribution de produits chimiques, secteurs agricoles et alimentaires...) pour toute entreprise employant plus de 250 personnes, dont le chiffre d'affaires annuel dépasse 50 millions d'euros et/ou dont le bilan annuel est supérieur à 43 millions d'euros.

Concernant **les fournisseurs de réseaux publics de communications électroniques**, ils devront appliquer ces mesures quelle que soit leur taille.

Le renforcement des exigences en matière de sécurité

Le renforcement des exigences de sécurité impose de :

- Fournir une liste minimale d'éléments de sécurité à appliquer
- Notifier les incidents (24 heures suivant la découverte de l'incident)
- Réaliser une évaluation des risques et mettre en place des politiques de sécurité des systèmes d'information suffisantes
- Prévenir, détecter et réagir rapidement aux incidents
- Gérer les crises et assurer la continuité opérationnelle en cas d'incident cybernétique majeur
- Assurer la sécurité de leur supply chain
- Assurer la sécurité de leur réseau et de leurs systèmes d'information
- Mettre en place des politiques et des procédures permettant d'évaluer l'efficacité du management de la sécurité informatique
- Utiliser un chiffrement fort

Une collaboration accrue

Création du réseau européen des organisation de liaison en cas de cybercrise (EU CyCLONe), spécifiquement dédié à ces initiatives. Une mesure qui vise à améliorer la collaboration entre les États membres de l'UE, en renforçant la confiance et en facilitant le partage d'informations pour mieux coordonner la gestion des crises

Les sanctions financières potentielles en cas de non-application :

- Jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial total pour un DSP (Fournisseur de Services Numériques)
- Jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial total pour un OES (Opérateur de Services Essentiels)

Des rapports d'incident plus rapide

Exigence de communication des entités concernées aux équipes nationales respectives de réponse aux incidents de sécurité informatique (CSIRT) de tout incident ayant un effet majeur sur leurs services :

- Envoi d'une alerte rapide dans les 24 heures suivant la prise de connaissance de l'incident, indiquant si l'incident pourrait résulter d'actes malveillants ou avoir une incidence transfrontalière
- Envoi d'une notification d'incident dans les 72 heures, comprenant une première analyse de l'incident, de son ampleur et de ses conséquences
- Envoi d'un rapport intermédiaire à la demande du CSIRT ou de l'autorité compétente
- Envoi d'un rapport final au plus tard un mois après la notification de l'incident, détaillant la cause probable de l'incident, les mesures d'atténuation mises en œuvre et les éventuelles répercussions transfrontalières de l'incident.

À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous @NumSpot @NumSpotCloud