One System
DATACENTER CLOUD SOLUTIONS

NIS2

2024

Sommaire

One System
DATACENTER CLOUD SOLUTIONS

01. Introduction à NIS2

Contexte et Objectifs de NIS2

Avant

Renforcer la coopération entre les états membres

Améliorer la sécurité nationale des réseaux et des systèmes d'information

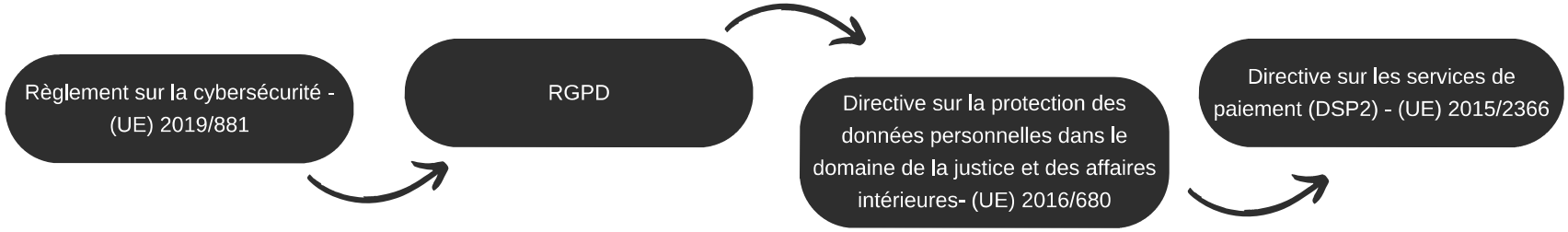
Sécuriser les réseaux et les systèmes

Maintenant

Protection étendue pour secteurs essentiels

Sécurité renforcée à l'échelle européenne

Gouvernance améliorée, responsabilité claire



One System
DATACENTER CLOUD SOLUTIONS

02. Pourquoi cette directive?

Contexte et Objectifs de NIS2

Pourquoi était-il nécessaire de faire évoluer NIS2 à l'échelle européenne?

385 000 attaques réussies ont touché les systèmes d'information des organisations

Soit une moyenne de **1,8 cyberattaque par organisation et par an**.

43 % d'organisations ayant subi au moins une cyberattaque au cours des **douze derniers mois**

Ce sont les PME qui sont les plus touchées : **330 000 fois**

Les grandes entreprises et entreprises de taille intermédiaire: **17 000 fois**.

De leur côté, les administrations publiques ont subi **37 000 cyberattaques**.

Il est toutefois important de noter que la part d'organisations publiques de 250 employés ou plus ayant été victime de cyberattaque s'élève à **51 %**.

Source: ANSSI - panorama de la menace 2022

03. Champ d'Application de NIS2

Entités concernées

Toutes entreprises dépendant des secteurs d'activité suivants ou intervenants dans la chaîne d'approvisionnement de ces secteurs.

Secteurs essentiels

- Energie
- Transports
- Santé
- Espace
- Administration publique
- Infrastructure numérique
- Eau potable
  Eaux usées
- Banque
  Marchés financiers

Secteurs importants

- Services postaux et d'expédition
- Gestion des déchets
- Machines équipements n.c.a
- Recherche
- Produits chimiques
- Dispositifs médicaux
- Véhicules
  Remorques
  Semi-remorques
- Informatiques
  Electroniques
  Optiques
- Autres matériels de transport

Entités Non-UE Fournissant des Services dans l'UE

Exclusion et Exception

Exclusion

Petite entreprise

- **Moins de 50 salariés**

- **Chiffre d'affaires annuel ou un total de bilan < 10 millions**

Exception

Si ces entreprises :

- Jouent un rôle clé dans la fourniture de services essentiels
- Ont un impact significatif sur la sécurité nationale ou européenne

Elles seront désignées comme des entités essentielles ou importantes et donc être soumises aux obligations de la NIS2.

Taille entité	Nombre d'employés	CA (en Millions d'euros)	Bilan annuel (en millions d'euros)
Intermédiaire et grande	x ≥ 250	y≥50	z≥43
Moyenne	50 ≥ x ≥250	10 ≥ y ≥ 50	10 ≥ z ≥43
Micro et petite	x < 50	y < 10	z < 10

One System
DATACENTER CLOUD SOLUTIONS

04. Exigences Clés de NIS2

Mesures de sécurité minimum

Tests et
audits de sécurité

Sécurité des
systèmes et réseaux

Gestion
des accès

Sécurité physique
et environnementale

Gestion
des risques

Formation
Sensibilisation

Cyberhygiène

Gestion
des incidents

Plan de continuité et
récupération après
sinistre

One System
DATACENTER CLOUD SOLUTIONS

05. Implication des entreprises

Sanctions

Amendes

Substantielles pouvant atteindre un pourcentage significatif de leur chiffre d'affaires annuel

Suspension des certifications et autorisations

Compromettant la capacité à opérer normalement.

Divulgation des non-conformités

Manquements publiquement divulgués, ce qui pourrait gravement nuire à la réputation.

Suspension des responsabilité de direction

Impactant la gouvernance et le management.

06. Se protéger

Une approche holistique

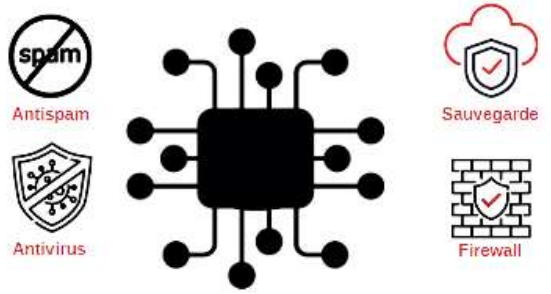
1.Auditer

Se protéger, c'est d'abord comprendre où l'on se situe pour pouvoir décider des meilleures mesures à adopter.

Pour une cybersécurité optimale, adoptez une approche holistique.
Auditez votre situation pour cibler les meilleures mesures, sensibilisez vos collaborateurs, et réduisez votre surface d'attaque avec des outils.

2.Protéger

Pour réduire efficacement votre surface d'attaque, équipez-vous des meilleurs outils : anti-spam, antivirus, sauvegarde, firewall, et notre solution avancée iPROTECT conçus pour renforcer votre cybersécurité à chaque niveau.



3.Sensibiliser

Savoir pour se défendre : Un collaborateur informé est un rempart supplémentaire contre les cybermenaces.

One System
DATACENTER CLOUD SOLUTIONS

Protéger votre responsabilité

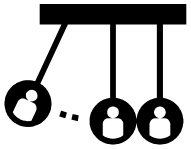
Source : Unsa

One System
DATACENTER CLOUD SOLUTIONS

S’assurer

- Assistance/ Gestion de crise 24/7

- Prise en charge des dommages subis



- Dommages causés à des tiers

Couts visibles
Frais investigation & monitoring
Restauration système information
Renforcement cybersécurité
Coût communication / Gestion crise
Frais notification
Frais mise en conformité
Frais juridiques

Couts moins visibles
Préjudice financier causé aux tiers (RC Cyber)
Perte de CA / Marge Brute
Frais supplémentaires d’exploitation
Perte de propriété intellectuelle
Perte de client
Perte de valeur / Perte d’image
Coût de la nouvelle dette

- Frais de défense juridique
- Dommages et intérêts versés suite à une réclamation d’un tiers.

One System

DATACENTER CLOUD SOLUTIONS

Merci pour votre attention !

A vos questions.

Contact@one-system.fr 09 72 50 59 75 29 Rue de Foliouses Miribel 01700 www.one-system.fr