Cyber Resilience Act

Nantes Université

Guilhem MOUROUVIN
Habiba BAKRY
Mahir SOULTANA
Ward JACQUET
Marvin ROLLO

Sommaire

C’est quoi le Cyber resilience Act?

Une législation européenne visant à renforcer la résilience des produits et services numériques face aux cybermenaces. Cette loi introduit des exigences de sécurité pour les fabricants et fournisseurs.

Les 4 attendus du CRA

ÉTAPES	EXIGENCES POUR LES FABRICANTS	
Évaluation des Risques	**Les produits doivent être livrés**	Sans vulnérabilités connues exploitables
		Sécurisés par défaut avec une surface d'attaque limitée
		Minimisant le traitement des données
Documentation	**Les fabricants doivent fournir une documentation couvrant**	La conception du produit, la livraison et la gestion des vulnérabilités
		L'évaluation des risques et la déclaration de conformité
		La liste des composants logiciels (SBOM)
Évaluation de la Conformité	**Les fabricants doivent fournir une déclaration de conformité**	Auto-évaluation
		Fournie par un auditeur tiers indépendant
		Les vulnérabilités activement exploitées
Signalement des Vulnérabilités	**Les vulnérabilités doivent être signalées à l'ENISA**	Les incidents de sécurité affectant le produit
		Dans les 24 heures suivant leur découverte

Quelles sont ses ambitions et utilité ?

01 Renforcer la sécurité des produits numériques

02 Protéger les consommateurs et les entreprises

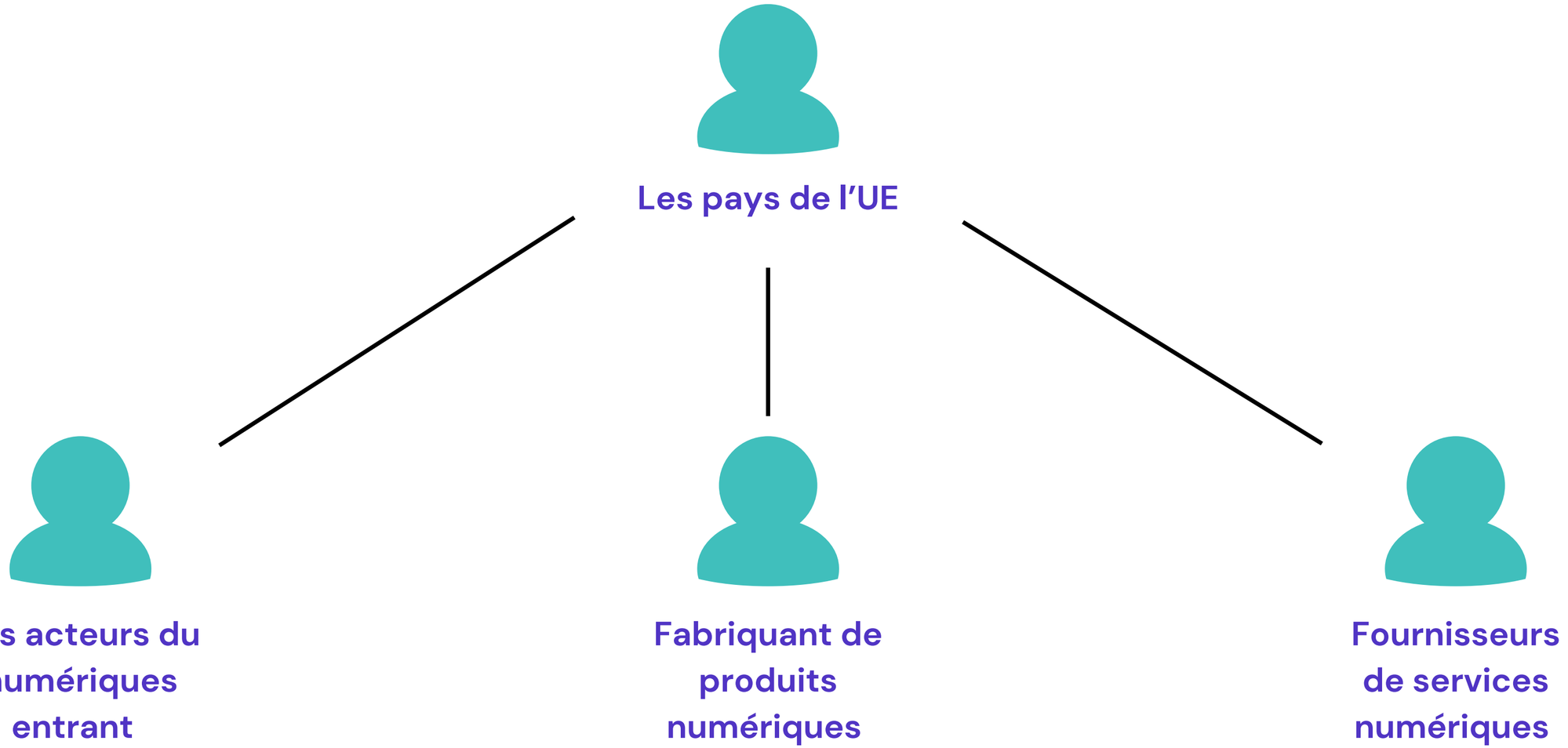
03 Harmoniser les normes de sécurité en Europe

04 Favoriser l'innovation responsable

Historique de la CRA

- **Septembre 2022** : Règlement sur la cyber-résilience a été publiée
- **Novembre 2023:** Parlement européen et le Conseil sont parvenus à un accord politique
- **Mars 2024:** Le texte a été voté par le Parlement
- **Octobre 2024:** Le texte a été voté par le Conseil

Qui est concerné ?



Comment s’y conformer ?

Face à ce texte européen, un grand chantier attend les entreprises pour s’y conformer

EVALUATION DES RISQUES

Les entreprises doivent évaluer les risques de sécurité associés à leurs produits et services numériques.

CONCEPTION SECURITAIRE

Adopter des pratiques de sécurité dès les premières étapes du développement.

TEST ET CERTIFICATIONS

Soumettre les produits et services à des tests de sécurité rigoureux et obtenir des certifications conformes aux normes européennes.

Comment s’y conformer ?

Face à ce texte européen, un grand chantier attend les entreprises pour s’y conformer

MISE A JOUR ET SUPPORT

Garantir des mises à jour régulières et un support continu pour corriger les vulnérabilités découvertes.

DOCUMENTATION ET TRANSPARENCE

Fournir une documentation détaillée sur les mesures de sécurité mises en place et informer les utilisateurs des risques potentiels.

Quelles sont les sanctions ?

01 AMENDES FINANCIÈRES

02 INTERDICTION DE MISE SUR LE MARCHÉ

03 RESPONSABILITÉ CIVILE

La finalité du CRA

01 ENCOURAGER L’INNOVATION

02 FAVORISER L’ÉQUITÉ

03 CONSOLIDER LA CONFIANCE

Merci de votre écoute

Nantes Université

Guilhem MOUROUVIN
Habiba BAKRY
Mahir SOULTANA
Ward JACQUET
Marvin ROLLO