🧾 Résumé du Panorama de la cybermenace 2024 – ANSSI

Document complet disponible ici :

📄 Panorama de la cybermenace 2024 - ANSSI (PDF)

🔗 [Site officiel de l’ANSSI](https://www.ssi.gouv.fr/)

🎯 Objectif

Document de synthèse publié annuellement par l’ANSSI, il analyse les principales menaces, attaques, techniques et tendances de cybersécurité observées en France sur l'année 2023. Il vise à sensibiliser les institutions, entreprises et partenaires à la réalité opérationnelle des cyberattaques.

🧨 Acteurs menaçants principaux

Cybercriminels (rançongiciels, extorsion)

États étrangers (Russie, Chine)

Hacktivistes (groupes idéologiques)

🏟️ Événements majeurs

Jeux Olympiques et Paralympiques Paris 2024 : surveillance renforcée, attaques observées mais sans interruption des épreuves.

Attaques par rançongiciel contre l’université Paris-Saclay et la RMN.

Tentatives d’espionnage et de désinformation dans un contexte géopolitique tendu.

🔧 Techniques d’attaque en hausse

Chaîne d’approvisionnement (logicielle et prestataires)

Exploitation de vulnérabilités sur les équipements en bordure de réseau (VPN, pares-feux, etc.)

Utilisation d’infrastructures d’anonymisation

Professionnalisation des cybercriminels et partage d’outils avec des acteurs étatiques

💰 Finalités des attaques

Financières : rançongiciels, extorsion de données.

Politiques : déstabilisation et influence (DDoS, sabotage, hameçonnage).

Stratégiques : espionnage (télécoms, services publics, cloud).

🛡️ Recommandations de l’ANSSI

Sécurisation des SI (mises à jour, durcissement, cloisonnement).

Supervision active : détection comportementale.

Réponse à incident structurée.

Priorisation de la sécurité sur les équipements critiques (Active Directory, VPN, sauvegardes hors ligne).

Segmentation réseau, authentification forte, plans de remédiation.

📊 Chiffres clés

4386 événements de sécurité traités en 2023 (+15 %).

3004 signalements, 1361 incidents confirmés.

Pics lors de la période des JOP (mai–septembre 2023).

📘 Cadre réglementaire

🇪🇺 Cyber Resilience Act (CRA)

Adopté le 23 octobre 2024 par l’Union européenne, ce règlement impose :

Une cybersécurité intégrée dès la conception des produits numériques.

Des configurations sécurisées par défaut.

Une obligation de notification des vulnérabilités.

📄 Texte officiel :

👉 [Règlement (UE) 2024/2847 dit Cyber Resilience Act (EUR-Lex)](https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32024R2847)

🇫🇷 Dispositif national de signalement des vulnérabilités

Article L.2321-4 et L.2321-4-1 du Code de la défense

Oblige les éditeurs de logiciels à notifier l’ANSSI des vulnérabilités et incidents majeurs

📄 Texte officiel :

👉 Code de la défense – Légifrance – L2321-4

👉 Code de la défense – L2321-4-1 (créé en 2024)

🔐 CERT-FR – Coordination de vulnérabilités

Opéré par l’ANSSI, le CERT-FR est chargé du traitement sécurisé des vulnérabilités :

Plateforme officielle :

👉 [Déclaration au CERT-FR via ClubSSI](https://club.ssi.gouv.fr/#/declarations)