VILLE DE CHELLES

Direction des Systèmes d'Information

Cybersécurité : nous sommes déjà attaqués, tous les jours

Ouverture de la visio cyber
à l'attention des DGS

DSI | Octobre 2026

« Pas si, mais quand » ?

Une formule souvent entendue… mais dépassée

On l'a beaucoup entendu :
« La question n'est pas de savoir si l'on va se faire attaquer, mais quand. »

En réalité, nous sommes attaqués tout le temps.

218 incidents en collectivités traités par l'ANSSI en 2024, soit 18 par mois

Source : ANSSI, état de la menace sur les collectivités 2024 (févr. 2025)

La question n'est donc plus « quand », mais « sommes-nous protégés ? »

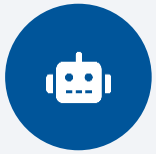
Messagerie
≈ 30 % des incidents en collectivité : compromission de comptes de messagerie

VPN et accès distants
Cible des identifiants volés et des failles non corrigées : MFA obligatoire

Services exposés sur Internet
Sites, extranets, portails : scannés en continu par des robots

Une menace permanente et automatisée

Les attaquants ne nous choisissent pas : des robots cherchent la porte ouverte



Des robots

scannent Internet 24 h/24 à la recherche de failles



Des identifiants

de nos agents déjà en vente sur le dark web



Une porte ouverte

faille non corrigée, compte sans double authentification



L'impact

rançongiciel, vol de données, services à l'arrêt

Pour quels types de collectivités ? Toutes.

Petites communes
moins de moyens, souvent une cible facile

Villes moyennes
SI étendu, NIS 2 dès 30 000 hab. (seuil à confirmer)

Grandes villes & EPCI
forte exposition, services critiques

Départements & régions
ciblés au-delà de leur poids

Le socle minimal, quelle que soit la taille de la collectivité

Sauvegardes
Quotidiennes, une copie mensuelle en lieu sûr (hors ligne), restaurations testées

Messagerie
Point d'entrée préféré des cybercriminels : filtrage, anti-hameçonnage

Périmètre exposé
Sécuriser le SI et tout ce qui est exposé sur Internet

Antivirus à jour
Sur l'ensemble des équipements : postes et serveurs

EDR / sandbox
Antivirus de dernière génération, basés sur le comportement

Mises à jour
Postes, serveurs et équipements de sécurité

Mots de passe & MFA
Politique renforcée, double authentification sur VPN, messagerie, extranet

Comptes admin
Comptes à privilèges séparés, nominatifs et limités au strict nécessaire

En bleu clair : mesure ajoutée au socle

Et également…

Pour détecter et contenir une attaque, pas seulement l'empêcher

Segmentation des réseaux
Séparer serveurs, DSI, IT et OT (bâtiments, vidéoprotection…)

Cartographie du SI
On ne protège bien que ce que l'on connaît

Gestion des tiers
Supervision des accès prestataires : tracés, limités dans le temps

SOC / SIEM : journalisation centralisée

EDR | Pare-feu | NDR | AD / journaux

↓

Corrélation et surveillance 24/7

↓

Alerte : modification en masse de fichiers

Un SOC limité à l'EDR ne suffit pas : intégrer au minimum 2 à 3 technologies.

Gouvernance : piloter avec quelques indicateurs

Trois indicateurs simples à suivre en comité de direction

Exposition sur Internet

Périmètre suivi via le service Silène de l'ANSSI

Avec un WAF : volume de requêtes bloquées

Mises à jour de sécurité

Niveau de mise à jour de vos équipements

Part des postes, serveurs et équipements à jour

Sécurité de l'Active Directory

Évaluée avec l'outil ORADAD de l'ANSSI

Niveau de sécurité de l'AD et son évolution

Un comité cyber à intervalle régulier

Rythme adapté à la taille de la collectivité, avec la DG, la DSI et le RSSI : suivi des indicateurs, incidents, arbitrages.

Se préparer à la crise

La différence entre un incident et une catastrophe se joue avant l'attaque

Avant

- Plan de réponse et fiches réflexes
- Annuaire de crise hors SI (papier)
- Exercice de crise annuel avec la DG et les élus
- Contrat d'assurance cyber à vérifier

Pendant

- Isoler sans éteindre les machines
- Alerter le CSIRT régional, 17Cyber, l'ANSSI
- Ne pas payer la rançon
- Communication maîtrisée

Après

- Dépôt de plainte
- Notification CNIL sous 72 h si données personnelles
- Reconstruction et retour d'expérience

Les contacts à avoir sous la main, hors SI

17Cyber (cybermalveillance.gouv.fr) • CSIRT régional • ANSSI / CERT-FR • assureur • prestataires

Les sujets à venir

Quatre chantiers à anticiper dès maintenant

NIS 2 – loi Résilience

- Transposition attendue depuis plus de 2 ans
- Examen à l'Assemblée encore reporté (oct. 2026)
- 3 ans pour être conforme après promulgation

Gestion des tiers : clauses dans les marchés

- Notification d'incident
- Réversibilité
- Localisation des données
- Accès des tiers

IA : éviter les fuites de données

- Charte d'usage et outils validés
- Pas de données sensibles dans les outils grand public
- Filtrage des requêtes avant envoi

Sensibilisation régulière et traçable

- Pour les agents comme pour les élus
- Les campagnes de phishing simulé servent de preuve directe

Ce que l’on attend de la direction générale

La cybersécurité est un risque de continuité du service public, pas un sujet technique

1

Porter le sujet
En faire une priorité de la direction générale et de l’exécutif

2

Arbitrer les moyens
Un budget pluriannuel : socle, détection, conformité NIS 2

3

Instaurer la gouvernance
Comité régulier, indicateurs, un RSSI identifié (même mutualisé)

4

Impliquer élus et directions
Sensibilisation, exercice de crise, clauses dans les marchés

VILLE DE CHELLES

Direction des Systèmes d'Information

Place aux échanges

Merci de votre attention