PERIMETRY RESEARCH

# Baromètre de la sécurité des collectivités allemandes

Les Landkreise, villes-arrondissements et Länder allemands protègent-ils bien leurs sites et leur messagerie ? Mesures passives, comparées aux collectivités françaises.

**Édition de novembre 2026**

**387**
domaines avec un site à eux, notés

**41,1 %**
appliquent DMARC (quarantine ou reject)

**32,3 %**
ont A ou B

**Perimetry Cloud**
perimetry.cloud · Publiée le 14 novembre 2026

# À propos de ce rapport

Perimetry Research publie des études sur la façon dont les organisations protègent leurs sites et leur messagerie, mesurée avec les mêmes contrôles passifs que Perimetry Cloud. Cette édition porte sur 411 domaines des Landkreise, villes-arrondissements et Länder allemands ; 410 sont actifs, et les 387 qui ont un site à eux sont notés. Elle ne nomme que les collectivités qui font bien ; tous les autres chiffres sont des moyennes, et les problèmes graves ont été signalés en privé aux collectivités avant la publication. Aucun e-mail n'est envoyé à ces collectivités : l'étude est seulement publiée.

# Sommaire


01 Synthèse 3

02 Principaux constats 4

03 Notes 5

04 Contrôle par contrôle 6

05 Par catégorie 8

06 Les domaines sans site à eux 9

07 Comparaison avec nos autres études 10

08 Les collectivités qui font bien 11

09 Problèmes graves 12

10 Recommandations 13

11 Méthodologie 14

12 À propos de Perimetry 16

01

# Synthèse

**387**
domaines avec un site à eux, notés

**62**
note moyenne sur 100

**41,1 %**
appliquent DMARC (quarantine ou reject)

**32,3 %**
ont A ou B

Note moyenne des 387 domaines notés : 62 sur 100 ; médiane 67.

1. 73,6 % des domaines notés publient une politique DMARC et 41,1 % l'appliquent (collectivités françaises : 32,8 % ; councils britanniques : 95,5 %).
2. Côté sites : 96,4 % ont un certificat valide, 92 % renvoient vers HTTPS, 74,3 % utilisent HSTS d'au moins six mois.
3. 15 % des domaines notés sont signés avec DNSSEC ; 12,4 % publient un enregistrement CAA.
4. 23 domaines actifs n'ont pas de site à eux ; 73,9 % d'entre eux n'appliquent pas DMARC.

02

# Principaux constats

73,6 % des domaines notés publient une politique DMARC et 41,1 % l'appliquent (collectivités françaises : 32,8 % ; councils britanniques : 95,5 %).

Côté sites : 96,4 % ont un certificat valide, 92 % renvoient vers HTTPS, 74,3 % utilisent HSTS d'au moins six mois.

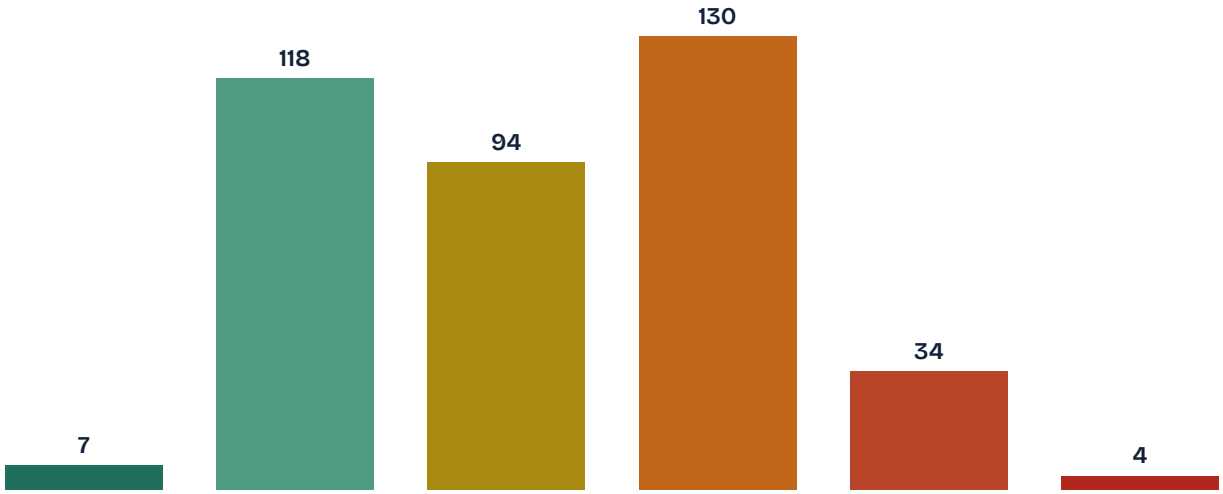
15 % des domaines notés sont signés avec DNSSEC ; 12,4 % publient un enregistrement CAA.

23 domaines actifs n'ont pas de site à eux ; 73,9 % d'entre eux n'appliquent pas DMARC.

03

# Notes

Chaque domaine qui a un site à lui reçoit une note : la part des neuf contrôles qu'il réussit, parmi ceux qui le concernent (la note de nos autres études, sans le contrôle de l'adresse de contact, que les listes ne donnent pas). A à partir de 90, B de 75, C de 60, D de 40, E de 20, F en dessous.

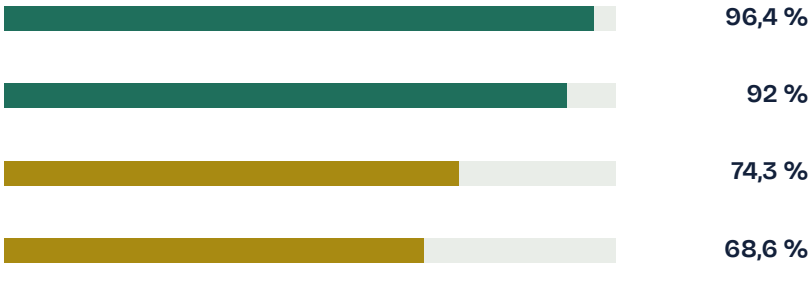


04

# Contrôle par contrôle

Part des domaines notés qui réussissent chaque contrôle, parmi ceux qu'il concerne.

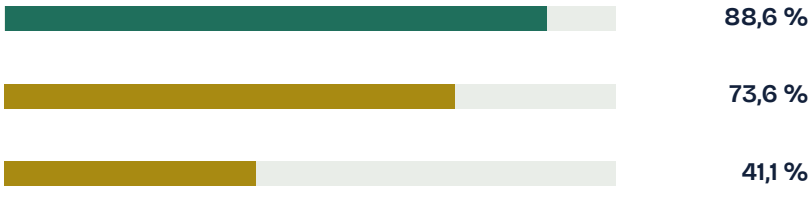
## Site web




## DNS




## E-mail




| Les neuf contrôles | |
|---|---|
| **Site web · Certificat HTTPS valide** | Le site répond en HTTPS avec un certificat en cours de validité, émis pour son nom et reconnu par les navigateurs. |
| **Site web · HTTP renvoie vers HTTPS** | Quelqu'un qui tape l'adresse arrive sur le site chiffré, et non sur une page que n'importe qui sur le réseau peut lire ou modifier. |
| **Site web · HSTS d'au moins six mois** | Les navigateurs retiennent qu'il faut utiliser HTTPS : la première requête non chiffrée ne peut pas être détournée. |
| **Site web · En-têtes de protection de base** | X-Content-Type-Options: nosniff, et une protection contre l'affichage du site dans le cadre d'un autre site (X-Frame-Options ou frame-ancestors dans la CSP). |
| **DNS · DNSSEC** | Les réponses DNS du domaine sont signées : on ne peut pas faire croire à un résolveur que le site ou la messagerie de l'administration sont ailleurs. |
| **DNS · Enregistrement CAA** | Le domaine désigne les autorités de certification autorisées à émettre des certificats à son nom. |
| **E-mail · SPF strict** | Le domaine liste les serveurs autorisés à envoyer son courrier et demande de rejeter ou de signaler les autres (-all ou ~all). |

| Les neuf contrôles | |
|---|---|
| **E-mail · Enregistrement DMARC** | Le domaine publie une politique DMARC, la norme qui relie SPF et DKIM à l'expéditeur affiché. |
| **E-mail · DMARC appliqué** | La politique est quarantine ou reject : un message falsifié au nom de l'administration, adressé à des usagers par exemple, part en indésirables ou est refusé, au lieu d'être distribué. |

05

# Par catégorie

Les catégories de moins de dix domaines notés ne sont pas détaillées.

| Groupe | Notés | Moyenne | A ou B | DMARC appliqué | Médiane |
|---|---|---|---|---|---|
| **Landkreise (arrondissements)** | 274 | 62 | 31,8 % | 40,1 % | 67 |
| **Kreisfreie Städte (villes-arrondissements)** | 100 | 63 | 31 % | 44 % | 67 |
| **Länder (États fédérés)** | 13 | 71 | 53,8 % | 38,5 % | – |

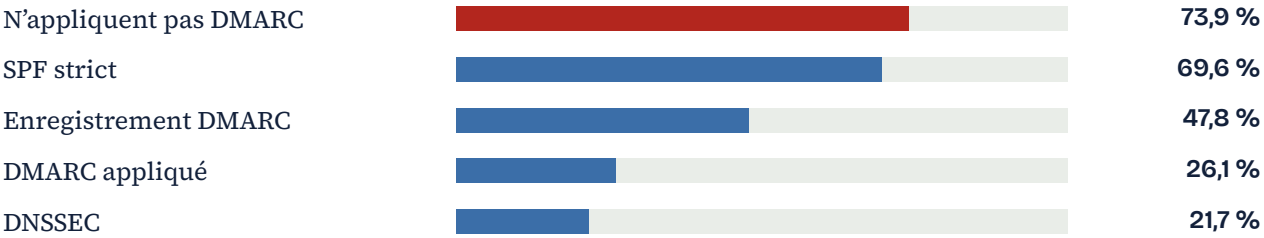
## Moyenne



06

# Les domaines sans site à eux

23 domaines actifs n'ont pas de site à eux : 13 renvoient vers un autre site, 10 ne servent qu'à la messagerie. Ils peuvent quand même servir à falsifier des e-mails au nom de la collectivité, et sont jugés sur leur DNS et leur messagerie seulement.




Note moyenne sur le DNS et la messagerie seulement : 36 sur 100.

07

# Comparaison avec nos autres études

Les mêmes contrôles dans nos autres études (dernières éditions) : part des domaines notés qui réussissent chacun. Les collectivités françaises comptent dix contrôles, les autres neuf.

| | Allemagne | Councils | Collectivités FR | État français |
|---|---|---|---|---|
| **Note moyenne** | 62 | 69 | 60 | 46 |
| **Certificat HTTPS valide** | 96,4 % | 98,1 % | 98,7 % | 63,8 % |
| **HTTP renvoie vers HTTPS** | 92 % | 85,5 % | 90,9 % | 77,3 % |
| **HSTS d'au moins six mois** | 74,3 % | 57 % | 38,8 % | 33,3 % |
| **En-têtes de protection de base** | 68,6 % | 74,3 % | 40,7 % | 51,9 % |
| **DNSSEC** | 15 % | 1,9 % | 25,9 % | 3,8 % |
| **Enregistrement CAA** | 12,4 % | 11,4 % | 2,6 % | 18,5 % |
| **SPF strict** | 88,6 % | 100 % | 97,1 % | 56,2 % |
| **Enregistrement DMARC** | 73,6 % | 99,4 % | 77,8 % | 56,7 % |
| **DMARC appliqué** | 41,1 % | 95,5 % | 32,8 % | 43,3 % |

08

# Les collectivités qui font bien

7 collectivités réussissent les neuf contrôles et n’ont aucun problème grave.

| Collectivité | Catégorie |
|---|---|
| **Bayern** | Länder (États fédérés) |
| **Hamburg** | Länder (États fédérés) |
| **Landkreis Haßberge** | Landkreise (arrondissements) |
| **Heilbronn** | Kreisfreie Städte (villes-arrondissements) |
| **Ingolstadt** | Kreisfreie Städte (villes-arrondissements) |
| **Kreis Plön** | Landkreise (arrondissements) |
| **Landkreis Teltow-Fläming** | Landkreise (arrondissements) |

09

# Problèmes graves

Un domaine a un problème grave qui pourrait être utilisé contre lui. Il n'est nommé ni dans ce rapport ni ailleurs : la collectivité a été prévenue en privé avant la publication.

| | |
|---|---|
| Certificats expirés | 1 |

10

# Recommandations

**1** **Appliquer DMARC**
Moins de la moitié le font. Une politique quarantine, puis reject, empêche les e-mails falsifiés au nom de la collectivité d'arriver chez les habitants.

**2** **Activer HSTS et les en-têtes de protection**
HSTS fait retenir aux navigateurs de n'utiliser que HTTPS ; deux en-têtes empêchent une autre page d'afficher le site dans un cadre et le navigateur de mal lire ses fichiers.

**3** **Signer les domaines avec DNSSEC**
Peu de collectivités le font ; le registre du .de le permet.

**4** **Vérifier l'adresse sans « www »**
Plusieurs certificats expirés ont été trouvés sur le domaine nu alors que le site en www allait bien : un visiteur qui tape l'adresse courte reçoit un avertissement.

**5** **Surveiller dans la durée**
Les certificats expirent, les prestataires changent, des enregistrements se perdent lors d'une migration. Un contrôle régulier le voit avant les habitants.

11

# Méthodologie

## Des contrôles passifs uniquement

Nous lisons ce que n'importe quel visiteur ou serveur de messagerie peut voir : les enregistrements DNS publics, l'enregistrement du domaine (RDAP), le certificat TLS, une requête sur la page d'accueil en HTTP (sa redirection est lue, pas suivie), et la page d'accueil en HTTPS (en suivant ses redirections, comme un navigateur). Rien d'autre n'est demandé au site. Quand un domaine publie une politique MTA-STS, son fichier de politique est lu aussi, comme le font les serveurs de messagerie.

Pas de balayage de ports, pas de recherche de sous-domaines, pas de tentative de connexion, pas de formulaire, pas de test de vulnérabilité. Le robot est lent exprès et répartit ses requêtes sur plusieurs heures.

## Le robot

Il se présente comme PerimetryResearch/1.0 (+https://perimetry.cloud/research/methodology/). Si vous gérez un site qu'il a visité et préférez qu'il ne le fasse plus, écrivez à hello@perimetry.cloud : nous retirerons le domaine des prochaines éditions.

## L'étude des collectivités allemandes

Population étudiée : les Landkreise, villes-arrondissements (kreisfreie Städte) et Länder allemands, d'après Wikidata (CC0) : chacun avec sa clé officielle (AGS) et son site officiel. Une liste dont les effectifs s'écartent des effectifs officiels (294 Landkreise, environ 107 villes-arrondissements, 16 Länder) arrête la mesure. Berlin et Hambourg comptent comme Länder. Les communes (Gemeinden) feront l'objet d'une autre étude.

Publication seulement : aucun e-mail n'est jamais envoyé à ces collectivités ; une vulnérabilité trouvée leur est signalée en privé, sans aucune promotion, avant la publication. Une collectivité peut demander elle-même son résultat. Le reste suit l'étude de l'État français, sur neuf contrôles ; la comparaison avec les collectivités françaises porte sur ces neuf contrôles, le dixième de l'étude française (une adresse de contact sur le domaine de la collectivité) étant laissé de côté.

## Uniquement les bons élèves

Nous nommons les communes qui font bien (le tableau d'honneur et les meilleures de chaque tranche de population), jamais celles qui font mal, et jamais une commune qui a un problème grave, quelle que soit sa note. Tout le reste est publié en moyennes : par taille de commune et par département, où un département de moins de dix communes notées n'est pas détaillé, pour qu'aucune d'elles ne puisse être reconnue.

Les plateformes de sites sont notées sur un échantillon de cinq sites de communes au plus : un contrôle compte comme réussi quand la majorité de l'échantillon le réussit.

## Les problèmes graves sont signalés en privé

Certains constats pourraient servir tout de suite contre une commune : un domaine inscrit dans l'annuaire officiel qui n'existe plus (n'importe qui pourrait l'enregistrer), un domaine que le registre est en train de supprimer, un certificat expiré, un enregistrement SPF qui permet à n'importe qui d'envoyer du courrier en son nom. Ils ne sont jamais publiés. Nous prévenons d'abord la commune, discrètement, et nous les comptons dans l'étude sans nommer personne.

## Limites

Chaque édition est une photographie prise en quelques heures. L'annuaire peut être en retard ou erroné ; nous l'utilisons tel qu'il est publié. Les clés DKIM ne sont cherchées que sur les sélecteurs courants : elles ne sont donc pas notées. Un site derrière un service de protection peut répondre à un robot autrement qu'à un visiteur. Les serveurs de messagerie ne sont pas testés (STARTTLS demande le port 25, que l'infrastructure de l'étude ne peut pas joindre).

12

# À propos de Perimetry

Perimetry est un outil libre qui audite l'extérieur d'un domaine comme n'importe qui sur Internet le voit : authentification des e-mails, DNS, certificats, serveurs de messagerie, sites. Perimetry Cloud en est la version hébergée, avec surveillance continue, alertes et rapports, pour les organisations et les agences qui s'en occupent.

Citer : Perimetry Research, Baromètre de la sécurité des collectivités allemandes, novembre 2026. https://perimetry.cloud/fr/research/german-local-authorities/

Vous pouvez réutiliser les chiffres de ce rapport avec un lien vers l'étude. Liste tirée de Wikidata (CC0).

Contact : hello@perimetry.cloud

`https://perimetry.cloud/fr/research/german-local-authorities/`