PERIMETRY RESEARCH

Security barometer of the German local authorities

How well do Germany's Landkreise, kreisfreie Städte and Länder protect their websites and e-mail? Passive measurements, compared with the French local authorities.

November 2026 edition

387
domains with a site of their own, graded

41.1%
enforce DMARC (quarantine or reject)

32.3%
get an A or a B

Perimetry Cloud
perimetry.cloud · Published 14 November 2026

About this report

Perimetry Research publishes studies of how well organisations protect their websites and e-mail, measured with the same passive checks as Perimetry Cloud. This edition covers 411 domains of Germany's Landkreise, kreisfreie Städte and Länder; 410 are active, and the 387 with a site of their own are graded. It names only the authorities that do well; every other figure is an aggregate, and the serious issues were reported privately to the authorities before publication. No e-mail is sent to these authorities: the study is published only.

Contents

01 Executive summary 3

02 Key findings 4

03 Grades 5

04 Check by check 6

05 By category 8

06 Domains without a site of their own 9

07 Compared with our other studies 10

08 The authorities that get it right 11

09 Serious issues 12

10 Recommendations 13

11 Methodology 14

12 About Perimetry 16

01

Executive summary

387
domains with a site of their own, graded

62
average score out of 100

41.1%
enforce DMARC (quarantine or reject)

32.3%
get an A or a B

Average score of the 387 graded domains: 62 out of 100; median 67.

1. 73.6% of the graded domains publish a DMARC policy and 41.1% enforce it (French local authorities: 32.8%; UK councils: 95.5%).
2. Websites: 96.4% have a valid certificate, 92% send visitors to HTTPS, 74.3% use HSTS for six months or more.
3. 15% of the graded domains are signed with DNSSEC; 12.4% publish a CAA record.
4. 23 active domains have no site of their own; 73.9% of them do not enforce DMARC.

02

Key findings

73.6% of the graded domains publish a DMARC policy and 41.1% enforce it (French local authorities: 32.8%; UK councils: 95.5%).

Websites: 96.4% have a valid certificate, 92% send visitors to HTTPS, 74.3% use HSTS for six months or more.

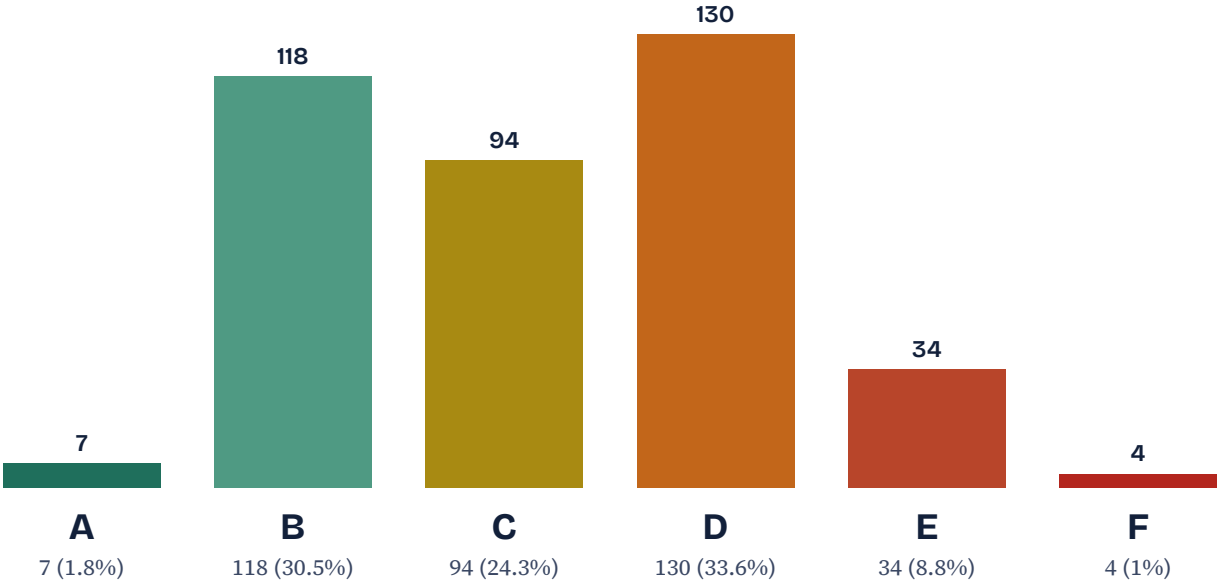
15% of the graded domains are signed with DNSSEC; 12.4% publish a CAA record.

23 active domains have no site of their own; 73.9% of them do not enforce DMARC.

03

Grades

Each domain with a site of its own gets a score: the share of the nine checks that it passes, among those that apply to it (the score of our other studies, without the check on the contact address, which the lists do not give). Grades: A from 90, B from 75, C from 60, D from 40, E from 20, F below.

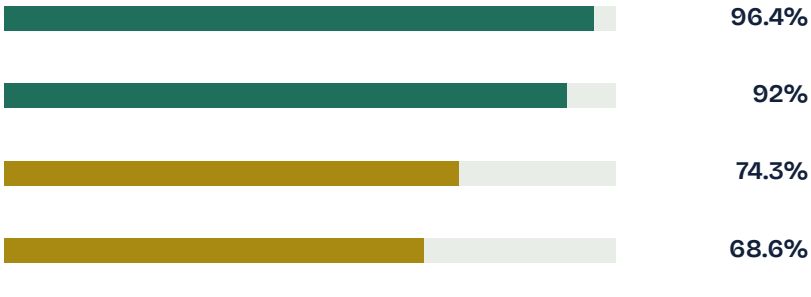


04

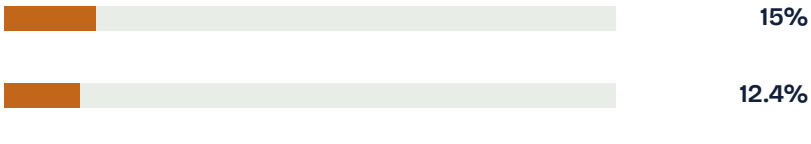
Check by check

Share of the graded domains that pass each check, among those it applies to.

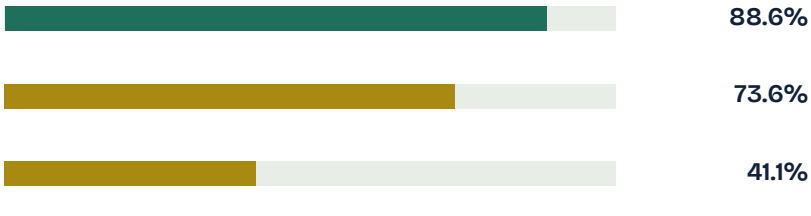
Website



DNS



E-mail



The nine checks	
Website · Valid HTTPS certificate	The site answers over HTTPS with a certificate that is in date, issued for its name, and trusted by browsers.
Website · HTTP sends visitors to HTTPS	Someone who types the address lands on the encrypted site, not on a page anyone on the network can read or alter.
Website · HSTS for six months or more	Browsers remember to use HTTPS only, so the first unencrypted request cannot be hijacked.
Website · Basic protective headers	X-Content-Type-Options: nosniff, and protection against being framed by another site (X-Frame-Options or CSP frame-ancestors).
DNS · DNSSEC	Answers about the domain are signed, so a resolver cannot be fed false addresses for the administration's site or mail.
DNS · CAA record	The domain names the certificate authorities allowed to issue certificates for it.
E-mail · Strict SPF	The domain lists the servers allowed to send its mail and asks receivers to reject or flag the others (-all or ~all).

The nine checks	
E-mail · DMARC record	The domain publishes a DMARC policy, the standard that ties SPF and DKIM to the visible sender.
E-mail · DMARC enforced	The policy is quarantine or reject: messages forged in the administration's name, to citizens for example, go to spam or are refused, not delivered.

05

By category

Categories with fewer than ten graded domains show no figures.

Group	Graded	Average	A or B	DMARC enforced	Median
Landkreise (rural districts)	274	62	31.8%	40.1%	67
Kreisfreie Städte (district-free cities)	100	63	31%	44%	67
Länder (federal states)	13	71	53.8%	38.5%	–

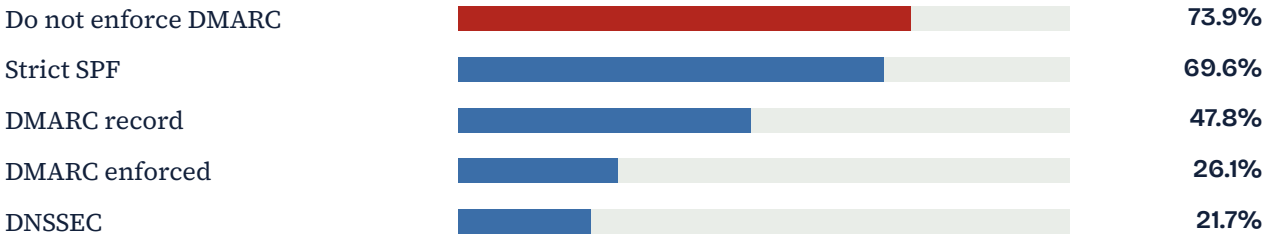
Average



06

Domains without a site of their own

23 active domains have no site of their own: 13 send visitors to another site, 10 are used for mail only. They can still be used to forge e-mail in the authority's name, and are judged on DNS and mail only.



Average score on DNS and mail only: 36 out of 100.

07

Compared with our other studies

The same checks in our other studies (latest editions): share of the graded domains that pass each one. The French local authorities count ten checks, the others nine.

	German authorities	UK councils	French authorities	French State
Average score	62	69	60	46
Valid HTTPS certificate	96.4%	98.1%	98.7%	63.8%
HTTP sends visitors to HTTPS	92%	85.5%	90.9%	77.3%
HSTS for six months or more	74.3%	57%	38.8%	33.3%
Basic protective headers	68.6%	74.3%	40.7%	51.9%
DNSSEC	15%	1.9%	25.9%	3.8%
CAA record	12.4%	11.4%	2.6%	18.5%
Strict SPF	88.6%	100%	97.1%	56.2%
DMARC record	73.6%	99.4%	77.8%	56.7%
DMARC enforced	41.1%	95.5%	32.8%	43.3%

08

The authorities that get it right

7 authorities pass every one of the nine checks and have no serious issue.

Authority	Category
Bayern	Länder (federal states)
Hamburg	Länder (federal states)
Landkreis Haßberge	Landkreise (rural districts)
Heilbronn	Kreisfreie Städte (district-free cities)
Ingolstadt	Kreisfreie Städte (district-free cities)
Kreis Plön	Landkreise (rural districts)
Landkreis Teltow-Fläming	Landkreise (rural districts)

09

Serious issues

One domain has a serious issue that could be used against it. It is not named in this report or anywhere else: the authority was told privately before publication.

Expired certificates	1

10

Recommendations

1 Enforce DMARC

Fewer than half do. A policy of quarantine, then reject, stops e-mail forged in the authority's name from reaching residents.

2 Turn on HSTS and the protective headers

HSTS makes browsers remember to use HTTPS only; two headers stop another page from framing the site and the browser from misreading its files.

3 Sign the domains with DNSSEC

Few authorities do; the .de registry supports it.

4 Check the address without "www"

Several expired certificates were found on the bare domain while the www site was fine: a visitor who types the short address gets a warning.

5 Watch it over time

Certificates expire, providers change, records get lost in a migration. A regular check catches it before residents do.

11

Methodology

Passive checks only

We read what any visitor or mail server can see: public DNS records, the domain registration (RDAP), the TLS certificate, one request for the home page over HTTP (its redirect is read, not followed), and the home page over HTTPS (following its redirects, as a browser would). Nothing else on the site is requested. When a domain publishes an MTA-STS policy, its policy file is read too, as mail servers do.

No port scanning, no subdomain discovery, no login attempts, no forms, no testing for vulnerabilities. The robot is slow on purpose and spreads its requests over several hours.

The robot

It identifies itself as PerimetryResearch/1.0 (+https://perimetry.cloud/research/methodology/). If you run a site it visited and would rather it did not, write to hello@perimetry.cloud and we will leave the domain out of the next editions.

The study of the German local authorities

Population: Germany's Landkreise, kreisfreie Städte and Länder, from Wikidata (CC0): each with its official key (AGS) and its official website. A list whose sizes stray from the official ones (294 Landkreise, about 107 kreisfreie Städte, 16 Länder) stops the run. Berlin and Hamburg count as Länder. Municipalities (Gemeinden) are left for a later study.

Publication only: no e-mail is ever sent to these authorities; a vulnerability found is reported privately to the authority, without any promotion, before publication. An authority can ask for its own result itself. Everything else follows the study of the French State, on nine checks; the comparison with the French local authorities uses those nine checks, the French study's tenth (a contact address on the authority's own domain) being left out.

Good performers only

We name the communes that do well (the honour roll and the best of each size band), never the ones that do badly, and never a commune with a serious issue, whatever its score. Everything else is published as aggregates: by size of commune and by département, where a département with fewer than ten graded communes shows no figures, so that none of them can be singled out.

Website platforms are graded on a sample of up to five communes' sites there: a check counts as passed when most of the sample passes it.

Serious issues are reported privately

Some findings could be used against a commune right away: a domain listed in the official directory that no longer exists (anyone could register it), a registration the registry is deleting, an expired certificate, an SPF record that lets anyone send mail in its name. These are never published. We tell the commune first, quietly, and count them in the study without naming anyone.

Limits

Each edition is a snapshot taken over a few hours. The directory can be out of date or wrong; we use it as published. DKIM keys are looked for on common selectors only, so they are not graded. A site behind a protection service may answer differently to a robot than to a visitor. Mail servers are not tested (STARTTLS needs port 25, which the study's infrastructure cannot reach).

12

About Perimetry

Perimetry is an open source tool that audits the outside of a domain the way anyone on the internet sees it: e-mail authentication, DNS, certificates, mail servers, websites. Perimetry Cloud is its hosted version, with continuous monitoring, alerts and reports, for organisations and the agencies that look after them.

Cite as: Perimetry Research, Security barometer of the German local authorities, November 2026. https://perimetry.cloud/research/german-local-authorities/

You may reuse the figures of this report with a link to the study. List from Wikidata (CC0).

Contact: hello@perimetry.cloud

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