



**PRIVACYScore.ORG**

**Ein Benchmarking-Portal zur Analyse von Webseiten  
auf Sicherheits- und Privatheitsprobleme**

**Pascal Wichmann**  
Universität Hamburg

**Dominik Herrmann**  
Universität Bamberg

mit Max Maaß (TU Darmstadt) und Henning Pridöhl (Uni Bamberg)



**PRIVACYScore.ORG**

**Pascal Wichmann**

Universität Hamburg

Bachelor-Student in Informatik

**Dominik Herrmann**

Universität Bamberg

Professor für Privacy & Security

# Motivation

# Wer weiß eigentlich, dass ich mich für Sozialhilfe interessiere?

The image shows a browser window with the URL [www.hamburg.de/mitte/hilfen-lebensunterhalt/](http://www.hamburg.de/mitte/hilfen-lebensunterhalt/). The page content includes a navigation bar with 'HAMBURGER', 'BESUCHER', 'POLITISCHES', and 'TOP-SERVICES'. Below this is a header for 'hamburg.de' and 'Bezirk Hamburg-Mitte'. The main content area features a large white box with a thinking emoji (🤔) and the text 'THE NEW NORMAL?'. A Privacy Badger notification is overlaid on the right side of the page, displaying a list of detected trackers and their status.

Tracker	Status
www.google-analytics.com	Blocked (Red)
de.ioam.de	Blocked (Red)
qs.ioam.de	Blocked (Red)
script.ioam.de	Allowed (Yellow)
collect-eu-central-1.tealiu...	Blocked (Red)
visitor-service.tealiumiq.com	Blocked (Red)

Buttons at the bottom of the Privacy Badger notification:

- Disable Privacy Badger for This Site
- Did Privacy Badger break this site? Let us know!
- Donate to EFF

Existierende Scanning-Dienste  
konzentrieren sich auf einzelne Seiten

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [youtube.com](#) > 216.58.212.142

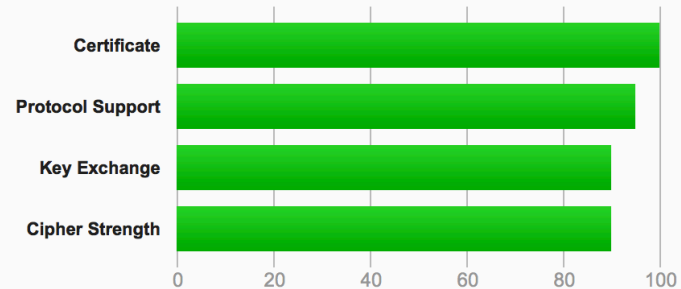
## SSL Report: [youtube.com](#) (216.58.212.142)

Assessed on: Wed, 01 Mar 2017 20:48:35 UTC | [Clear cache](#)

[Scan Another](#)

### Summary

#### Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. [MORE INFO »](#)

<https://www.ssllabs.com/ssltest/>

<https://observatory.mozilla.org/> – <https://securityheaders.io/> – <http://urlscan.io/>

# Results for **www.bundestag.de**

 [Check again](#)

🕒 2017-03-02 07:12:21

Input URL: <http://www.bundestag.de/>

Final URL: <http://www.bundestag.de/>



Insecure



Referrers leaked

2

Cookies

1

Third-party request

1

Third-party contacted

## Insecure connection

**www.bundestag.de** does **not** use HTTPS by default.

HTTPS encrypts nearly all information sent between a client and a web service. Properly configured, it guarantees three things:

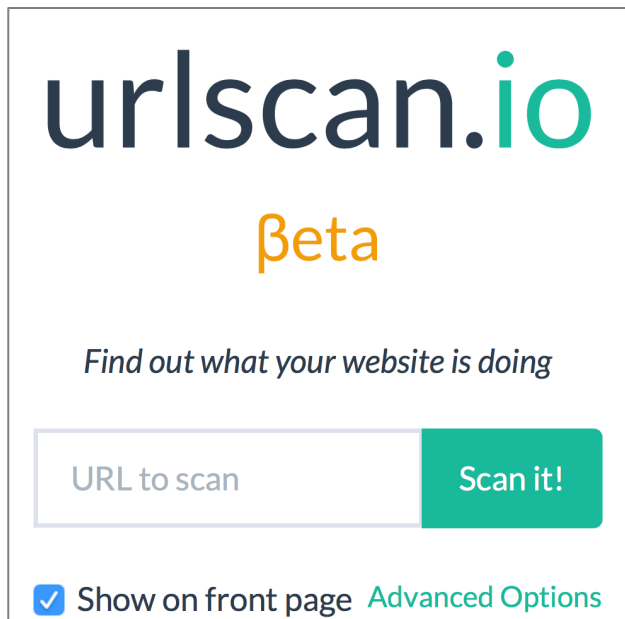
To enable HTTPS on a website, a **certificate** for the domain needs to be installed on the web server. To get a certificate that browsers will trust, you need one issued by a trusted certificate authority (otherwise a visitor's browser will show a warning).

<https://webbkoll.dataskydd.net/en/>

<https://www.sit.fraunhofer.de/de/track-your-tracker/> – <https://https.jetzt/> 7

## Existierende Scanning-Dienste ...

richten sich an  
Server-Betreiber



The screenshot shows the urlscan.io website. At the top, the logo "urlscan.io" is displayed in a dark blue font, with "Beta" written below it in orange. Below the logo, the text "Find out what your website is doing" is centered. There is a search input field with the placeholder text "URL to scan" and a green "Scan it!" button. At the bottom left, there is a checked checkbox labeled "Show on front page" and a link for "Advanced Options".

verwenden ein vordefiniertes  
Bewertungsschema

Description	Modifier
HSTS preloaded	5
HSTS header max age $\geq$ 6 months	0
HSTS header max age < six months	-10
HSTS header not implemented	-20
HSTS header cannot be set, as site contains an invalid certificate chain	-20

<https://github.com/mozilla/http-observatory/blob/master/httpobs/docs/scoring.md>



## PrivacyScore hat anderen Fokus

Ziel: **öffentliche Benchmarks**, um **Anreize** für Betreiber schaffen, den Schutz der Privatsphäre zu verbessern.

Jeder kann (annotierte) **Listen** von Webseiten hochladen und (bald™) das **Ranking beeinflussen**.

Open Source (GPLv3+) und Open Data

**Out of scope:** Pentesting, SQLI, XSS, ...

### NUTZERDEFINIERTER ATTRIBUTE

*Schneiden Städte in Bayern besser ab als in Hamburg?*

*Korreliert Größe eines Krankenhauses mit Rang seiner Webseite?*

# Ausgewählte Listen

## News Sites Popular in Germany

### Top 100 German Banks

### German OWASP Day 2017 Sponsors

#	URL		Type	NoTrack	E
1	<a href="http://www.sicsec.de/">http://www.sicsec.de/</a>	/ 2017-11-14 @ 08:05:28	Standard		
2	<a href="http://www.psi.de/">http://www.psi.de/</a>	(1 failure) / 2017-11-14 @ 08:07:12	Standard	< ? >	
3	<a href="http://www.secuvera.de/">http://www.secuvera.de/</a>	(1 failure) / 2017-11-14 @ 08:10:34	Gold		
4	<a href="http://www.contextis.com/">http://www.contextis.com/</a>	(1 failure) / 2017-11-14 @ 08:06:09	Standard		
5	<a href="http://www.nttsecurity.com/">http://www.nttsecurity.com/</a>	/ 2017-11-14 @ 08:05:38	Gold		
6	<a href="http://www.schutzwerk.com/">http://www.schutzwerk.com/</a>	/ 2017-11-14 @ 08:07:12	Standard		
7	<a href="http://www.mgm-sp.com/">http://www.mgm-sp.com/</a>	/ 2017-11-14 @ 07:38:05	Standard		

# Check-Gruppen

## No Tracking

Third Parties  
Bekannte Tracker  
Server-Standorte

## Encryption to Website

HTTPS/STARTTLS verfügbar?  
Zertifikat: validity / key size  
Unsichere Protokollversionen: SSLv3...  
Bekannte Schwachstellen: Heartbleed...

## Encryption to Mailserver

## Protection Against Other Attacks

Informationsleck  
Referer-Policy  
Security-Header

HSTS

HPKP

Automatische  
Umleitung zu  
HTTPS

# Ranking und Detail-Ergebnisse



PRIVACYScore BETA

Sortierung ändern

# Large German Cities

Tags: de public cities

Author: Dominik Herrmann

This list contains the websites of the Top 20 German Cities in terms of population count according to Wikipedia.

## Results Overview

This list contains 20 websites (with 1 scan error).

0 passed all checks

5 failed one or more checks

0 failed all tests in at least one group

15 failed at least one critical check

0 could not be judged due to missing data

Take this with a grain of salt! Some of our checks may report wrong results. BETA

» Configure sorting and grouping

Re-scan all sites now










NO SCANS RUNNING

Download List as CSV







# Öffentliches Ranking

		NoTrack	EncWeb	Attacks	EncMail	Rating
1	<a href="http://dortmund.de/">http://dortmund.de/</a>	✓	✗	!	!	✗
2	<a href="http://nuernberg.de/">http://nuernberg.de/</a>	✓	✗	!	!	✗
3	<a href="http://muenster.de/">http://muenster.de/</a>	✓	✗	!	✗	✗
4	<a href="http://bonn.de/">http://bonn.de/</a>	!	< ? >	!	!	!
5	<a href="http://wuppertal.de/">http://wuppertal.de/</a>	!	!	!	!	!
6	<a href="http://essen.de/">http://essen.de/</a>	!	!	!	!	!
7	<a href="http://bochum.de/">http://bochum.de/</a>	!	!	!	!	!
8	<a href="http://hannover.de/">http://hannover.de/</a>	!	!	!	!	!
9	<a href="http://berlin.de/">http://berlin.de/</a>	!	!	!	✗	✗
		!	!	!	✗	✗
		!	✗	!	?	✗
		!	✗	!	?	✗
13	<a href="http://frankfurt.de/">http://frankfurt.de/</a>	!	✗	!	!	✗
14	<a href="http://bielefeld.de/">http://bielefeld.de/</a>	!	✗	!	!	✗
15	<a href="http://hamburg.de/">http://hamburg.de/</a>	!	✗	!	!	✗
16	<a href="http://dresden.de/">http://dresden.de/</a>	!	✗	!	!	✗
17	<a href="http://stadt-koeln.de/">http://stadt-koeln.de/</a>	!	✗	!	!	✗
18	<a href="http://leipzig.de/">http://leipzig.de/</a>	!	✗	!	!	✗
19	<a href="http://stuttgart.de/">http://stuttgart.de/</a>	!	✗	!	!	✗
20	<a href="http://muenchen.de/">http://muenchen.de/</a>	!	✗	!	!	✗

## NoTrack: No Tracking by Website and Third Parties

	<b>Check if 3rd party embeds are being used</b> The site does not use any third parties.	reliable	▼
	<b>Check if embedded 3rd parties are known trackers</b> The site does not use known tracking or advertising services.	reliable	▼
	<b>Determine how many cookies the website sets</b> The site sets 1 short-term, 1 long-term, and 0 Flash cookies.	reliable	▼
	<b>Determine how many cookies are set by third parties</b> No one else is setting any cookies.	reliable	▼
	<b>Check if Google Analytics is being used</b> The site does not use Google Analytics.	reliable	▼
	<b>Check if Google Analytics has privacy extension enabled</b> Not checking as the site does not use Google Analytics.	reliable	▼
	<b>Check whether web server is located in EU</b> All web servers are located in Germany.		▼
	<b>Check whether mail server is located in EU</b> All mail servers are located in Germany.		▼
	<b>Check whether web and mail servers in same country</b> The geo-location(s) of the web and mail server(s) are identical.	unreliable	▼

## Attacks: Protection Against Various Attacks

	<b>Check for unintentional information leaks</b> The site does not disclose internal system information.	unreliable	▼
	<b>Check for presence of Content Security Policy</b> The site does not set a Content-Security-Policy (CSP) header.	shallow	▼
	<b>Check for presence of X-Frame-Options</b> The site does not set a X-Frame-Options (XFO) header.	unreliable	▼
	<b>Check for secure XSS Protection</b> The site does not set a X-XSS-Protection header.	unreliable	▼
	<b>Check for secure X-Content-Type-Options</b> The site does not set a X-Content-Type-Options header.	unreliable	▼
	<b>Check for privacy-friendly Referrer Policy</b> The site does not set a referrer-policy header.	unreliable	▲

## Detail-Ergebnisse

vents the browser from disclosing the URL of the . Without a referrer policy most browsers send a content is retrieved from third parties or when you king on a link. This may disclose sensitive informa-

**Conditions for passing:** Referrer-Policy header is present. Referrer-Policy is set to "no-referrer" (which is the only recommended policy recommended by [dataskydd.net](https://dataskydd.net) in their Webbkoll scan service).

**Reliability:** unreliable. At the moment we only check for this header in the response that belongs to the first request for the final URL (after following potential redirects to other HTTP/HTTPS URLs).

**Potential scan errors:** We may miss security problems on sites that redirect multiple times. We may also miss security problems on sites that issue multi-

# Prüfung auf typische Informationslecks

*phpinfo.php*

*test.php*

*backup.sql*

*server-info*

*server-status*

*.git*

*.svn*

*server.key*

*<domain>.key*

...

PHP Version 5.5.9-1ubuntu4.14



*5.5.9-1ubuntu4.22  
is the current version*



System

Linux SMP Wed Jan 20 10:50:59 UTC 2016 i686

Build Date

Oct 20 2015 07:07:00

Server API

Apache 2.0 Handler

Virtual  
Directory  
Support

disabled

Configuration  
File (php.ini)  
Path

/etc/php5/apache2

Loaded  
Configuration  
File

/etc/php5/apache2/php.ini

<http://www.zensiert.bg/phpinfo.php>

*phpinfo.php*

*test.php*

*backup.sql*

*server-info*

*server-status*

*.git*

*.svn*

*server.key*

*<domain>.key*

...

## Erste ernstzunehmende Beschwerde im November 2017.

### Rechtliche Zulässigkeit

Dürfen wir Webseiten ohne Zustimmung scannen?

Siehe [arxiv.org/abs/1705.08889](https://arxiv.org/abs/1705.08889) (GI INFORMATIK 2017)

**TL;DR: Betrieb in Deutschland grundsätzlich erlaubt**

### Ethische Abwägungen

PrivacyScore ist ein Dual-Use-Tool.

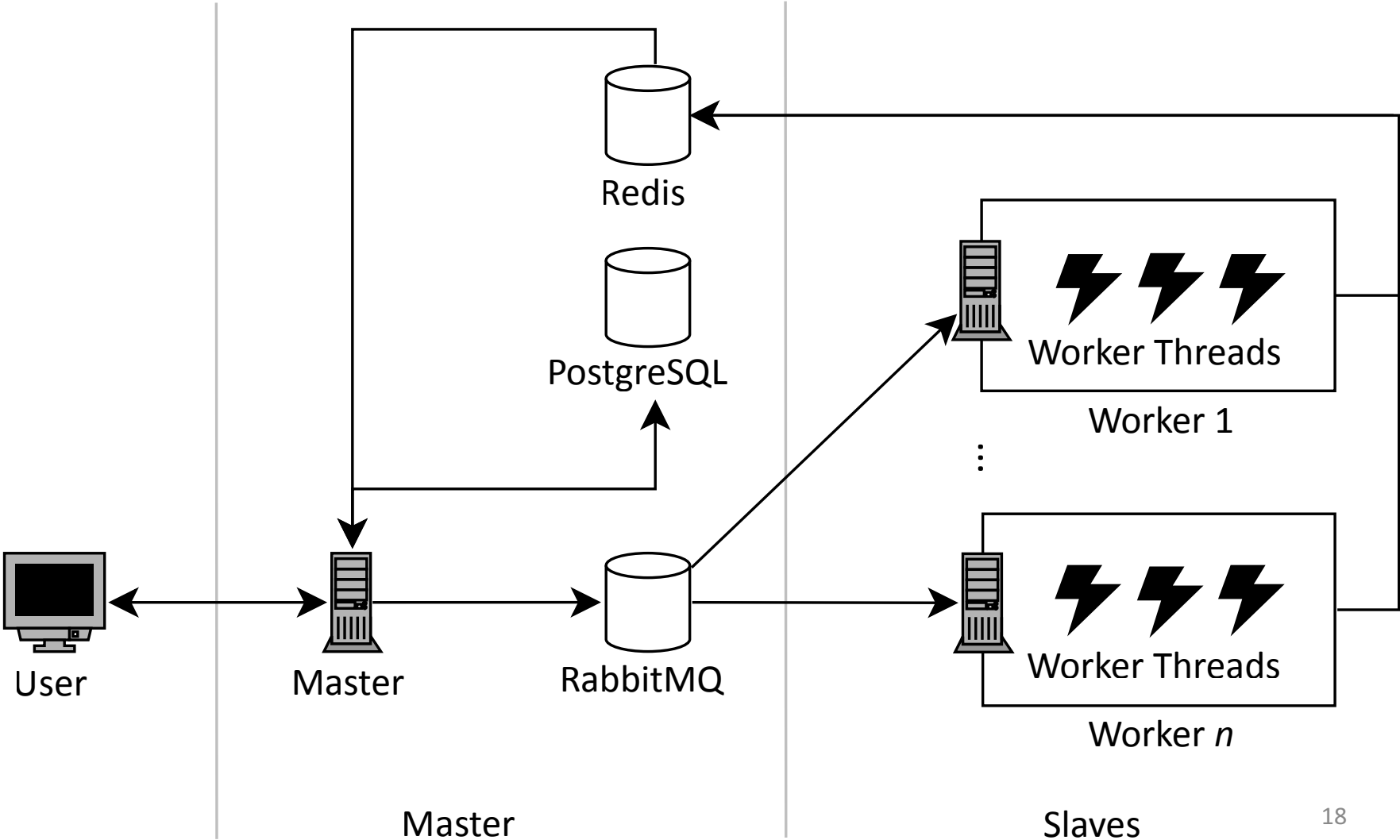
- nicht alle Ergebnisse **leicht zugänglich**
- **Rate-Limiting** als Schutz vor DoS
- **Blacklisting** auf Wunsch



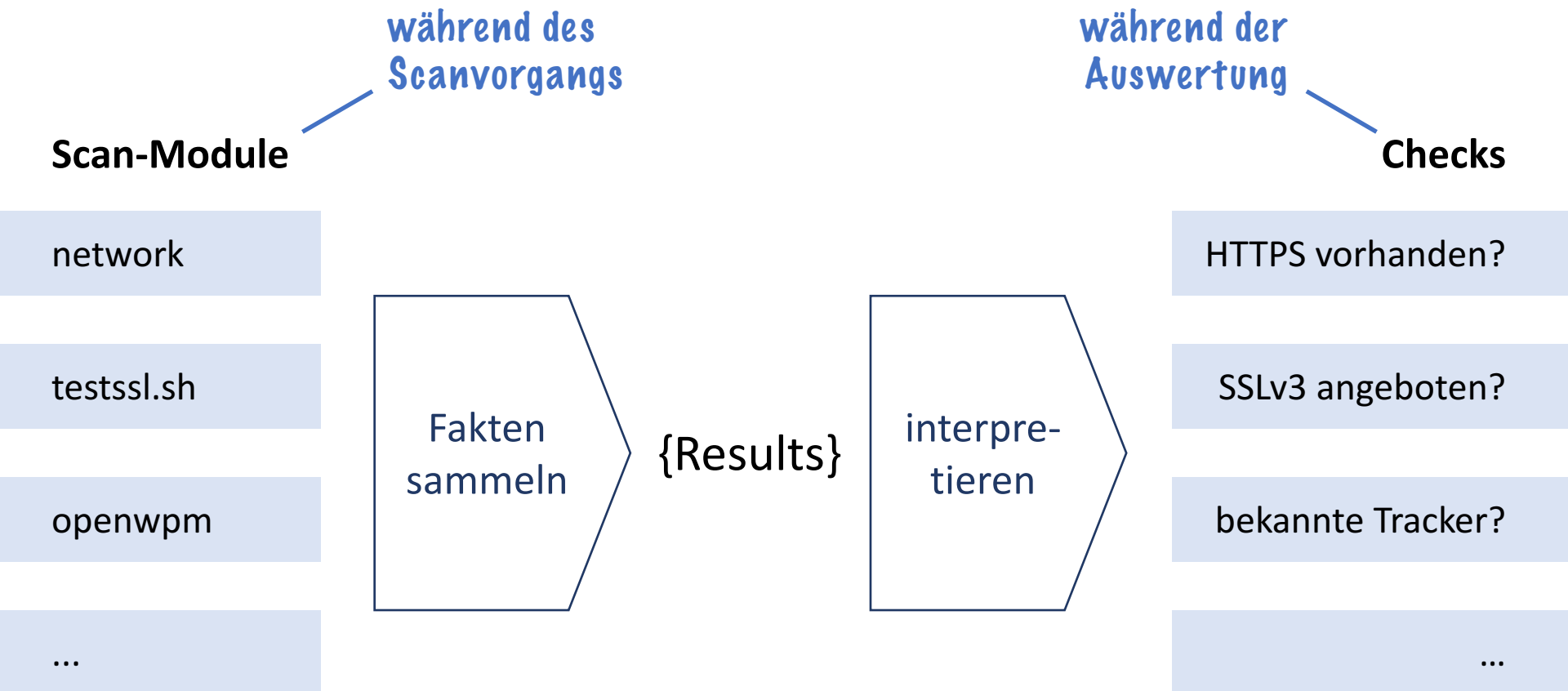
# Technische Umsetzung

# Verteilte Infrastruktur mit virtuellen Maschinen

(derzeit ca. 30 VMs)



# Entkopplung von Scan-Modulen und Checks



# Statistiken

# Ausgewählte Statistiken (November 2017)

leider noch nicht öffentlich



## Deutsche Kommunen

	Gesamt		Alexa Top 500 82 %		Deutsche Kommunen
<b>Anzahl Seiten</b>	19.794				8.466
Anzahl Scans	150.872				70.285
<b>HTTPS verfügbar</b>	5.428	27 %		<b>19 %</b>	1.636
mit Umleitung	4.564	23 %		<b>19 %</b>	1.636
veraltetes SSL: v2/v3	381	2 %		<b>1 %</b>	106
<b>Informationslecks</b>	585	3,0 %		<b>2,7 %</b>	230
Status/Debuginfo	503	2,5 %		<b>2,0 %</b>	174
Repositories (git/svn)	87	0,4 %		0,0 %	7
Datenbank-Dumps	17	0,0 %		0,0 %	8
Private-Keys	2	0,0 %		0,0 %	0
<b>Anz. Cookies (Mittelwert)</b>	4,5				<b>1,6</b>
für Third-Party-Tracking	2,0				<b>0,3</b>

# Wie verbreitet ist Tracking auf Seiten von Kommunen? (November 2017)

Betrieb  
durch  
Media-  
agentur

Top 20 Cities	Known Trackers	Third Party Servers	Third Party Cookies
● Hamburg	40	81	49
● Berlin	22	37	17
Leipzig	6	10	5
● München	5	11	3
● Bremen	4	13	3
● Dresden	3	8	4
Düsseldorf	2	3	3
● Hannover	2	3	1
Köln	2	3	1
● Stuttgart	1	7	2
● Bielefeld	1	2	0
● Bonn	1	1	0
Duisburg	0	4	0
Essen	0	2	1
Wuppertal	0	2	0
Münster	0	0	0
Dortmund	0	0	0
Nürnberg	0	0	0
Bochum	0	0	0
Frankfurt	0	0	0

**Check if embedded 3rd parties are known trackers** reliable

The site is using 40 known tracking- or advertising companies. ▼

adnxs.com googlesyndication.com  
mxcdn.net adsafeprotected.com  
tealiumiq.com youtube.com  
mookie1.com adform.net criteo.com  
adtech.de google-analytics.com  
gstatic.com truste.com oms.eu  
tiqcdn.com adnet.de mathtag.com  
refinedads.com stickyadstv.com  
googleapis.com smartadserver.com  
doubleclick.net theadex.com m6r.eu  
mpnrs.com adition.com fqtag.com  
2mdn.net intelliad.de ioam.de  
meetrics.net turn.com fonts.com  
cloudfront.net mp-success.com  
sascdn.com adscale.de nuggad.net  
content-recommendation.net [...]

# Änderungen im Zeitverlauf nachvollziehbar machen (in Entwicklung)



## NO. OF KNOWN TRACKERS

	14 Aug	27 Oct	Delta
Piraten	0	0	-
Linke	0	1	!!
Die PARTEI	0	0	-
CDU	1	1	-
Grüne	1	2	!!
SPD	1	0	😊
FDP	2	2	-
AFD	4	4	-
CSU	5	38	!!

Alle URLs werden (mehr oder weniger) regelmäßig erneut überprüft.





# PrivacyScore.org: Ein Benchmarking-Portal zur Analyse von Webseiten auf Sicherheits- und Privatheitsprobleme

BETA

**TODOs** Listen editieren, private Listen, User-Management, ...

Ranking-Templates, benutzbarere Auswertungen

OCSP, OCSP-Stapling, Browser-Fingerprinting,  
Inferieren von Versionsnummern

Abuse-Prozess, Containment, ...

**Was fehlt**

**OWASP-Ranking-Schema**

**Eure Ideen?**

**Eure Listen!**