

Responsible Disclosure at Scale

Max Maass

@hacksilon@infosec.exchange

„Max Maass klingt wie ein ausgedachter Name“ - Webseitenbetreiber

- ▶ Aktuell bei iteratec als Security Specialist
 - ▶ Security-Beratung, Threat Modeling, Pentesting, ...
- ▶ Vorher an der TU Darmstadt (Secure Mobile Networking Lab)
 - ▶ Promotionsthema: Wie kriegen wir das Web gefixt?
- ▶ Dieser Talk: Zusammenfassung von zwei Studien
 - ▶ „Effective Notification Campaigns for the Web“
USENIX Security 2021. Maass, Stöver, Pridöhl, Bretthauer, Herrmann, Hollick, Spiecker.
 - ▶ „Snail Mail Beats Email Any Day“
ARES 2021. Maass, Clement, Hollick.

iteratec



TECHNISCHE
UNIVERSITÄT
DARMSTADT



Privacy and Trust
for Mobile Users

Forschungsfrage

- ▶ Gegeben einer Liste an verwundbaren Systemen, wie bekomme ich möglichst viele Betreiber:innen dazu, ihre Systeme zu reparieren?
 - ▶ Wie sende ich die Benachrichtigungen? Von welchem Absender?
 - ▶ Wie formuliere ich sie?
 - ▶ Was sollte ich ansonsten beachten?

Methodik



- Information leaks
- Datenschutzprobleme

- PrivacyScore.org
- Automatische Crawls

- Email
- Briefe



Ja, Briefe.

Wer fragt...

...kriegt Antworten

- ▶ Viel Dankbarkeit
 - ▶ Teilweise auch zu viel wenn man an einer Uni ist
- ▶ Viele Rückfragen
 - ▶ Self-Service Scan Tool ist hilfreich
- ▶ Misstrauen
 - ▶ Willst du mir was verkaufen? Willst du mich abmahnen?
- ▶ Juristische Drohungen wg. Ungefragten Scans
 - ▶ Zusammenarbeit mit Jurist*innen sehr hilfreich

Internationales Zentrum für Menschenrecht

Bielfeldtweg 26. [DE-21682] STADE

völkerrechtliche Verträge:

Art. 125 genfer Konvention 0.518.42, Anhang III

Art. 142 genfer Konvention 0.518.51, Anhang IV

Art. 1 genfer Konvention 0.518.42 und 0.518.51

Die Hohen Vertragsparteien verpflichten sich, das vorliegende Abkommen unter allen Umständen einzuhalten und seine Einhaltung durchzusetzen.

Art. 25 GG: portofreie **KRIEGSOPFER** - und **ZWANGSINTERNIERTENPOST**


PORTOFREI



Im Entwurf ihrer Katalogkonservenwerbepost, -im Zusammenhang mit der Datenschutzgrundverordnung-, behauptet sie, daß sie Unsere Tätigkeit im weltweiten Internet untersucht haben. Wir haben ihnen weder einen Auftrag erteilt noch sie um ihre Meinung gefragt, da Wir vorstaatlich im originären Recht sind, denn das Zentrum ist eine nichtwirtschaftliche Nichtregierungsorganisationen mit besonderen Vorrechten.

Sie dürfen keine Spionage- und Sabotagefunktionen ausüben, und sie haben im Bereich Recht keine Erkenntnisse. Das Internationale Zentrum für Menschenrecht ist keine Demokratieeinrichtung, und die Seite wurde mit WebSite X5 erstellt. Wenden sie sich an diese Firma mit ihrem Problem. Sie haben ein Problem.

Die Datenschutzgrundverordnung ist für Unsere Einrichtungen im öffentlichen Recht nicht gültig. Die Immunitäten sind vertraglich im Völkerrecht geregelt, so daß Wir ihren Angriff als Verbrechen der Aggression für Streit- und Feindhandlungen mit dem Ziel eines bewaffneten Konfliktes einordnen.

e Post 

REIBEN
(à l'adresse)



EIGENHÄNDIG
(À remettre en
main propre)

ENTREPRISE
(à l'adresse)



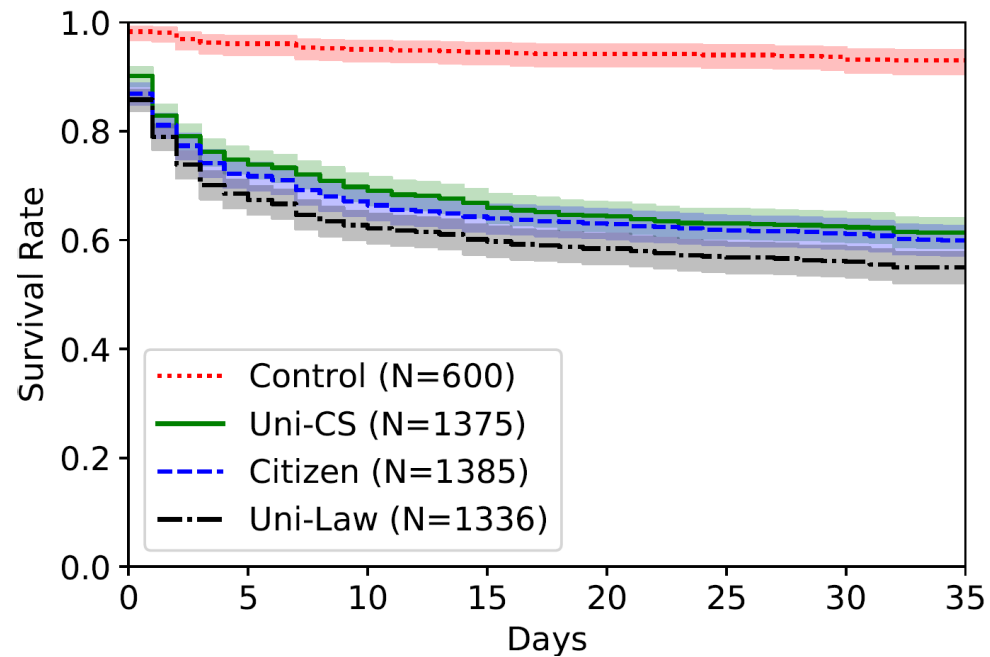
RÜCKSCHEIN
(Avis de réception)

67 172 026 2DE



Was ist Effektiv?

- ▶ Briefe sind effektiver als Emails, aber kosten Geld und Aufwand
- ▶ Der richtige Text in der Benachrichtigung macht einen großen Unterschied
- ▶ Auch der Absender kann einen Unterschied machen, aber kleiner als man denkt



"Kleine" Unterschiede?

Medium	Sender	Framing	Owners	Sites	Pre-rem. [%]	Post-rem. [%]	End of study [%]
EMAIL	CITIZEN	PRIVACY	146	163	79.8±7.5	80.7±8.7	63.5±8.4
		GDPR	149	153	63.8±8.2	77.8±10.1	49.0±8.2
		GDPR+FINE	148	159	64.3±8.3	74.1±10.3	48.8±8.3
	UNI-CS	PRIVACY	146	166	82.0±7.5	78.7±9.0	66.1±8.3
		GDPR	149	152	62.4±8.3	74.7±10.8	47.0±8.2
		GDPR+FINE	145	147	61.0±8.5	63.4±11.4	39.3±7.9
	UNI-LAW	PRIVACY	147	149	65.6±8.3	88.1±9.1	55.6±8.4
		GDPR	144	147	65.6±8.3	78.8±10.7	53.1±8.5
		GDPR+FINE	147	149	52.3±8.3	67.6±12.5	35.4±7.7
LETTER	CITIZEN	PRIVACY	294	308	69.2±5.6	70.6±7.1	52.9±5.9
		GDPR	294	304	50.5±5.8	60.9±8.8	33.0±5.4
		GDPR+FINE	292	298	48.4±5.8	59.0±8.9	30.9±5.4
	UNI-CS	PRIVACY	294	302	68.5±5.6	76.7±6.7	55.8±5.9
		GDPR	292	305	54.6±5.9	65.0±8.7	39.8±5.6
		GDPR+FINE	293	303	51.9±5.8	64.4±8.5	35.4±5.5
	UNI-LAW	PRIVACY	293	293	62.5±5.8	70.4±7.5†	44.7±5.8†
		GDPR	288	294	55.6±5.9	68.5±8.2†	41.3±5.7†
		GDPR+FINE	293	304	39.4±5.6	54.7±10.0	23.7±5.0
All notified			3954	4096	58.8±1.6	70.3±2.0†	43.4±1.6†
CONTROL			585	600	93.0±2.4	97.6±1.7	90.8±2.6



Ungeplante Weiterverwendung



Universität Bamberg

Fakultät Wirtschaftsinformatik und Angewandte Informatik

Lehrstuhl Privatsphäre und Sicherheit in Informationssystemen

Überprüfen Sie Ihre Google-Analytics-Konfiguration

Mit unserem Dienst „**Check Google Analytics**“, den wir hier kostenlos zur Verfügung stellen, können Sie jederzeit überprüfen, ob Sie die IP-Anonymisierung auf Ihren Webseiten korrekt einsetzen. Wir hoffen, dass unser Dienst dabei hilft, die Verbreitung der IP-Anonymisierung zu steigern.

[Datenschutzhinweis](#)

Google-Analytics-Prüfung für „https://nytimes.com“

Die Angaben auf dieser Seite wurden am 08.04.2021 um 09:28 Uhr erhoben. Nach möglichen Weiterleitungen wurde final die folgende URL geprüft: „<https://www.nytimes.com/>“.

Zusammenfassung

Diese Seite nutzt Google Analytics ohne IP-Anonymisierung.

Hinweise dazu, wie das Problem behoben werden kann, finden Sie auf unserer [Howto-Seite](#).

Anfragen an Google Analytics

... **mit** IP-Anonymisierung: **0**

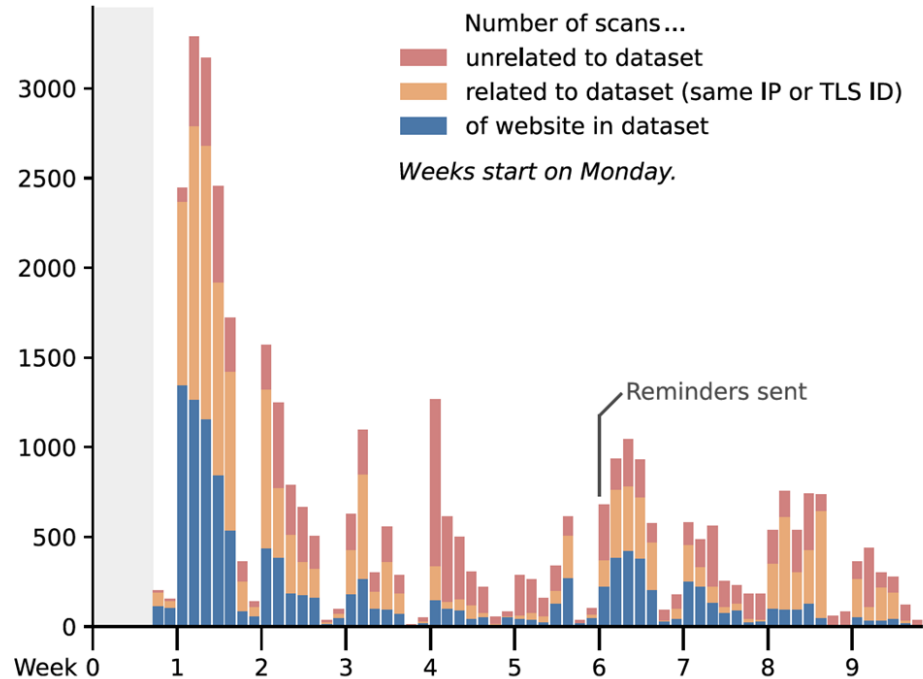
... **ohne** IP-Anonymisierung: **3**

Tracker

Seitenbetreiber können mehrere Google-Analytics-Tracker einbinden, um unterschiedliche Benutzeraktionen auf der Webseite getrennt zu erfassen. Die folgenden Tracker sind eingebunden.

Name	Tracking ID	Ursprung	Objektname	IP-Anonymisierung
gtm164	UA-58630905-2	https://www.nytimes.com	ga	× NEIN
gtm459	UA-58630905-2	https://www.nytimes.com	ga	× NEIN
gtm698	UA-58630905-2	https://www.nytimes.com	ga	× NEIN

Ungeplante Weiterverwendung



KOSTENLOSER GOOGLE ANALYTICS CHECK DER UNI BAMBERG

Viele Webseiten nutzen den für sie kostenlosen Analysedienst Google Analytics. Google nutzt diese Daten jedoch auch für deren Dienste und steht im Verdacht diese auch an Dritte weiterzuverkaufen. Für eine Nutzung von Google Analytics ist eine Anonymisierung der IP verpflichtend (letzte Zahl wird entfernt). Dies kann jeder nun über eine Abfrage an der Uni Bamberg testen:

<https://checkgoogleanalytics.psi.uni-bamberg.de/>

Posted in Allgemein, Datenschutz, EU-Recht, Recht, Software and tagged Datenschutz, Google on 23. Juli 2019 by Raphael.

DSGVO konformes Web-Tracking mit Google Analytics - ...

mittwald.de › blog › webentwicklung-design › dsgvo-konformes-web-tracking
Jun 3, 2018 ... <https://checkgoogleanalytics.psi.uni-bamberg.de/>. Antworten. Jan am 11.12.2019 - 16:41. Leider geht das Fazit völlig an geltendem Recht vorbei ...

Anonymisierte IP für Google Analytics in Shopify

webservicexxl.de › blog › anonymisierte-ip-fuer-google-analytics-in-shopify
Aug 9, 2019 Über https://checkgoogleanalytics.psi.uni-bamberg.de kann man einfacher prüfen ob die IP anonymisiert ist. Twitter · LinkedIn · Facebook.

Jeder (!) kann Google Analytics ohne anonymizeIP abmahnen

ra-plutte.de › jeder-kann-website-mit-google-analytics-ohne-anonymizeip-abmahnen
Jun 26, 2019 26.06.2019 ... <https://checkgoogleanalytics.psi.uni-bamberg.de/>. Antworten. Schreibe einen Kommentar. Antworten abbrechen. Hinweis: Gesetzes- und ...

Was soll ich tun?

- ▶ Problematik leicht verständlich und aus Perspektive der Betreiber erläutern
- ▶ Klarstellen, dass kein kommerzielles oder jur. Interesse verfolgt wird
- ▶ Self-Service Tool bereitstellen
- ▶ Am besten: Jurist*innen kennen, um Antworten einordnen zu können

Danke, und Lesestoff

- ▶ Vielen Dank für eure Aufmerksamkeit!
- ▶ Volle Papers:
 - ▶ „Effective Notification Campaigns for the Web“
USENIX Security 2021. Maass, Stöver, Pridöhl, Bretthauer, Herrmann, Hollick, Spiecker.
<https://www.usenix.org/system/files/sec21-maass.pdf>
 - ▶ „Snail Mail Beats Email Any Day“
ARES 2021. Maass, Clement, Hollick.
<https://arxiv.org/pdf/2106.08024>
 - ▶ „How Website Owners Face Privacy Issues“
PETS 2023. Stöver, Gerber, Pridöhl, Maass, Bretthauer, Spiecker, Hollick, Herrmann
<https://petsymposium.org/popets/2023/popets-2023-0059.pdf>
- ▶ Kontakt zu mir: max.maass@iteratec.com oder @hacksilon@infosec.exchange