

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

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)



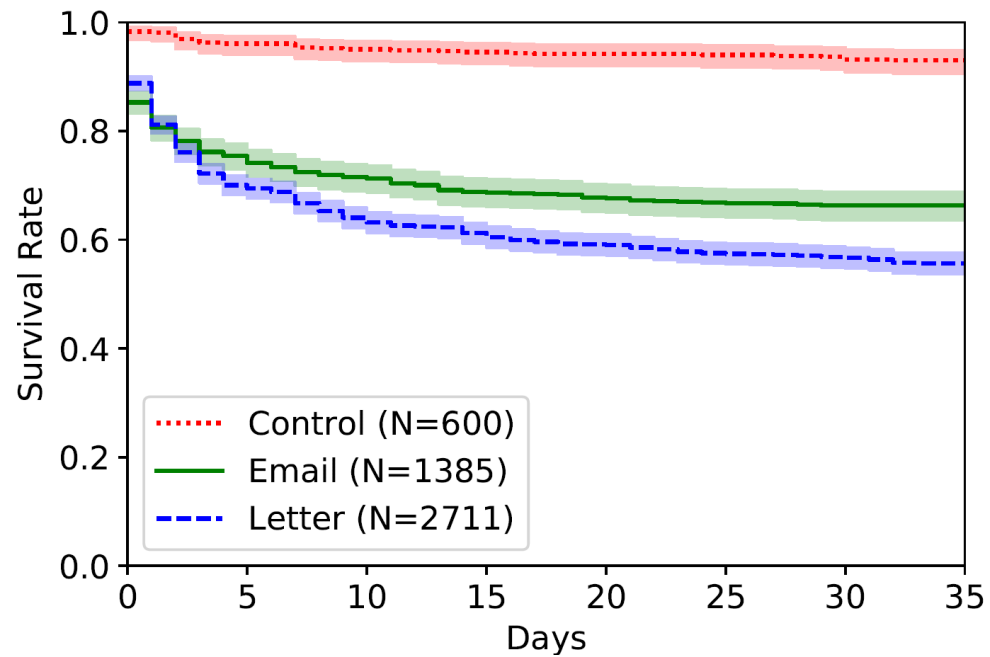
RÜCKSCHEIN
(Avis de réception)

67 172 026 2DE



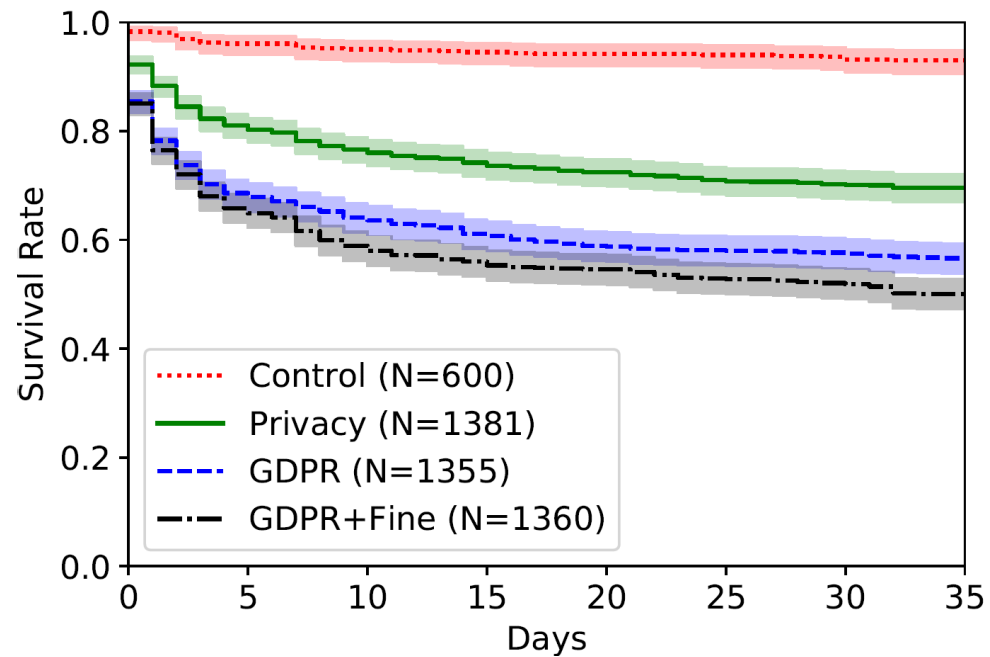
Was ist Effektiv?

- ▶ Briefe sind effektiver als Emails, aber kosten Geld und Aufwand



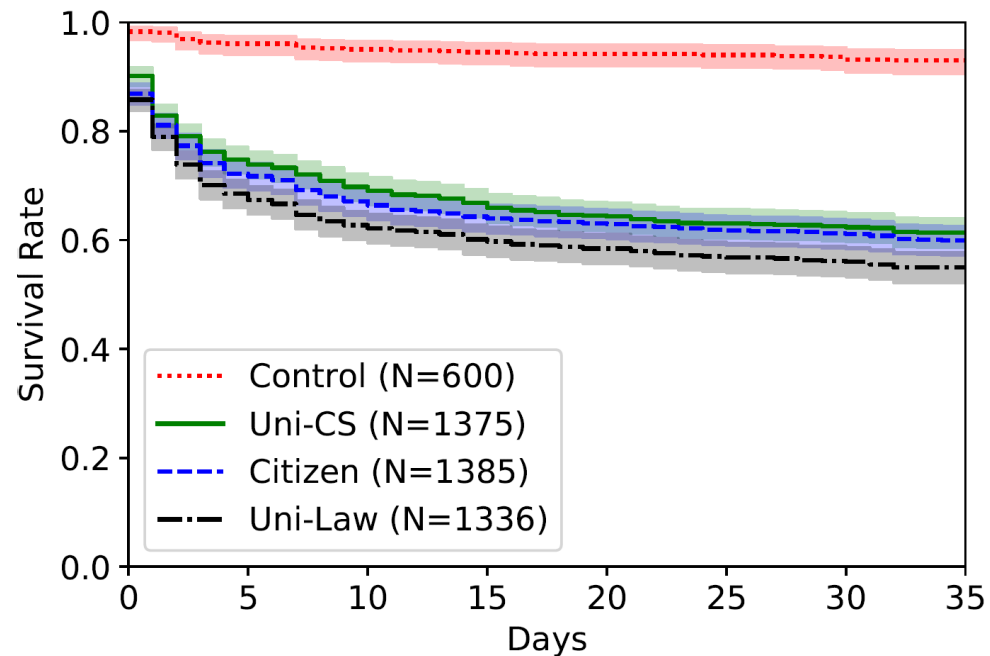
Was ist Effektiv?

- ▶ Briefe sind effektiver als Emails, aber kosten Geld und Aufwand
- ▶ Der richtige Text in der Benachrichtigung macht einen großen Unterschied



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



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>