



Kompetenzgruppe
E-Commerce
Zertifikate und
Regulierung im
Online-Handel
16. März 2015

WIR GESTALTEN
DAS INTERNET.



Certified Senders Alliance – ein Service von eco

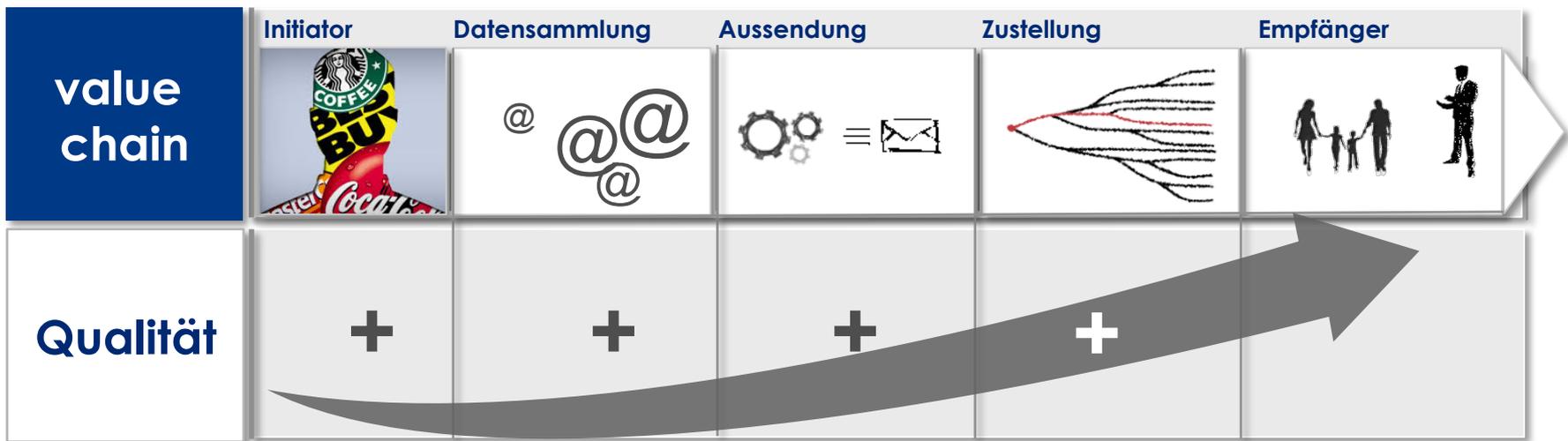
Berlin, 16. März 2015

Rosa Hafezi, Legal Consulting & Certification
Alexander Zeh, Engineering Manager

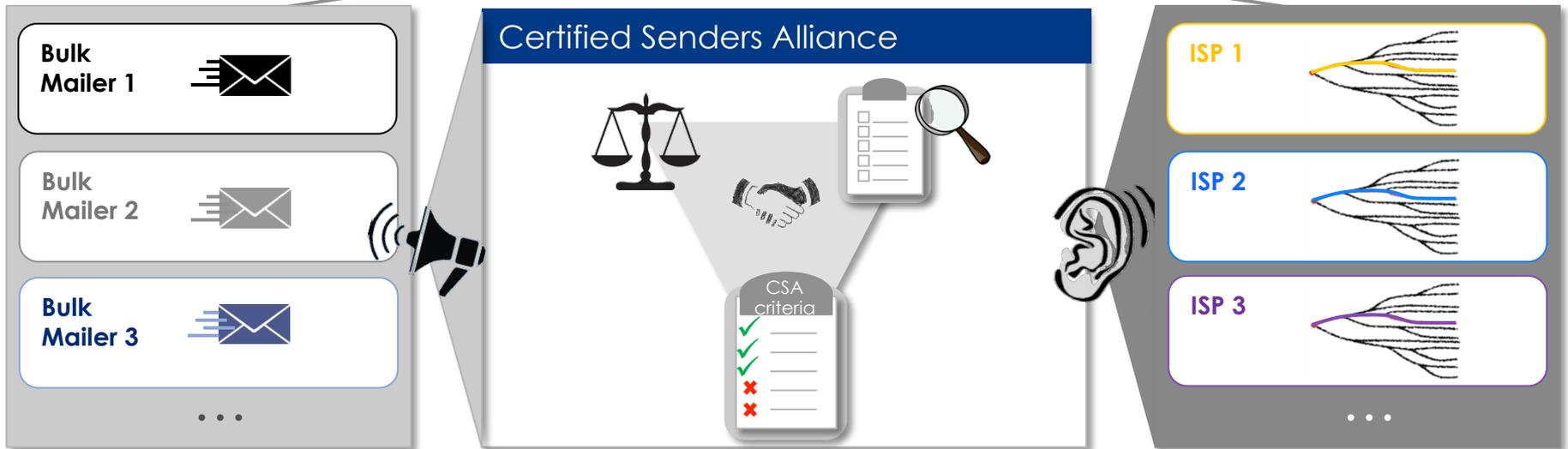
Agenda

- ✓ *CSA Mission und Tätigkeit*
- ✓ Rechtliche und technische Qualitätsstandards
- ✓ Was bringt die Zukunft?

Qualität im E-Mail Marketing betrifft alle Beteiligten im gesamten Prozess



Die CSA ist ein Moderator zwischen Versendern und ISPs



Vorteile durch die CSA für Versender und ISPs




CSA zertifizierte Versender:

- . Aktuellste Standards
- . Whitelisting bei CSA ISP Partnern

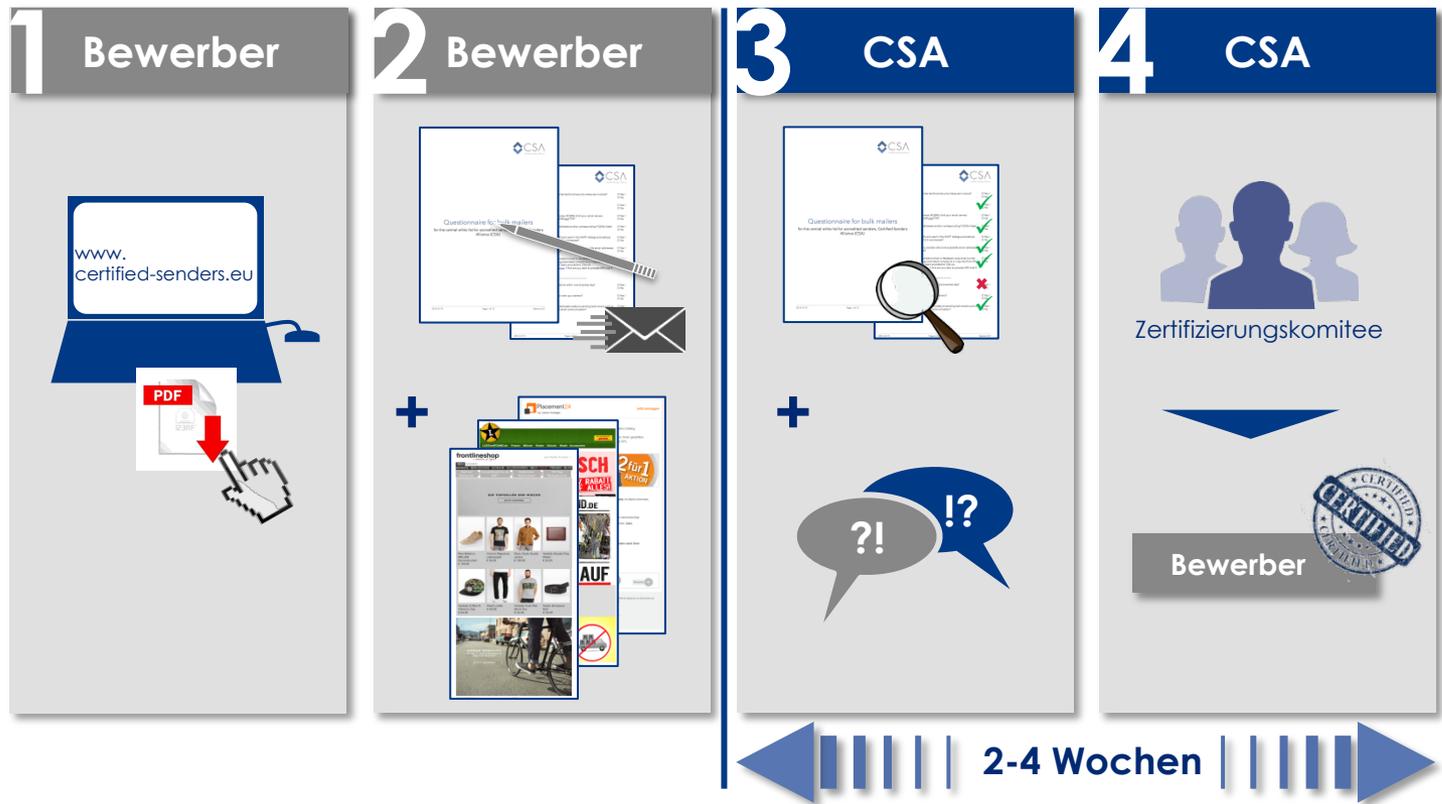
Certified Senders Alliance



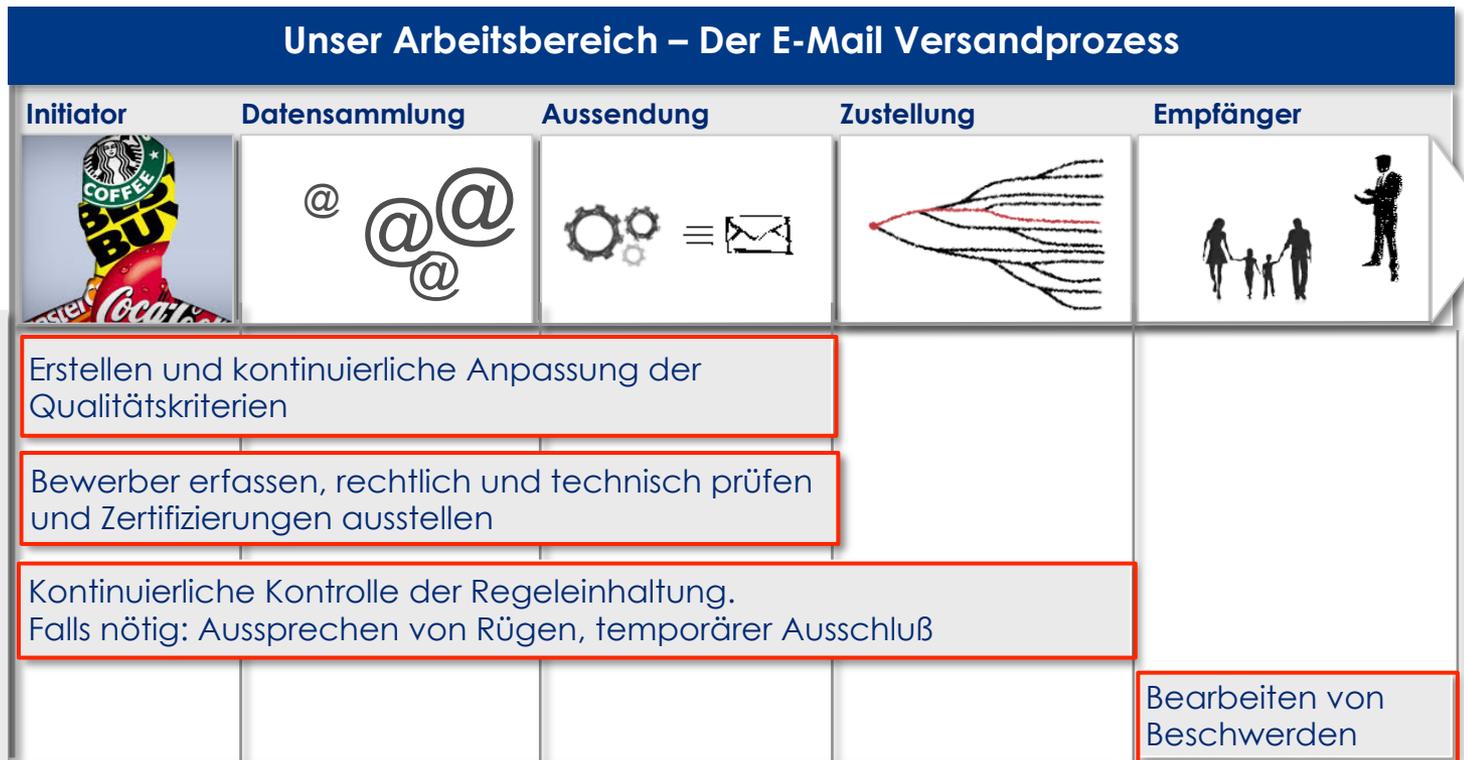

CSA ISP Partner:

- . Spamfilter werden Trennschärfer
- . Ein Kontakt für alle Versender

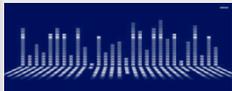
Zertifizierungsprozess



Sicherstellung der Qualität



CSA
Reich-
weite



Agenda

- ✓ CSA Mission und Tätigkeit
- ✓ *Rechtliche und technische Qualitätsstandards*
- ✓ Was bringt die Zukunft?



Qualitätsstandards aus rechtlicher Sicht

Rosa Hafezi

Legal Consulting and Certification
Certified Senders Alliance

Überblick

- ✓ Einwilligung
- ✓ Gestaltung der Inhalte
- ✓ Abbestellung
- ✓ Internationales E-Mailmarketing
- ✓ Rechtliche Konsequenzen
- ✓ Aktuelle Rechtsprechung

Einwilligung

- ✓ B2B und B2C → § 7 Abs. 2 Nr.3 UWG
- ✓ transparent, freiwillig, bewusst, eindeutig, ausdrücklich und separat
- ✓ Co-Registrierung
- ✓ Geltungsdauer
- ✓ Double Opt-In: Ja oder Nein?

Einwilligung

- ✓ Ausnahme vom Opt-In: bestehende Kundenbeziehung, §7 Abs. 3 UWG
- ✓ Voraussetzungen:
 - ◆ E-Mailadresse im Zusammenhang mit Verkauf einer Ware oder Dienstleistung
 - ◆ Werbung nur für gleiche oder ähnliche Produkte
 - ◆ Hinweis auf jederzeitigen Widerspruch und ohne weitere Kosten

Gestaltung der Inhalte

- ✓ Betreff: §6 Abs. 2 TMG: Verschleierungsverbot des kommerziellen Charakters
- ✓ keine falschen Versprechungen oder falsche Drohungen
- ✓ keine typischen Spam-Wörter

Abbestellen der E-Mail

- ✓ Pflicht für Versender gemäß §28 Abs. 4 BDSG, §7 Abs. 2 Nr.4 UWG
- ✓ Hinweis auf Abbestellung bei Einholung der Einwilligung
- ✓ Abbestellmöglichkeit bei jeder Werbe-E-Mail
- ✓ Bestätigungs-E-Mail nicht erforderlich

Internationales E-Mailmarketing

- ✓ Welches Recht ist maßgeblich?
 - Rechtslage des jeweiligen Ziellandes!
- ✓ EU: Opt-In
- ✓ Rechtslage anderer Länder vor Versand überprüfen
- ✓ mit Double Opt-In immer auf der sicheren Seite

Rechtliche Konsequenzen

- ✓ B2B: Unterlassungsanspruch §§ 1004, 823 BGB: Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb; unlautere Wettbewerbshandlung §8 Abs. 3 UWG, Abmahnkosten
- ✓ B2C: Unterlassungsanspruch §§1004, 823 BGB, Berufung auf allgemein. Persönlichkeitsrecht

Aktuelle Rechtsprechung

✓ Tell-a-friend-Funktion: Wann zulässig?

(BGH; LG Arnsberg „Amazon“)

1. Empfehlungs-E-Mail nach außen E-Mail des Nutzers und nicht des Anbieters
2. Nutzer muss die Möglichkeit haben, Betreffzeile und E-Mail-Text selbst zu formulieren oder zumindest ergänzenden Text hinzuzufügen
3. Beschränkung auf bestimmte Anzahl
4. keine Schaffung von Anreizen seitens des Anbieters

Aktuelle Rechtsprechung

✓ Streitwert bei Abmahnung

OLG Hamm: Der Streitwert einer Abmahnung wegen unverlangter Werbe-E-Mail (Spam) an eine Privatperson ist mit maximal 100,- Euro zu bewerten

→ entscheidend sind Umstände des Einzelfalls

Aktuelle Rechtsprechung

✓ Thema Impressum

LG Berlin: Angabe einer E-Mail Adresse dann nicht ausreichend, wenn Verbraucher auf automatisch generierte E-Mail nicht antworten kann



Qualitätsstandards aus technischer Sicht

Alexander Zeh

Engineering Manager
Certified Senders Alliance

Qualitätsstandards

✓ Basics

- ◆ technisch, organisatorisch

✓ DMARC

- ◆ Was ist das?
- ◆ SPF und DKIM?
- ◆ Warum?

Basics

Basics - DNS

✓ DNS-Auflösung

- ◆ A-Record und PTR-Record passen zusammen und sind eindeutig:

~> host mx1.example.org

mx1.example.org has address 12.34.56.78

~> host 12.34.56.78

78.56.34.12.in-addr.arpa domain name pointer
mx1.example.org.

Basics - Technik

- ✓ HELO/EHLO entsprechend dem DNS-Eintrag
- ✓ Einhaltung technischer Standards
 - ◆ z.B. RFCs 821, 2142, 2821, 2822
- ✓ Klare Trennung Massenmails und Individualmails, besondere Absicherung
- ✓ List-ID
- ✓ List-Unsubscribe

Basics - Organisatorisch

- ✓ Vollständige WHOIS-Angaben mit Abuse-Kontakt zu Hostnamen und/oder IP-Adresse
- ✓ Leistungsfähiges Abuse-Desk
- ✓ ARF (RFC 5965) und x-arf Reports automatisch verarbeiten



DMARC

DMARC

- ✓ Was ist DMARC?
 - ◆ **D**omain-based **M**essage **A**uthentication, **R**eporting and **C**onformance
- ✓ Vermindert Spam und Phishing, und ermöglicht es Phishing-Quellen auszumachen

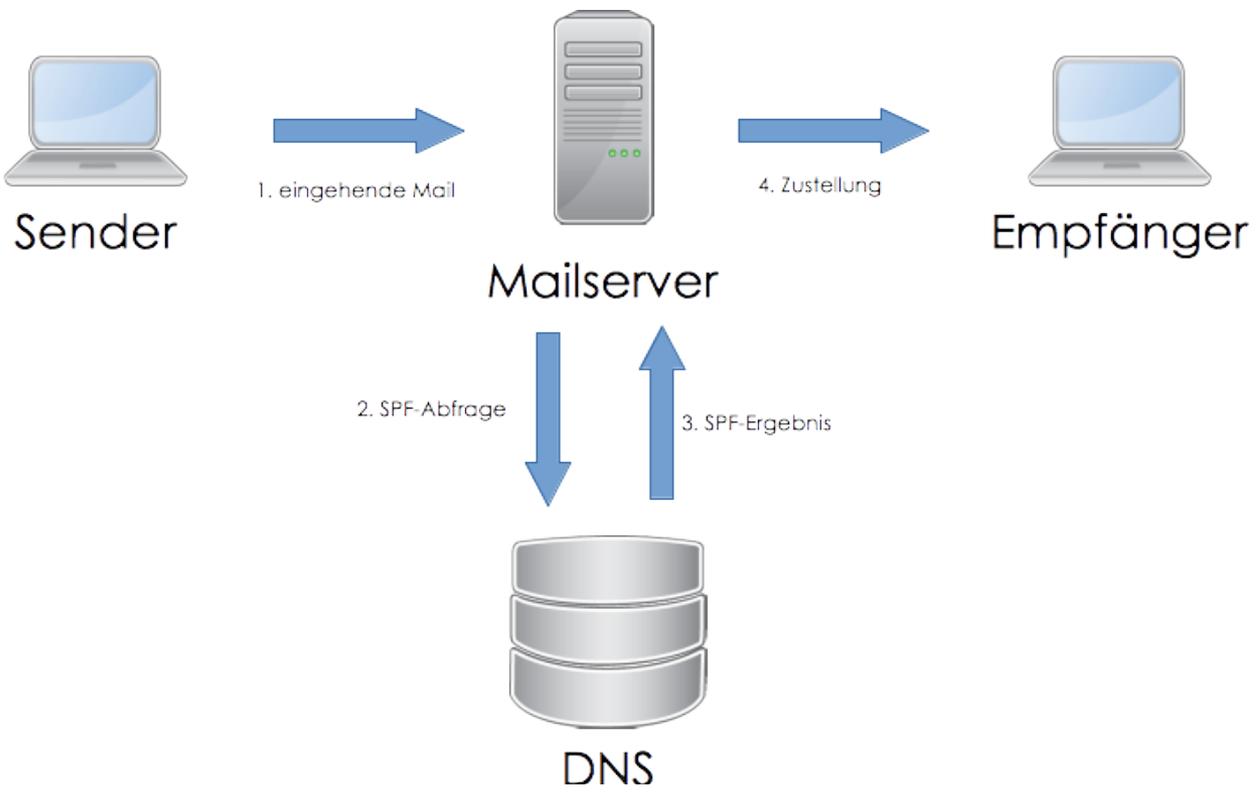
DMARC II

- ✓ IETF Draft, auf dem Weg zum RFC
 - ◆ <https://datatracker.ietf.org/doc/draft-kucherawy-dmarc-base/>
- ✓ <http://dmarc.org/>
- ✓ Setzt SPF und DKIM voraus
 - ◆ Was ist das nun schon wieder?
 - ◆ **Sender Policy Framework**
 - ◆ **DomainKeys Identified Mail**

SPF

SPF

- ✓ Domaininhaber definiert, welche Server zum Versand berechtigt sind.
- ✓ RFC 4408
- ✓ Beispiel:
~> host -t TXT example.org
example.org descriptive text "v=spf1
a:mx1.example.org ip4:11.22.33.44 -all"





DKIM

DKIM

- ✓ Ausgehende Mails werden signiert
- ✓ RFCs 4871, 6376
- ✓ asymmetrische Methode ähnlich S/MIME oder PGP
 - ◆ ausgehende E-Mails enthalten Signatur, die mittels privatem Schlüssel erstellt wurde.
 - ◆ Mit dem öffentlichen Schlüssel aus dem DNS kann diese Signatur geprüft werden.

SPF + DKIM + DMARC = 😊

DMARC im Detail

✓ Beispiel für einen DMARC-Eintrag:

```
v=DMARC1;p=quarantine;pct=100;rua=mailto:postmaster@example.org;ruf=mailto:forensik@example.org;dkim=s;aspf=r
```

◆ v=DMARC1

- ◆ Protokollversion

◆ p=quarantine

- ◆ Was ist zu tun, wenn SPF oder DKIM fehlschlägt?
- ◆ none, quarantine oder reject

DMARC im Detail II

- ◆ `rua=mailto:postmaster@example.org`
 - ◆ Empfänger für aggregierte Reports.
- ◆ `ruf=mailto:forensik@example.org`
 - ◆ Empfänger für forensische Reports.
 - ◆ Aktuell noch rechtliche Unsicherheit bei ISPs
- ◆ `dkim=s`
 - ◆ Auslegung der DKIM-Regeln
 - ◆ `s` = strict, `r` = relaxed
 - ◆ z.B. führt eine Subdomain wie „news.example.org“ im From-Header bei relaxed zu keinem Fehler

Warum der ganze Aufwand?

- ✓ ISPs schützen ihre Kunden vor Spam und Phishing
- ✓ E-Mail-Dienstleister schützen die Marken ihrer Kunden und erhöhen die Zustellbarkeit
- ✓ Markeninhaber schützen ihre Marke/Domain vor Missbrauch

Ein paar Zahlen zur Wirkung

- ✓ PayPal: in 2013 wurden 70% weniger verdächtige E-Mails durch Kunden gemeldet
- ✓ Outlook.com: Meldungen über Phishing in 2013 gegenüber 2012 um 50% gesunken
- ✓ PayPal/ebay: Im Vergleich zu 2012 nur noch halb so viele Phishing-Attacken
- ✓ Gmail: Rückgang des Volumens gefälschter E-Mails um 5000% (!)

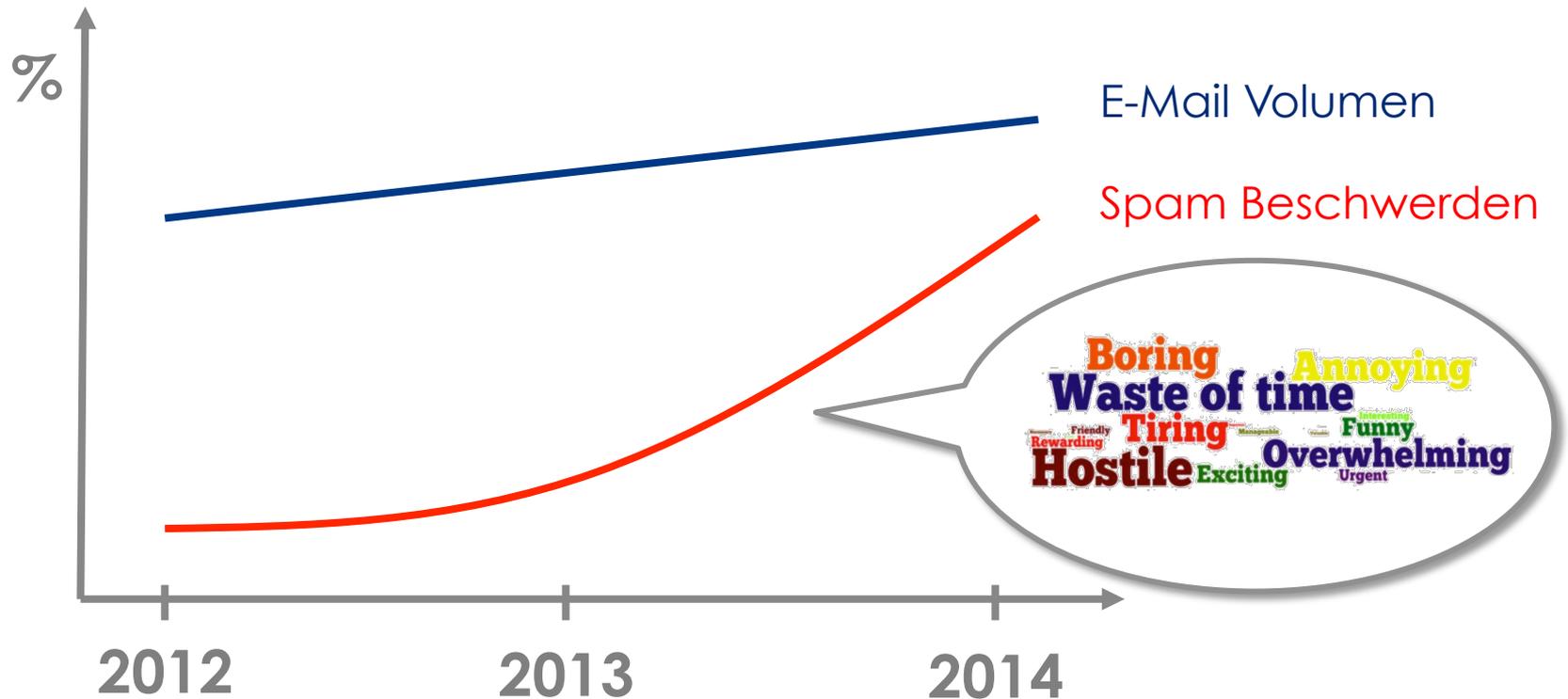
weitere Zahlen

- ✓ Facebook: über 85% der Facebook User vor Phishing geschützt
- ✓ Twitter
 - ◆ zunächst Reports: etwa 2,5 Mrd E-Mails in 45 Tagen.
 - ◆ nach Umstellung auf „reject“: wenige Tausend in mehreren Tagen.

Agenda

- ✓ CSA Mission und Tätigkeit
- ✓ Rechtliche und technische Qualitätsstandards
- ✓ *Was bringt die Zukunft?*

Das Volumen als Spam empfundener E-Mails wächst exponentiell



Wechsel der Verantwortlichkeiten

CSA heute

E-Mail Versender

IP-Reputation (ESP)

Zustellbarkeit

Halbautomatische
Kontrollen



CSA in der Zukunft

Inhaber der E-Mail Listen

IP & Domain Reputation (Marke)

Zustellbarkeit & Markenreputation

Vollautomatische
Kontrollen

eco Richtlinie für zulässiges E-Mail-Marketing



<https://certified-senders.eu>



info@certified-senders.eu

Vielen Dank für die Aufmerksamkeit



Rosa Hafezi

Legal Consulting and Certification

rosa.hafezi@eco.de

+49 (0) 221 / 7000 48 - 255



Alexander Zeh

Engineering Manager

alexander.zeh@eco.de

+49 (0) 221 / 7000 48 - 171