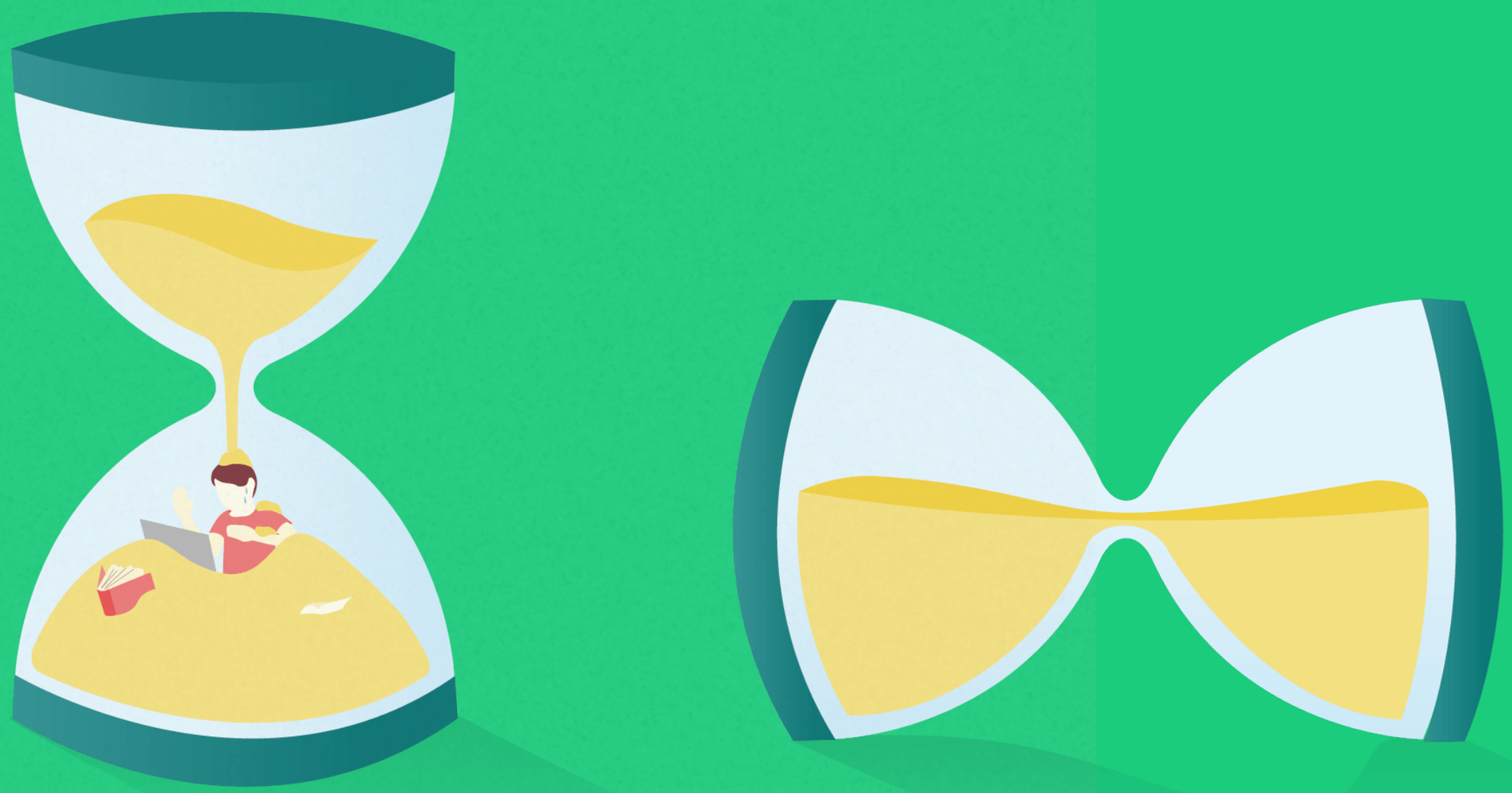
E-Mail & Domain-Security

Back to the 90s. Veraltet und doch in Mode

nextindex

Überblick, Ablauf & Fragen



Über nextindex.

nextindex GmbH & Co. KG

- Dienstleistungs- und Beratungsunternehmen
- Fokus: Digitale Infrastrukturen, Sicherheit in Web-Sicherheit, Datenschutz, Datensicherheit
- Sitz: Bochum
- Leistungen:
  Datenschutz (Audits, DSB), Beratung zu TOMs, Software-Entwicklung, Pentest für Websysteme, Awareness-Trainings, Phishing Simulationen
- Abteilung Datenschutz (DSB Ruhr)

DSBRuhr

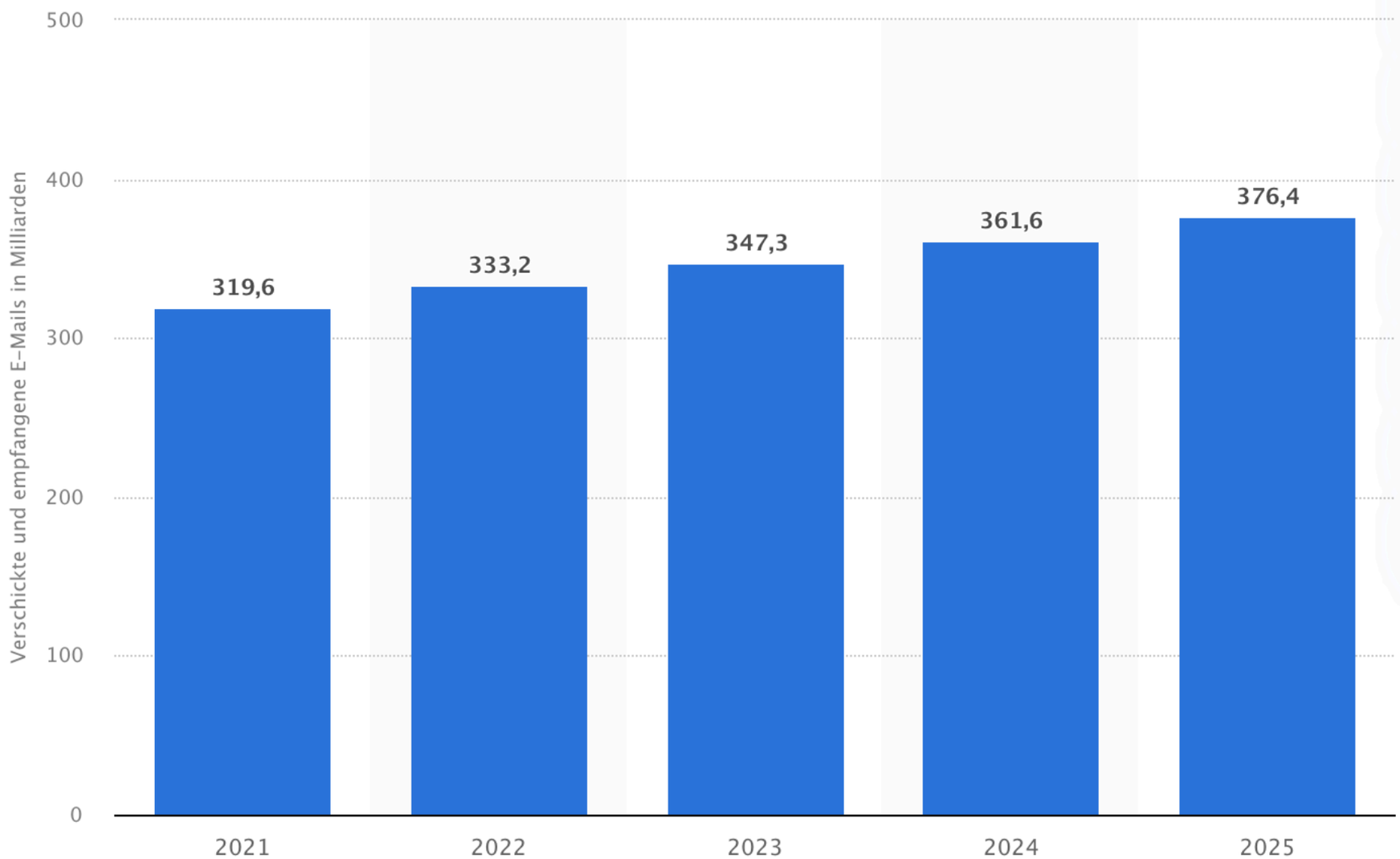
Patrick Grihn

- zert. Datenschutzauditor
  zert. Datenschutzbeauftragter
- Geschäftsführender Gesellschafter
  nextindex GmbH & Co. KG
  (Leitung Datenschutz & Consulting)
- Leiter KG Informationssicherheit
  networker NRW e. V.
- Fachbereit Sicherheit
  eco - Verband der Internetwirtschaft
- Initiator & Mitglied AK Stand der Technik
  eco, TeleTrusT, networker NRW
- BvD: Stv. Leiter RG West,
  Ausschuss Prüfaufgaben des DSB

Warum eigentlich E-Mails?

nextindex

Prognose Weltweite Nutzung von E-Mails (Milliarden)

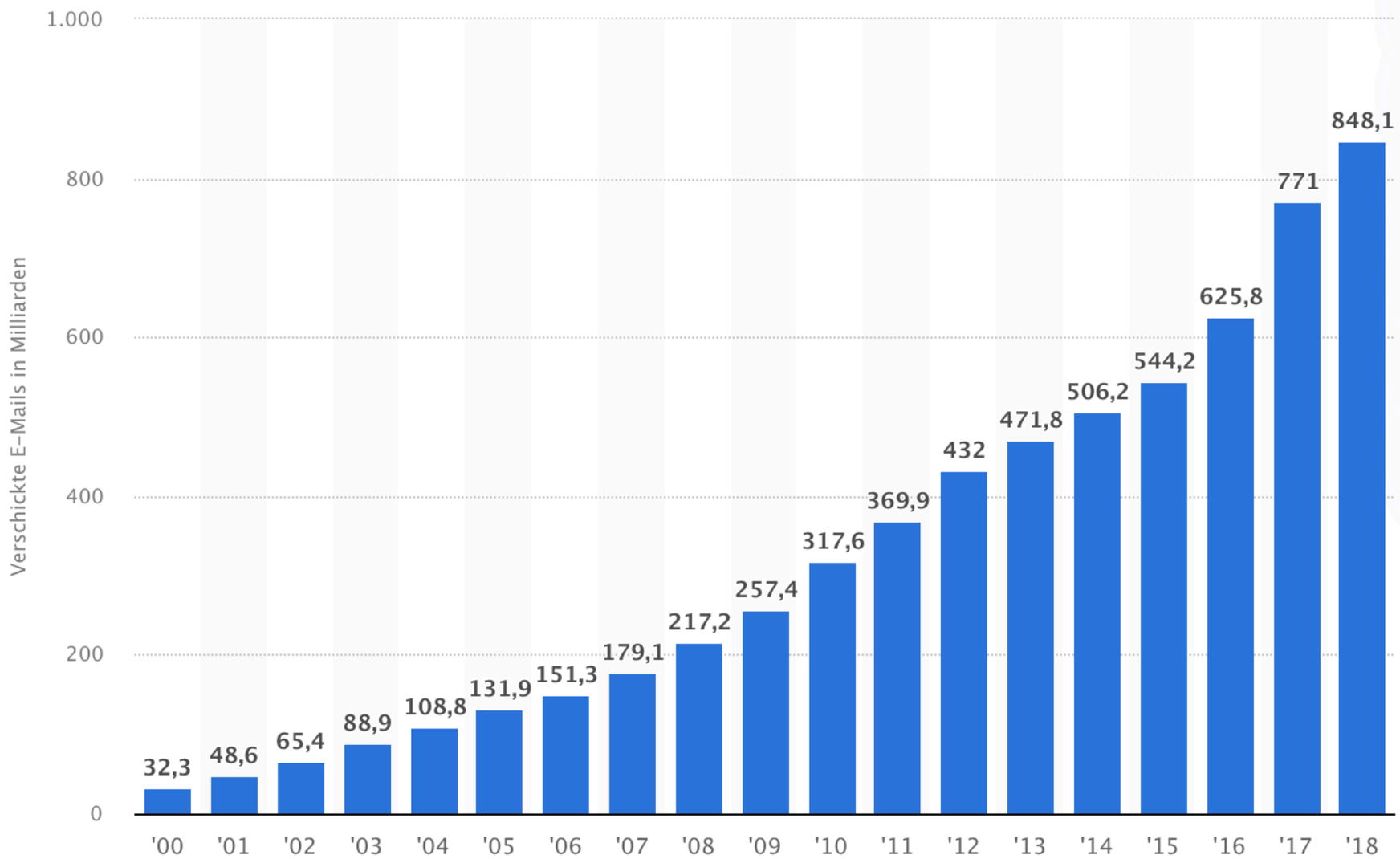


© Statista 2022

Details zur Statistik

Quellen anzeigen

Versendete Mails pro Jahr Deutschland (Milliarden)



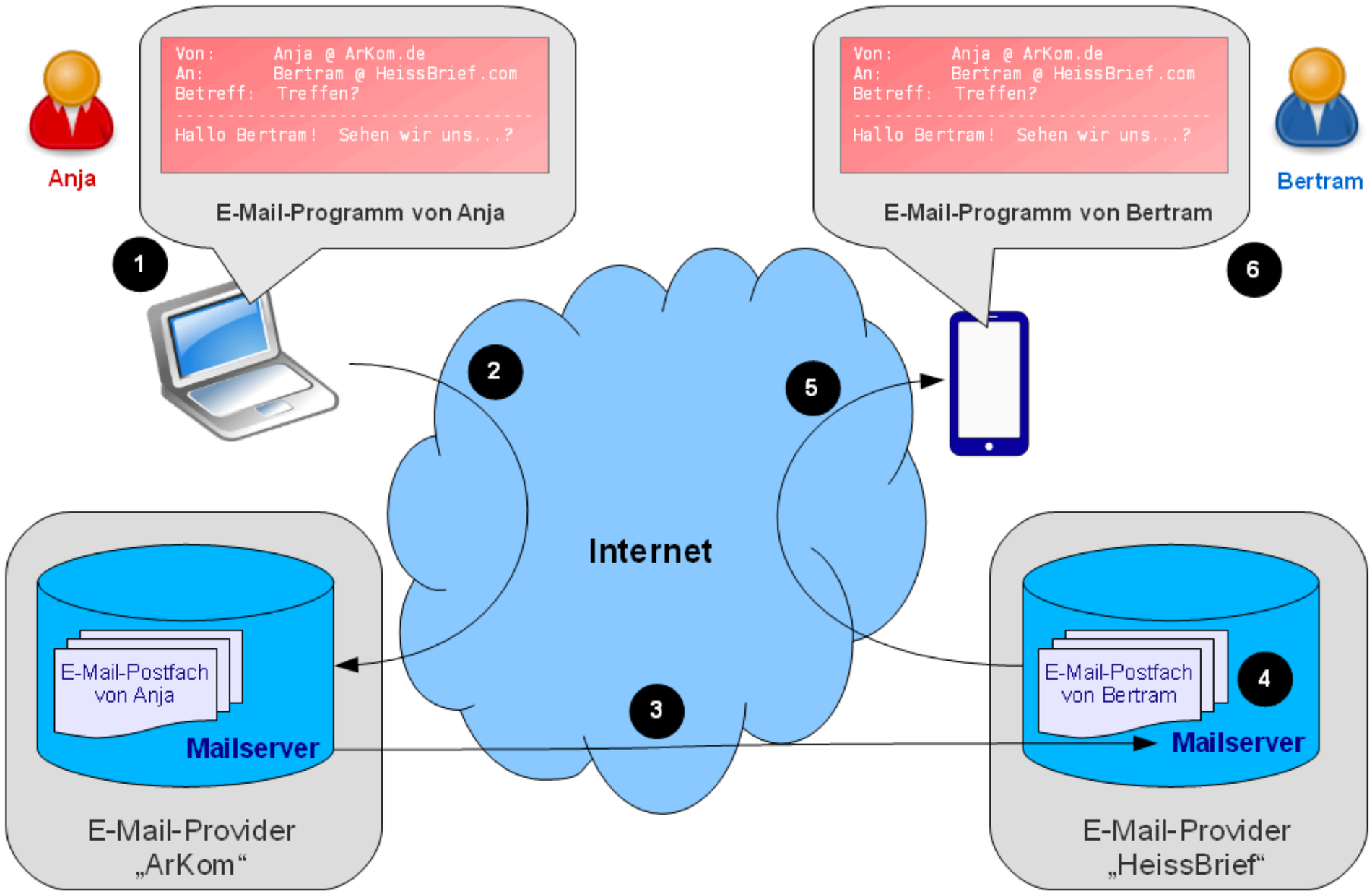
© Statista 2022

Details zur Statistik

Quellen anzeigen

Wie funktionieren E-Mails?

nextindex



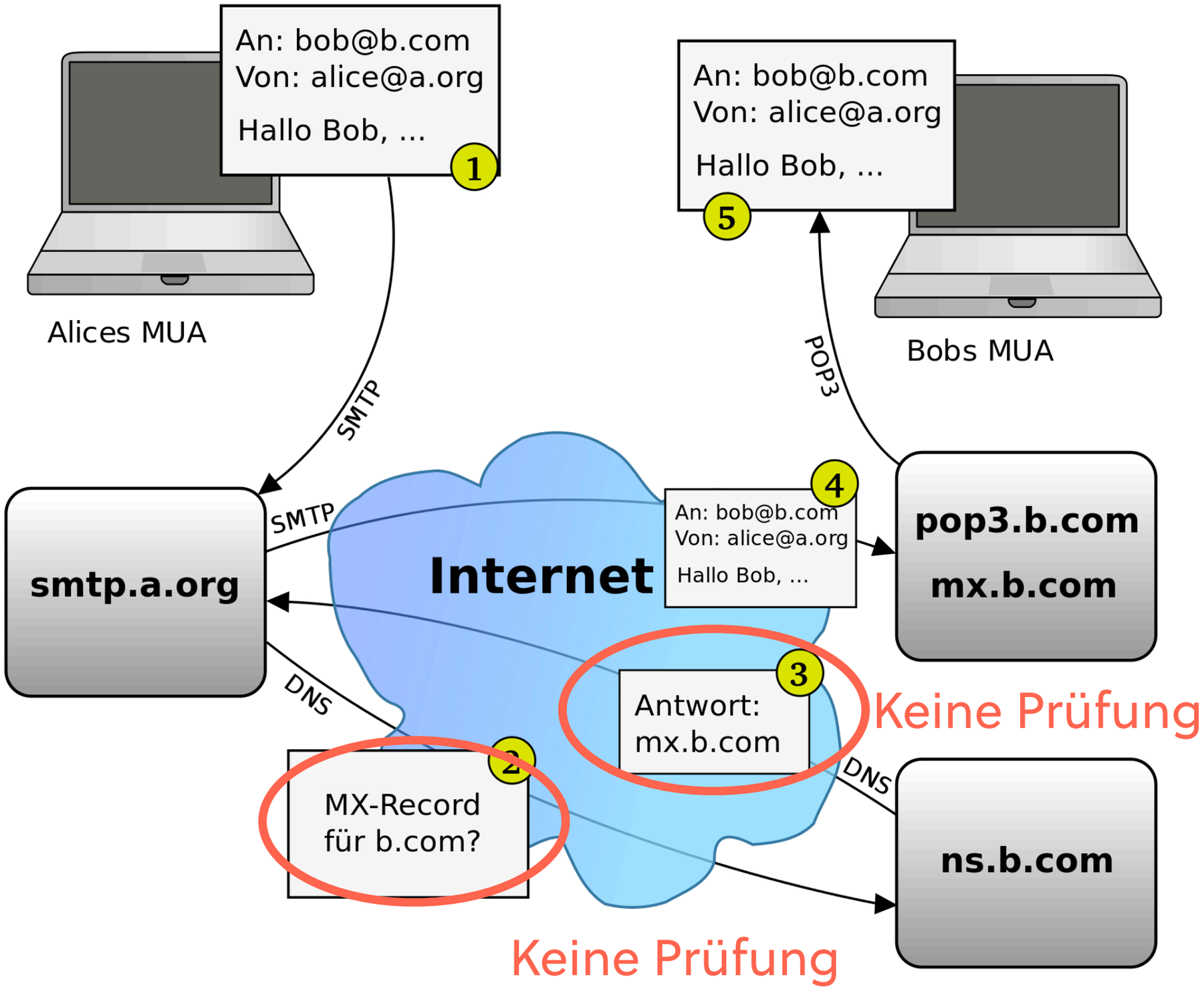
Quelle: Wikipedia

```
S: 220 smtp2go.com ESMTP Exim
C: HELO mydomain.com
S: 250 Hello mydomain.com
C: MAIL FROM:<sender@mydomain.com>
S: 250 Ok
C: RCPT TO:<recipient@anotherdomain.com>
S: 250 Accepted
C: DATA
S: 354 Enter message, ending with "." on a line by itself
C: Subject: sample message
C: From: sender@mydomain.com
C: To: recipient@anotherdomain.com
C:
C: Greetings,
C: Typed message (content)
C: Goodbye.
C: .
S: 250 OK
C: QUIT
S: 221 www.sample.com closing connection
```

Quelle: smtp2go.com

Status Quo

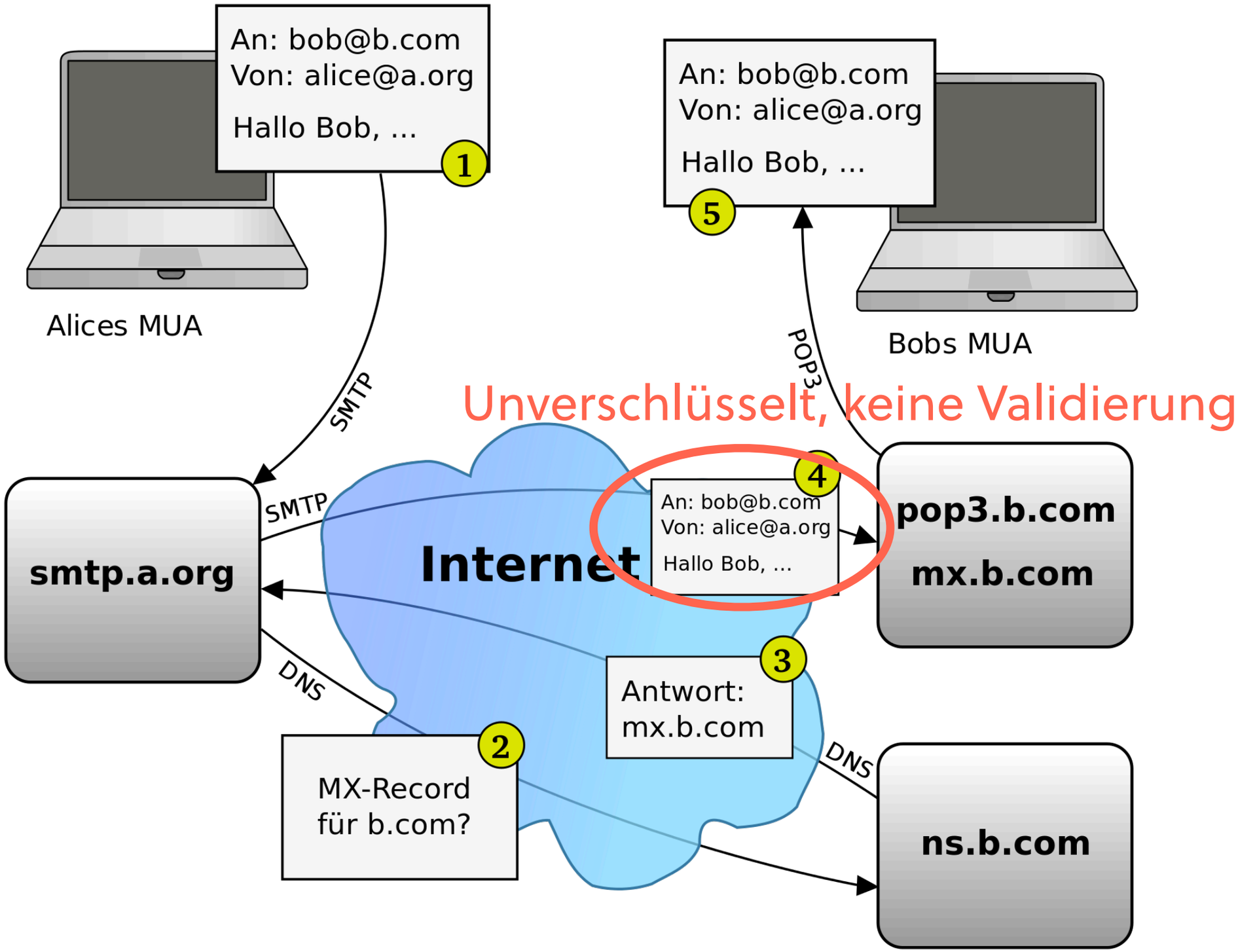
- E-Mail Protokoll per se unsicher (und veraltet)
- Verschlüsselung häufig nur zwischen Client und Mailserver
- Keine Authentifizierung zwischen Servern
- TLS häufig nur optional (Mailserver)
- SPF Records häufig nicht gesetzt oder auf Soft-Fail
- Keine Ausreichende Prüfung von Mailservern



Quelle: wikipedia.org

DNS

- Abfragen Manipulierbar (z. B. durch internen DNS)
- DNS Anfragen i. d. R. unverschlüsselt (Port 53)
  - -> Häufig Ansatz für Deep-Packet-Inspection
- Lösung: DNSSEC, DNS over TLS (DoT), DNS over https (DoH)
- Persönliche Lösung: Vertrauenswürdige DNS setzen + Verschlüsselung



Quelle: wikipedia.org

Also warum eigentlich Mails?

- Keine zentrale Instanz (wie bei WhatsApp o. ä.)
- Interoperabel
- Weltweit akzeptierter (offener) Standard

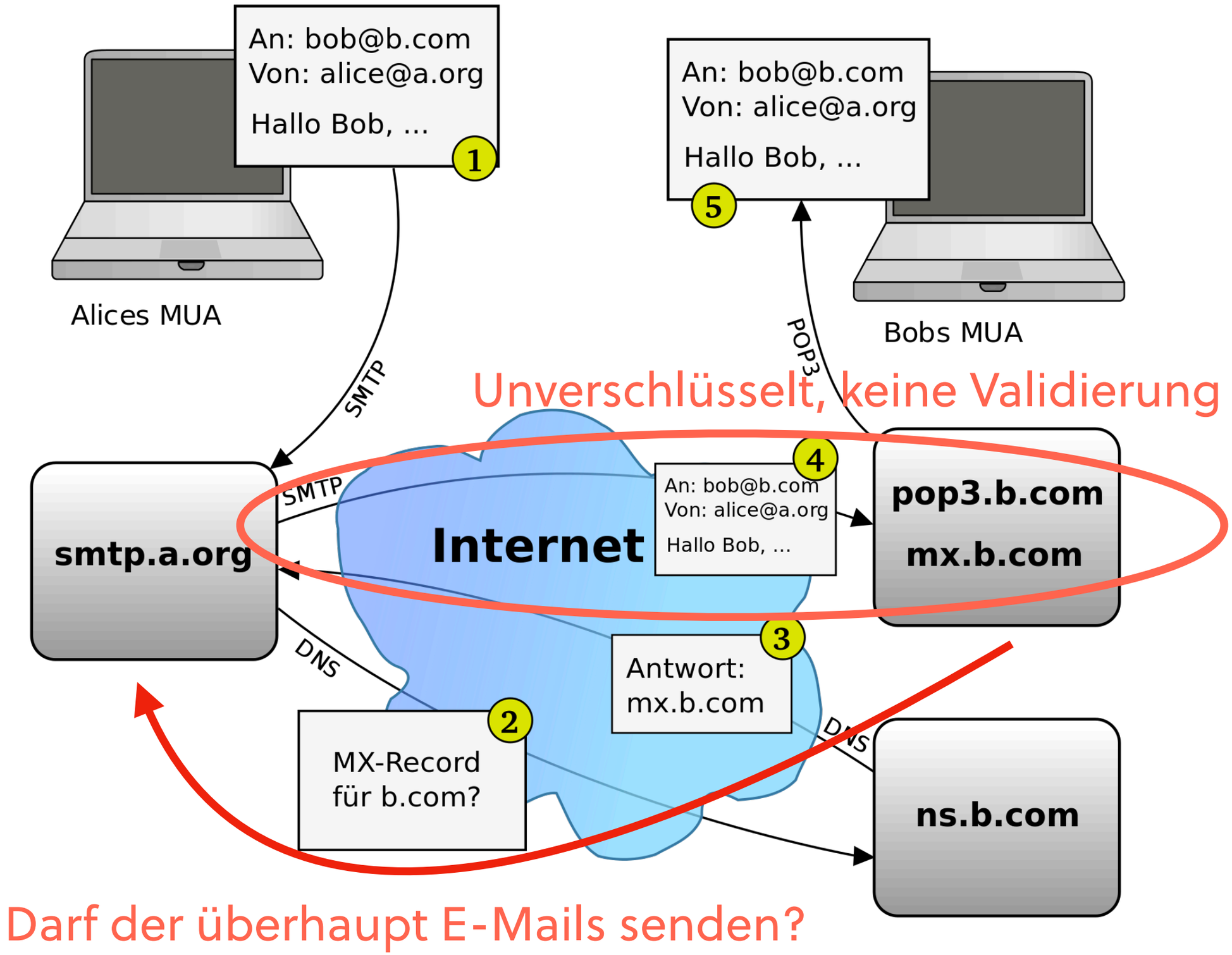
Probleme

- Standard vom Ende der 1980er
- Gedacht zum Austausch zwischen Universitäten
- Teilnehmer galten als „Vertrauenswürdig“
- Standard hat sich im Wesentlichen nicht verändert
- Verschlüsselung und Autorisierung war niemals vorgesehen
- Authentizität nicht gegeben

Zwischenfazit: E-Mails sind kaputt

nextindex

Lösungsansätze



Quelle: wikipedia.org

SPF

SPF - Sender Policy Framework

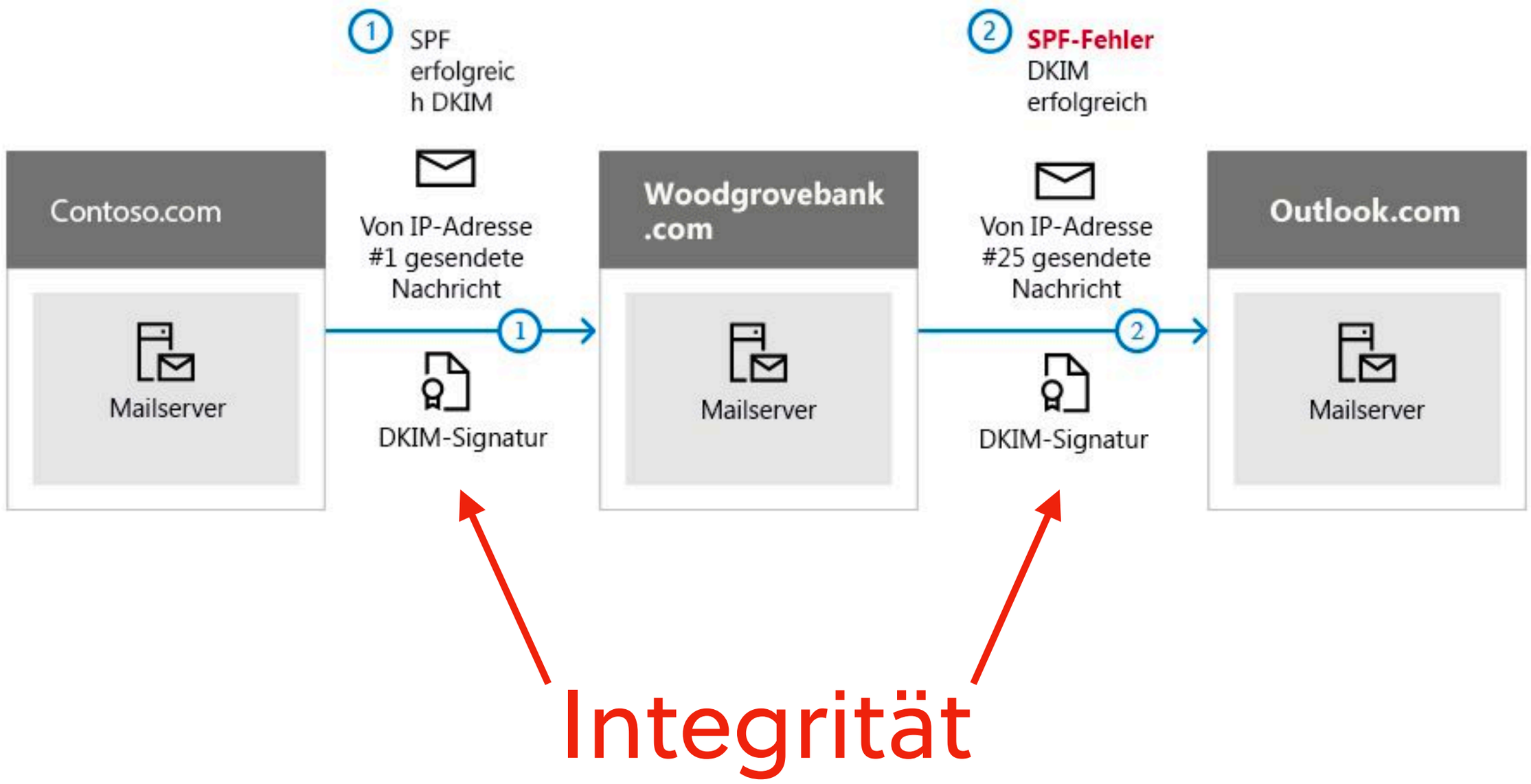
- Ziel: in der Domain werden Server (IPs) hinterlegt, die E-Mails versenden dürfen
- Beispiel: Microsoft erlaubt, Webserver erlaubt, alle anderen Server verboten (Mails wegschmeißen)
- Häufigste Einstellung: Alles erlauben (weder verboten noch explizit genehmigt) s. g. softfail

Vorteile

- Versender können eigene Richtlinien vorgeben
- Versender erhalten Kontrolle über die Mails
- Empfänger können Authentizität prüfen
- Empfänger können eigene Regeln erstellen, wie mit Richtlinien des Empfängers umgehen wollen (Gleichzeitig ein Nachteil)
- Große Provider integrieren automatisch SPF Records (GMX, WEB, Microsoft) - aber nur mit „alles erlaubt“ Softfail

Nachteile

- Viele IT-ler kennen SPF nicht
- Häufig alles auf Softfail
- Empfänger kann eigene Richtlinien zum Umgang erstellen
- Problem bei Weiterleitungen (Da der Server in der „Mitte“ nicht als erlaubter Server genannt ist)



Quelle: microsoft

DKIM

DKIM - DomainKeys Identified Mail

- Schlüssel wird ebenfalls im DNS Server hinterlegt
- Der Header einer Mail wird via Key mit RSA signiert
- Signatur erfolgt auf dem sendenden Mailserver
- Der Empfänger kann mittels des Keys auf dem DNS die Signatur prüfen und somit die Echtheit der Mail sicherstellen
- Kein Spamschutz, sondern Sicherstellung der Mailstrecke
- DKIM vor allem in Verbindung mit SPF sinnvoll

Prüfung von Mails

nextindex

```
v=spf1 mx a include:_spf.manitu.net -all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	mx		Pass	Match if IP is one of the MX hosts for given domain name.
+	a		Pass	Match if IP has a DNS 'A' record in given domain.
+	include	_spf.manitu.net	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

	Test	Result	
!	SPF Record Deprecated	The DNS record type 99 (SPF) has been deprecated	More Info
✓	SPF Record Published	SPF Record found	
✓	SPF Multiple Records	Less than two records found	
✓	SPF Contains characters after ALL	No items after 'ALL'.	
✓	SPF Syntax Check	The record is valid	
✓	SPF Included Lookups	Number of included lookups is OK	
✓	SPF Type PTR Check	No type PTR found	
✓	SPF Void Lookups	Number of void lookups is OK	
✓	SPF MX Resource Records	Number of MX Resource Records is OK	
✓	SPF Record Null Value	No Null DNS Lookups found	

Quelle: mxtoolbox.com

Prüfung

- SPF kann öffentlich geprüft werden
- DKIM **kann** geprüft werden, allerdings die Validität nur mit einer DKIM Signatur aus dem Header

Alles liegt beim Empfänger, oder?

Empfang gelöst

- SPF und DKIM dienen vor allem dem Empfänger
- Vorteile: Empfänger kann Echtheit der Mail prüfen (Authentizität und Integrität)
- Nachteil: Ich erfahre als Versender nicht, ob das beachtet wird, **oder** ob jemand anderes versucht, in meinem Namen zu versenden

Lösung

DMARC: Domain-based Message **Authentication**, **Reporting** and **Conformance**

DMARC - Funktion

- SPF und DKIM sind Grundvoraussetzung
- Richtlinie zum Umgang mit Mails
  - Prüfung von SPF + DKIM und dann Umgang mit dem Ergebnis
  - Beispiel: Strikt oder ‚Relaxed': Quarantäne, Löschung/ Reject, none
- Rückmeldung möglich - DMARC Reports

DMARC Reports

- Enthalten Ergebnisse über Umgang mit Mails
- Gibt Rückschlüsse über Versender
- Beispiele:
  - SPF + DKIM ok
  - SPF fail, DKIM ok (Hinweis auf Weiterleitung)

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
▼<feedback xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <version>1.0</version>
 ▼<report_metadata>
    <org_name>Outlook.com</org_name>
    <email>dmarcreport@microsoft.com</email>
    <report_id>372a05528818494cb2efad0b1eeedf97</report_id>
   ▼<date_range>
      <begin>1648598400</begin>
      <end>1648684800</end>
    </date_range>
  </report_metadata>
 ▼<policy_published>
    <domain>nextindex.de</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>quarantine</p>
    <sp>quarantine</sp>
    <pct>100</pct>
    <fo>0</fo>
  </policy_published>
 ▼<record>
  ▼<row>
     <source_ip>216.201.81.212</source_ip>
     <count>1</count>
   ▼<policy_evaluated>
      <disposition>quarantine</disposition>
      <dkim>fail</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
 ▼<identifiers>
    <envelope_to>hotmail.com</envelope_to>
    <envelope_from>nextindex.de</envelope_from>
    <header_from>nextindex.de</header_from>
  </identifiers>
 ▼<auth_results>
   ▼<spf>
      <domain>nextindex.de</domain>
      <scope>mfrom</scope>
      <result>softfail</result>
    </spf>
  </auth_results>
 </record>
</feedback>
```

216.201.81.212 | digitalconvul-

dnslytics.com/ip/216.201.81.212

Inkognito (3)

DNSlytics

Login Pricing API About Support

Reports Addons Monitoring Domain Tools Reverse Tools More

Domain, IPv4/IPv6, ASN Search

IPv4 root -> 216/8 -> 216.201.80.0/20 -> 216.201.81.212

IP information 216.201.81.212

IP address	216.201.81.212
Location	United States (US)
Registry	arin

Network information

IP address	216.201.81.212
PTR record	digitalconvul-1.nationalnet.com
ASN number	46562
ASN name (ISP)	Performive LLC
IP-range/subnet	216.201.80.0/20 216.201.80.0 - 216.201.95.255
Network tools	Ping 216.201.81.212 Traceroute 216.201.81.212

Hosting information

Summary of domains, mail servers and name servers currently hosted on this IP address.

Number of domains hosted	1
Number of mail servers hosted	0
Number of name servers hosted	0

Tools for you

Your public IP Address
Information about your public IP Address like reverse dns, hosting info and whois data.

Chrome Extension
Our data and tools directly inside your Chrome browser.

My IP Address for Chrome
This extension shows detailed info about your IP, your domain and your provider. Get an IP change alert and see your IP history.

IP Domain Flag for Chrome
This extension shows a country flag for the current website's server.

Other services

Browser Addons
Our collection of browser extensions and apps.

Mögliche Ergebnisse

- Spam oder Spoofing ist im Umlauf
- Fehlkonfigurierte Server (Mailserver)
- Fehlkonfigurierte Webseiten
- Schatten-IT
- „Alles in Ordnung“

E-Mails: Infos, Prüfung &Lücken

nextindex

E-Mail Header

- Header haben häufig mehr Optionen als nötig
- Infrastruktur wird dritten offen gelegt
- Grund: „Debugging“ von Admins

```
Delivered-To: grihn@nextindex.de
Received: by 2002:a05:6830:16da:0:0:0:0 with SMTP id l26csp715913otr;
        Fri, 15 Feb 2019 06:54:29 -0800 (PST)
X-Received: by === with SMTP id ===;
        Fri, 15 Feb 2019 06:54:29 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1550242469; cv=none;
       ===
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d====; s=arc-20160816;
===
ARC-Authentication-Results: i=1; ===;
       spf=neutral (===: 212.227.17.10 is neither permitted nor denied by best guess record for domain of ===) smtp.mailfrom====
Return-Path: ===
Received: from mout.kundenserver.de (mout.kundenserver.de. [212.227.17.10])
        by mx.=== with ESMTPS id 013s1471i234wrj.243.2019.02.15.06.54.29
        for <grihn@nextindex.de>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Fri, 15 Feb 2019 06:54:29 -0800 (PST)
Received-SPF: neutral (===: 212.227.17.10 is neither permitted nor denied by best guess record for domain of ===) client-ip=212.227.17.10;
Authentication-Results: mx.===;
       spf=neutral (===: 212.227.17.10 is neither permitted nor denied by best guess record for domain of ===) smtp.mailfrom====
Received: from Ralfs-MacBook-Pro.local ([78.94.114.70]) by
 mrelayeu.kundenserver.de (mreue107 [212.227.15.183]) with ESMTPSA (Nemesis)
 id 1MekGB-1hStlp3Xjp-00an3A for <grihn@nextindex.de>; Fri, 15 Feb 2019
 15:54:28 +0100
Subject: ===
To: Patrick Grihn <grihn@nextindex.de>
References: ===
From: ===
Message-ID:===
Date: ===
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:60.0)
 Gecko/20100101 Thunderbird/60.5.0
```

#	Delay	From *		To *	Protocol	Time received
0	2 sec	b2b-130-180-102-27.unitymedia.biz	→	mail51.mittwald.de		23.5.2018, 9:26:47 MESZ
1		mail51.mittwald.de	→	localhost	ESMTP	23.5.2018, 9:26:47 MESZ
2	1 sec	ac01.internal	→	mail01.agenturserver.de	ESMTP	23.5.2018, 9:26:48 MESZ
3		mail01.internal	→	mailbulkout01.agenturserver.de	ESMTP	23.5.2018, 9:26:48 MESZ
4	1 sec	mailbulkout01.agenturserver.de	→	inbound-smtp.eu-west-1.amazonaws.com	SMTP	23.5.2018, 9:26:49 MESZ

```
Received: from mailbulkout01.agenturserver.de (mailbulkout01.agenturserver.de [185.15.192.48])
 for ===;
 Wed, ===
Received-SPF: neutral (spfCheck: 185.15.192.48 is neither permitted nor denied by domain of ===) client-ip=185.15.192.48; envelope-from====; hel
 spf=neutral (spfCheck: 185.15.192.48 is neither permitted nor denied by domain of ===) client-ip=185.15.192.48; envelope-from======; helo=mailb
Received: from mail01.agenturserver.de (mail01.internal [172.16.51.30])
    by mailbulkout01.agenturserver.de (Postfix) with ESMTP id 317E61301C0
Received: from localhost (ac01.internal [172.16.51.81])
    by mail01.agenturserver.de (Postfix) with ESMTP id 20F0120DAD
X-Virus-Scanned: Debian amavisd-new at ac01.mittwald.de
X-Spam-Level:
Received: from mail51.mittwald.de ([172.16.51.30])
    by localhost (ac01.mittwald.de [172.16.51.81]) (amavisd-new, port 10026)
    Wed, 23 May 2018 09:26:47 +0200 (CEST)
Received: from SRV-Exchange-01.====.local (b2b-130-180-102-27.unitymedia.biz [130.180.102.27])
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-SHA384 (256/256 bits))
    (No client certificate requested)
    (Authenticated sender: p123142p2)
    by mail51.mittwald.de (Postfix) with ESMTPSA
Received: from SRV-Exchange-01.====.local (192.168.16.237) by
 SRV-Exchange-01.====.local (192.168.16.237) with Microsoft SMTP Server (TLS)
 id 15.0.1210.3; Wed, 23 May 2018 09:26:46 +0200
Received: from SRV-Exchange-01.====.local ([fe80::68d9:59ad:55b9:729c]) by
 SRV-Exchange-01.====.local ([fe80::68d9:59ad:55b9:729c%12]) with mapi id
 15.00.1210.000; Wed, 23 May 2018 09:26:46 +0200
In-Reply-To: ===
Accept-Language: de-DE, en-US
Content-Language: de-DE
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
x-ms-exchange-transport-fromentityheader: Hosted
x-originating-ip: [192.168.16.246]
MIME-Version: 1.0
```

```
Received: from mailgate.==== (mailgate.==== [195.50.145.18])
 Fri, 18 May 2018 20:07:01 +0000 (UTC)
Received-SPF: none (spfCheck: 195.50.145.18 is neither permitted nor denied by domain of ====) client-ip=195.50.145.18; envelope-from=js@====; he
 spf=none (spfCheck: 195.50.145.18 is neither permitted nor denied by domain of ====) client-ip=195.50.145.18; envelope-from=js@====; helo=mailga
X-SES-DKIM-SIGNATURE: a=rsa-sha256; q=dns/txt; b=r6gaOx2QzDJfM93TK1nhFaviyElp4ApC1IXLd10SgWl4Q680ysrlYYHfToGN0izsxSaALdezLwQI4BJvu0WqO3clIxRNUI+8
Received: from mailgate2.==== (mailgate.dmz.==== [192.168.180.45])
    by mailgate.==== (8.14.4/...) with SMTP id w4IK70dh008542
Received: from [192.168.101.2] (helo=multi.bochum.====)
    by mailgate2.==== with G Data MailSecurity;
Received: from node01124.bochum.===.de (node01124.bochum.===.de [192.168.101.124])
    by multi.bochum.==== (8.15.2/8.13.4/Debian -2) with ESMTP id w4IK6sN2013862;
    Fri, 18 May 2018 22:06:54 +0200
Cc: "@====" <@====>
MI-Version: 1.0
X-KeepSent: 23F9460A:2E1CB7F1-C1258291:006DDA71;
 type=4; name=$KeepSent
X-Mailer: IBM Notes Release 9.0 March 08, 2013
Message-ID: <>
From: ""===
X-MIMETrack: Serialize by Router on BO-==-1/Server/Zerna-==(Release 9.0.1FP3|January  12, 2015) at
 === 22:06:52,
    Serialize complete at === 22:06:52
Content-Type: multipart/alternative; boundary="= alternative 006E7E72C1258291_="
X-AVK-Virus-Check: AVA 25.17102;===
```

Ergebnisse von Mails

- x originated ip / received by => IP Adresse oder Lokale Domäne
- Infrastruktur der Mailserver ist sichtbar
- SPF Record steht direkt mit im Header
- Teilweise sogar Anti-Spam Komponenten
- Teilweise interne IP-Kreise, Domänen und Hostnames

Fazit und Empfehlungen

Fazit

- Unternehmen haben die Möglichkeit ihre Domains und damit Ihre Authentizität zu schützen
- Empfänger können die Authentizität prüfen und aktive Maßnahmen ergreifen (und Mails bspw. markieren oder Abweisen)
- Mit DMARC bekommt man einen Überblick über funktionierende IT, Fehlfunktionen oder Identitätsmissbrauch
- Die Ziele Authentizität und Integrität können hierüber gestärkt oder überhaupt gewährleistet werden

Empfehlungen

- Führen Sie SPF Records ein, sofern nicht schon geschehen
  - Testbetrieb: Softfails
  - Live-Betrieb (nach 30 Tagen): Fail bei nicht autorisierten Versendern (IPs)
- DKIM Signaturen nutzen, wo möglich
- Beachten Sie: Mailserver, Webmails/Kontaktformulare, Weiterleitungen, Newslettersysteme u. ä.
- Führen Sie Schrittweise DMARC ein und werten Sie die Berichte aus, mindestens Stichproben

Danke.

nextindex

Patrick Grihn

Geschäftsführer nextindex GmbH & Co. KG
zert. Datenschutzauditor (TÜV®)
zert. Datenschutzbeauftragter (TÜV®)
zert. Sachverständiger für Datenschutz und IT-Sicherheit

Kontakt

nextindex GmbH & Co. KG
Grabenstr. 12
44787 Bochum

www.nextindex.de
www.dsb.ruhr

grihn@nextindex.de

nextindex