DNSSEC-Unterstützung durch Heimrouter

Thorsten Dietrich

Bundesamt für Sicherheit in der Informationstechnik

2. DNSSEC-Testbed Meeting / 26. Januar 2010

Inhalt

- Motivation
- Vergleichbare Studien
- Ziele
- Methodik
- Untersuchte Geräte
- Ergebnisse
- Fazit

Motivation

- DNS-Spezifikation enthält Schwachstellen
  → Angreifbar und unsicher (z.B. Cache-Poisoning)
- Verbesserung der Sicherheit durch DNSSEC-Spezifikation
  → Einführung von DNSSEC aus BSI-Sicht dringend erforderlich
- ABER:
  - Protokoll-Erweiterungen müssen durch aktuelle Hard- und Software unterstützt werden
  - Abwärtskompatibilität muss gewährleistet sein
- Start einer DNSSEC-Initiative durch DENIC, eco und BSI
- Hinweise auf Probleme im Heimrouterbereich durch vorausgehende Untersuchungen in .uk und .se
  → Notwendigkeit, Situation in Deutschland zu untersuchen

Vergleichbare Studien

- Ursprung in 2007:

  mit DNSSEC signierte schwedische Zone „gavle.se“, war für einige Benutzer plötzlich nicht mehr erreichbar

  → Ursache? Einige Heimrouter konnten die DNSSEC Flags nicht verarbeiten
- Untersuchungen der Heimroutereigenschaften in Schweden (Februar 2008) und Großbritannien (September 2008)
- Ergebnisse:
  - Nur wenige Geräte konnten ohne Einschränkungen DNSSEC-Anfragen bei Verwendung als DNS-Proxy verarbeiten
  - Die meisten Geräte konnten jedoch DNSSEC-Anfragen ohne Probleme routen

Ziele der BSI-Studie

- Getestete Produkte mehrheitlich für den schwedischen bzw. britischen Markt relevant
- Studien aus 2008
  Weiterentwicklungen / Technischer Fortschritt ?
- Zwischenzeitliche Erstellung des Internet-Draft „DNS Proxy Implementation Guidelines“

→ **Aktuelle Untersuchung von in Deutschland marktüblichen Geräten auf DNSSEC Tauglichkeit und weitere Sicherheitsaspekte**

Inhalt

- Motivation
- Vergleichbare Studien
- Ziele
- Methodik
- Untersuchte Geräte
- Ergebnisse
- Fazit

Hintergrund: DNSSEC Flags

- DO – Bit = **D**NSSEC **O**K
  Signalisierung von DNSSEC-Kompatibilität durch den Client
  (Definiert in RFC3225)
- AD – Bit = **A**uthenticated **D**ata
  Signalisierung einer erfolgreichen Validierung durch den Server
  (Definiert in RFC3655)
  Ergänzung in IETF-Draft “dnsext-dnssec-bis-updates“:

  „This document defines it as a signal indicating that the requester understands and is interested in the value of the AD bit in the response. This allows a requestor to indicate that it understands the AD bit without also requesting DNSSEC data via the DO bit“
- CD – Bit = **C**hecking **D**isabled
  Signalisierung an den Server, keine Validierung durchzuführen
  (Definiert in RFC2535)

Hintergrund: EDNS0

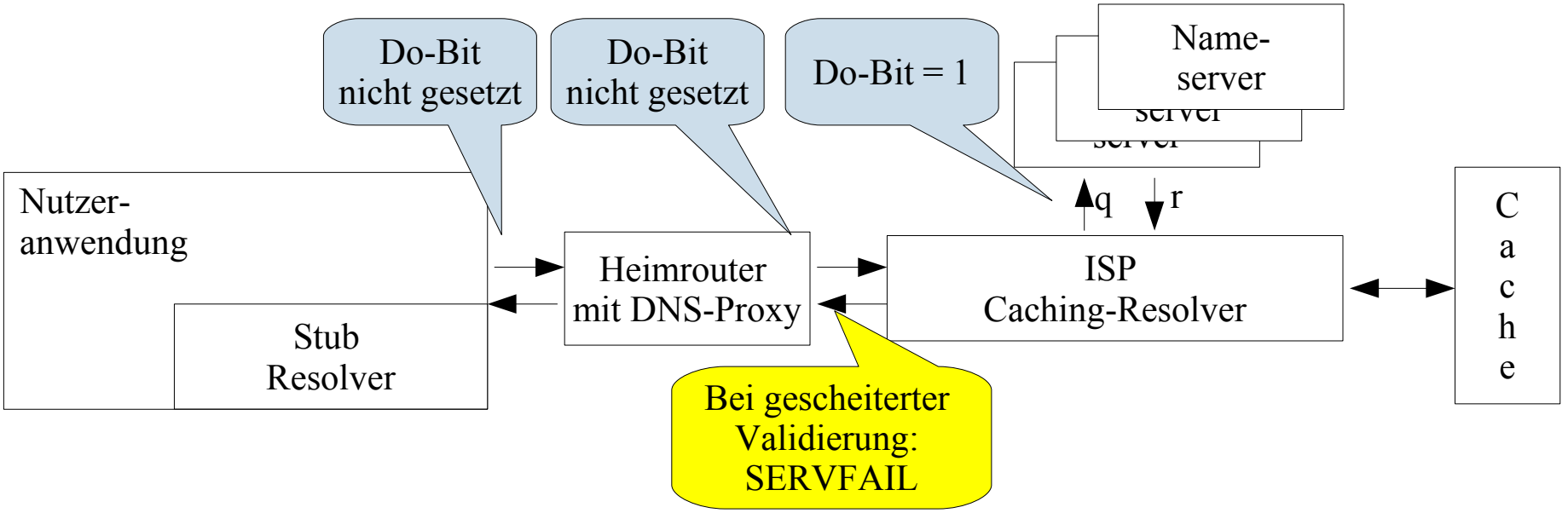
- RFC 1035:
  Beschränkung der Paketgröße auf 512 Bytes für DNS
- RFC 2671, EDNS0:
  Erweiterungsmechanismus für DNS, wurde 1999 spezifiziert
- Ermöglicht die Übertragung von UDP-Paketen >512 Byte
- Abwärtskompatibel über Handshake-Verfahren
- Falls Antwort nicht in signalisierte maximale Paketgröße passt, wird in Antwort TC (**T**run**c**ated) Bit gesetzt
- DNSSEC DO-Bit in EDNS0-Header definiert

Unterschiede DNS / DNSSEC

	DNS	DNS + DNSSEC
Größe Antwortpaket	< 512 Byte	Häufig > 512 Byte
DNSSEC-spezifische Header-Bits	-	Neue Bits: DO-Bit AD-Bit CD-Bit
EDNS0	i.d.R. Nicht erforderlich	Erforderlich zur Übertragung von DO-Bit und UDP-Antwortpaketen > 512 Byte
DNS-Abfragen per TCP	i.d.R. Nicht erforderlich	Alternative zu EDNS0

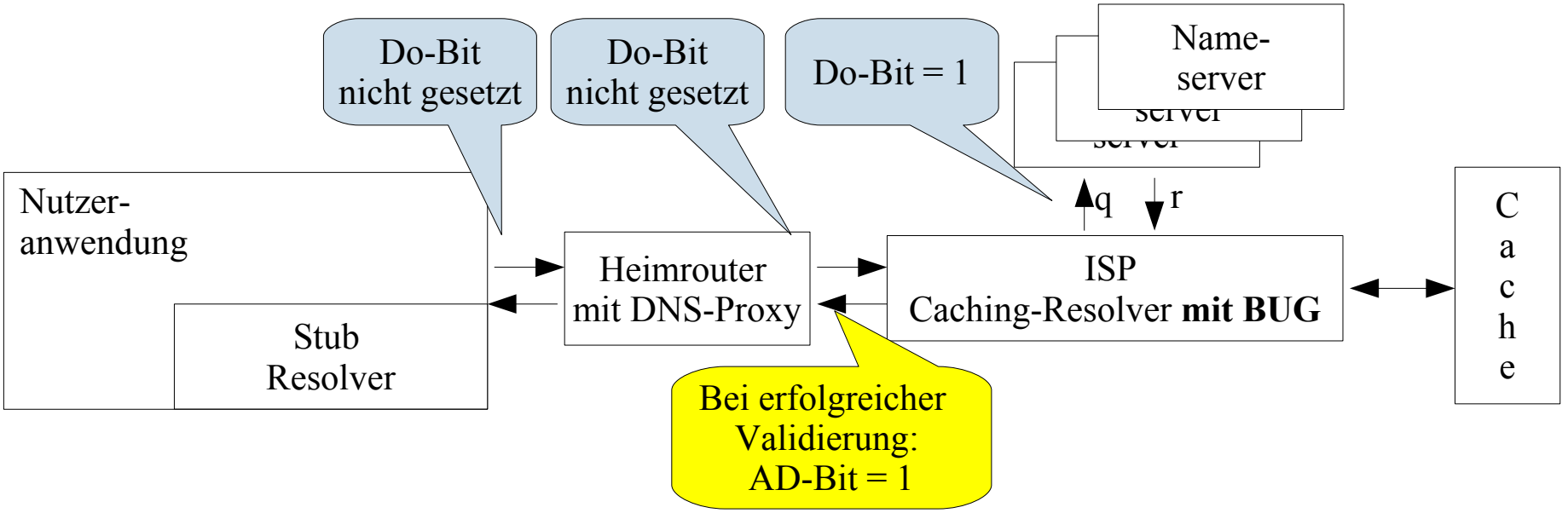
Testszenarien
1a. Abwärtskompatibilität

- DNSSEC-Validierung erfolgt durch Caching-Resolver des ISPs
  - → Client stellt DNS-Abfragen ohne DNSSEC-Bits
  - → DNS-Caching-Resolver liefert bei fehlgeschlagener Validierung SERVFAIL oder NXDOMAIN zurück
  - → Keine Veränderung an Hard- und Software des Kunden notwendig

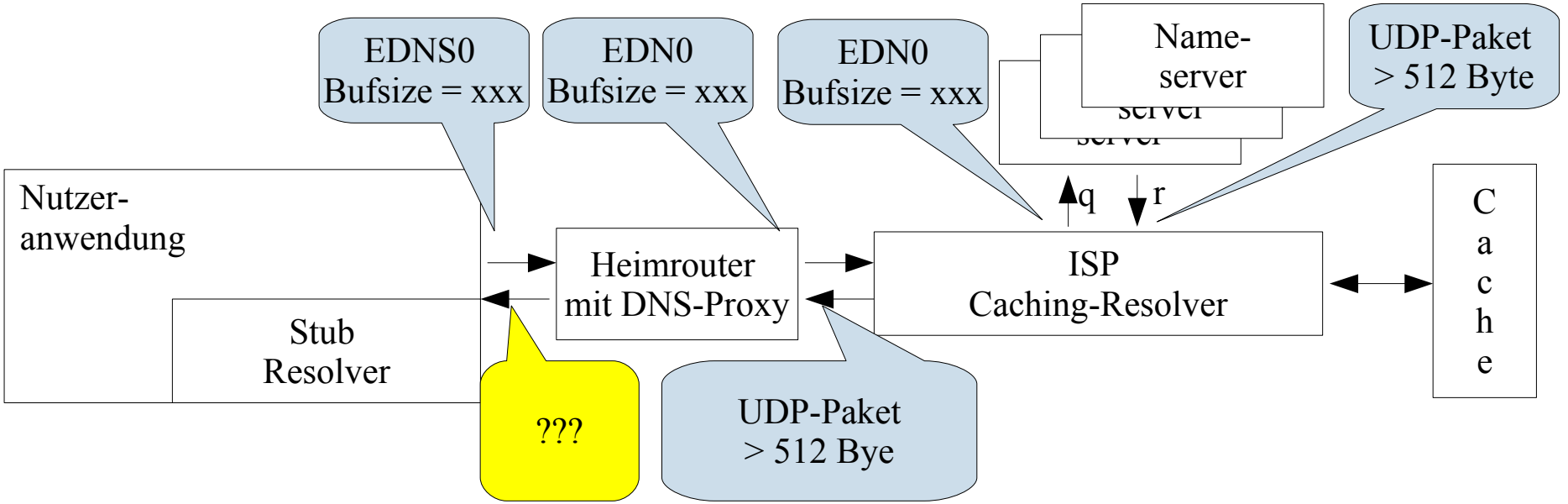


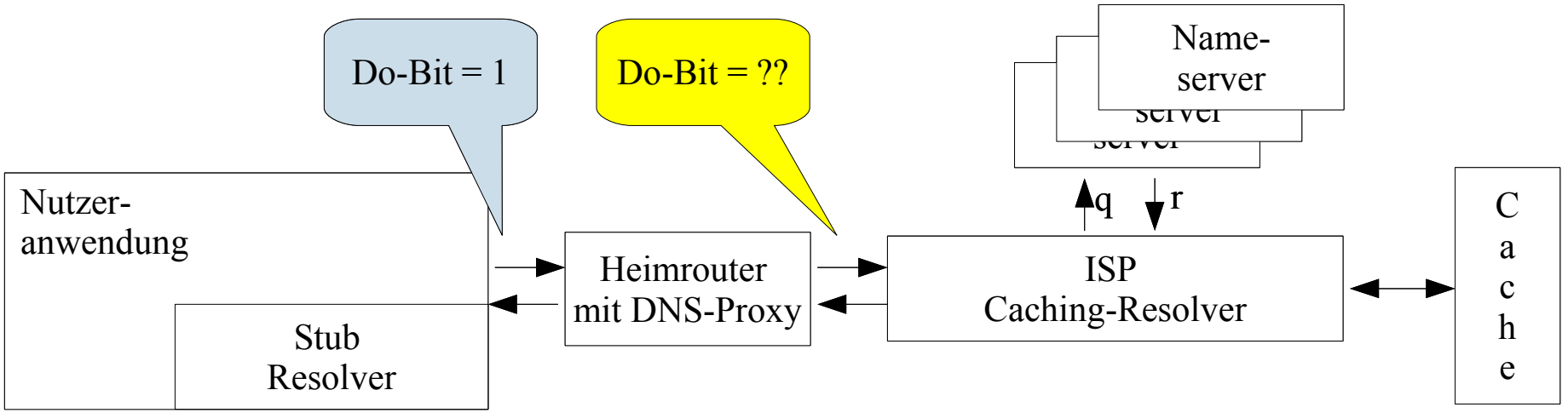
Testszenarien
1b. Abwärtskompatibilität - Spezialfall

- DNSSEC-Validierung erfolgt durch Caching-Resolver des ISPs
  - → Client stellt DNS-Abfragen ohne DNSSEC-Bits
  - → DNS-Caching-Resolver liefert bei fehlgeschlagener Validierung SERVFAIL oder NXDOMAIN zurück
  - → Keine Veränderung an Hard- und Software des Kunden notwendig



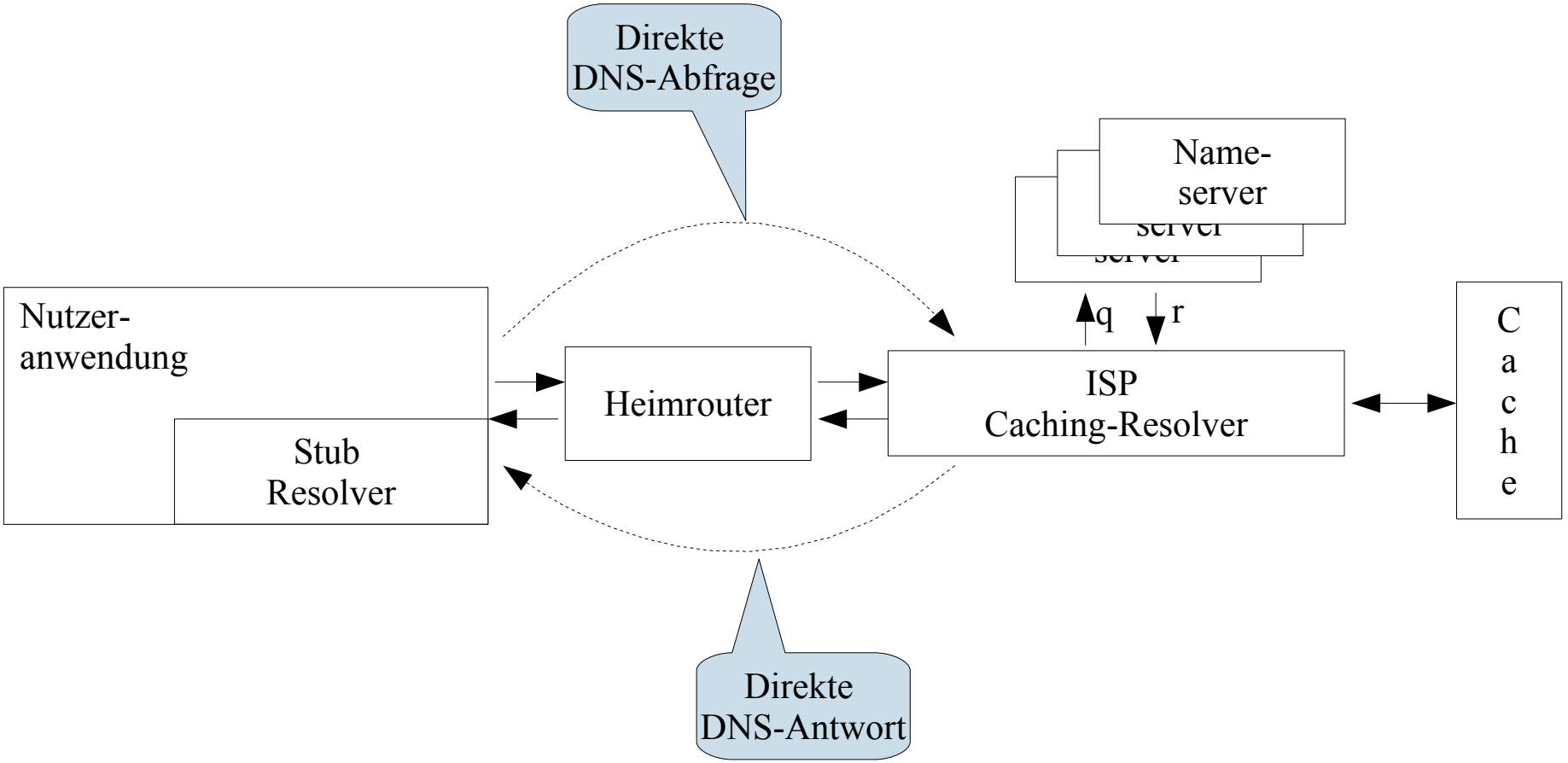
Testszenarien
2. DNSSEC-Unterstützung





Testszenarien
3. Direkte DNS-Abfragen

- Direkte DNS-Abfrage an den ISP Caching Resolver
  - Transparenz des Heimrouters?
  - Unterstützung einer solchen Konfiguration?



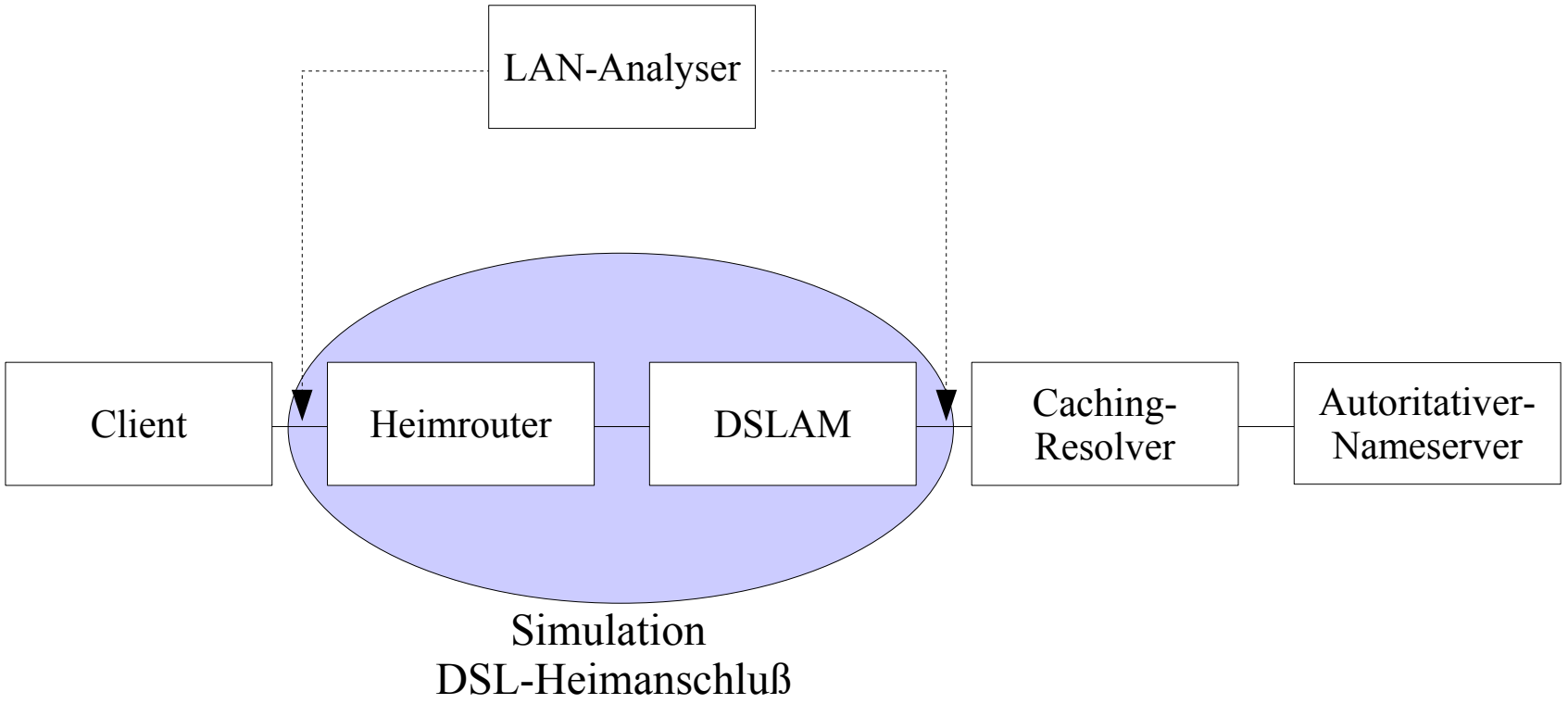
Durchgeführte Tests

- UDP und TCP-Unterstützung bei DNS-Abfragen
- EDNS0 Unterstützung
- Umgang mit DNSSEC-Flags
- Methodik:
  - Verschiedene Abfragen signierter und unsignierter Ressource-Records
  - Verwendung der Heimrouter als Proxy bzw. Router
- Weitere Sicherheitsaspekte:
  - Von außen offene Ports / Open Resolver
  - Port Randomisierung
  - IPv6 Unterstützung
  - WLAN Sicherheit
- Veröffentlichung der Studie in Kürze

Untersuchte Geräte

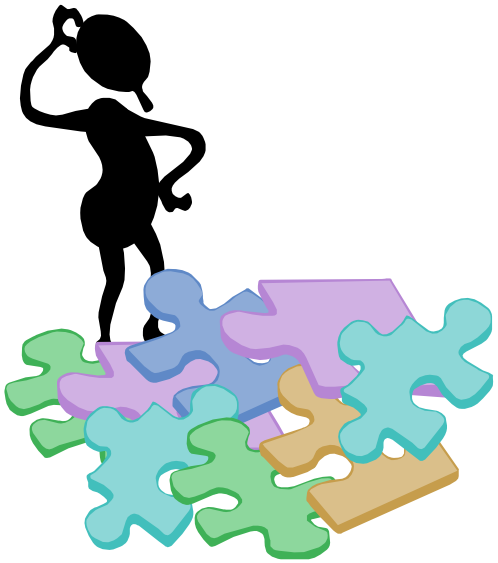
- Es wurden insgesamt 38 Heimrouter untersucht
- Davon 25 mit integriertem DSL-Modem
- Unterstützung der Studie durch verschiedene ISPs / Hersteller
- Vereinzelt gleiche Hardware mit unterschiedlichen Firmwareständen
- Studie berücksichtigt ca. 90% der zum Zeitpunkt der Marktrecherche im Zusammenhang mit DSL-Anschlüssen angebotenen Router
- Zusätzlich: Untersuchung einiger frei erhältlicher Geräte

Testaufbau

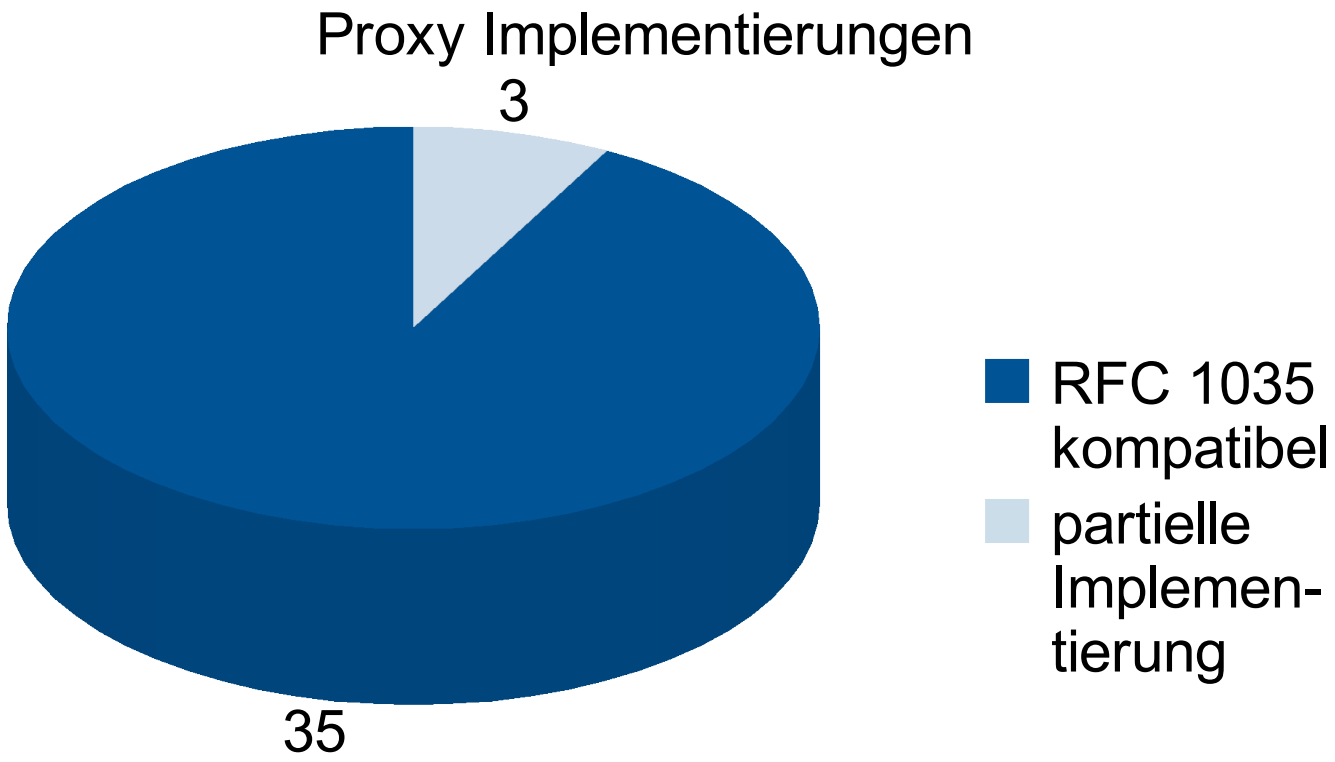

LAN-Analyser
Client
Heimrouter
DSLAM
Caching-
Resolver
Autoritativer-
Nameserver
Simulation
DSL-Heimanschluß

Inhalt

- Motivation
- Vergleichbare Studien
- Ziele
- Methodik
- Untersuchte Geräte
- Ergebnisse
- Fazit

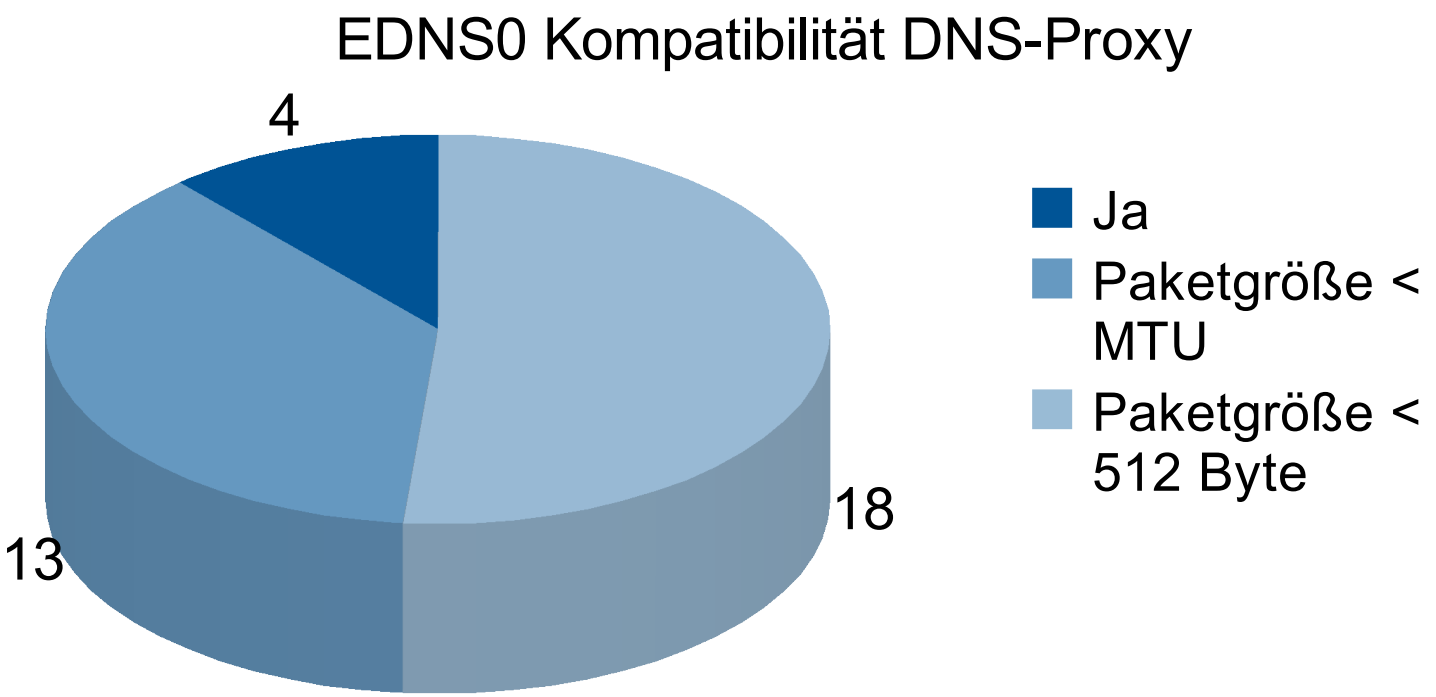


Testergebnisse
Proxy-Fähigkeit



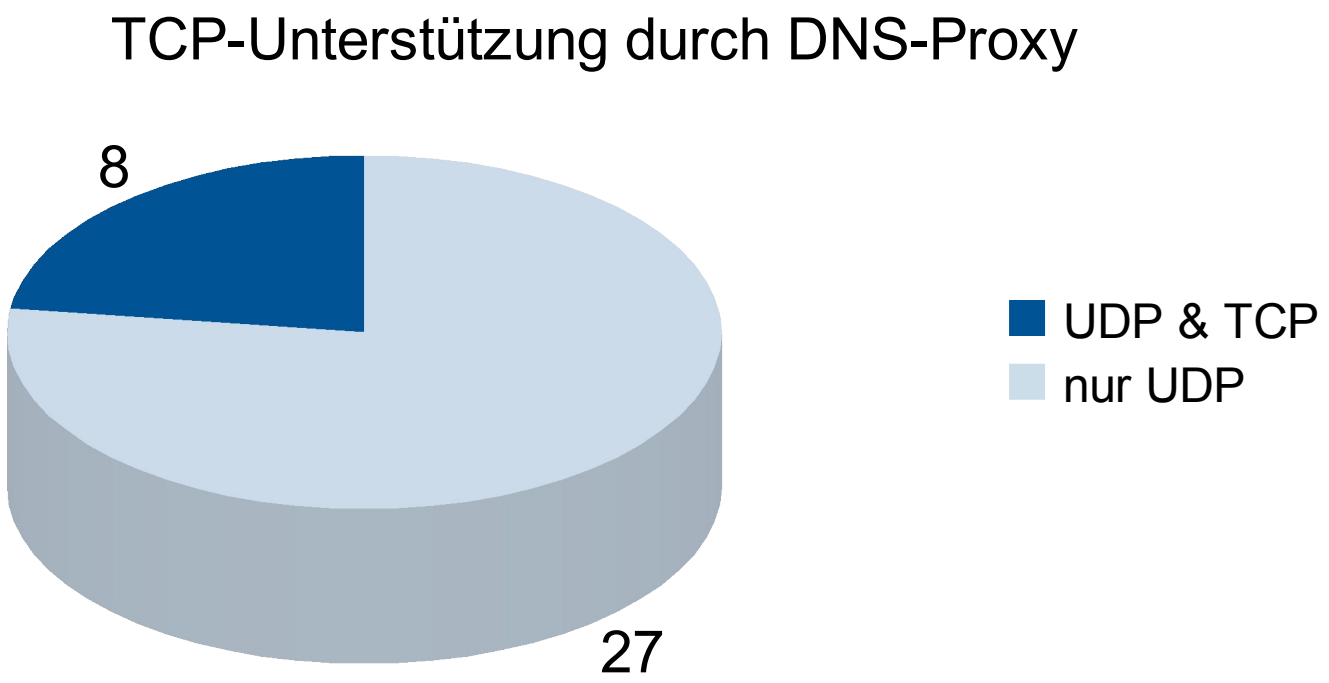
- 3 Geräte konnten nicht sämtliche Resource Records (RR) Typen verarbeiten
- Keine Berücksichtigung bei den weiteren Proxy-Tests

Testergebnisse
EDNS0-Kompatibilität



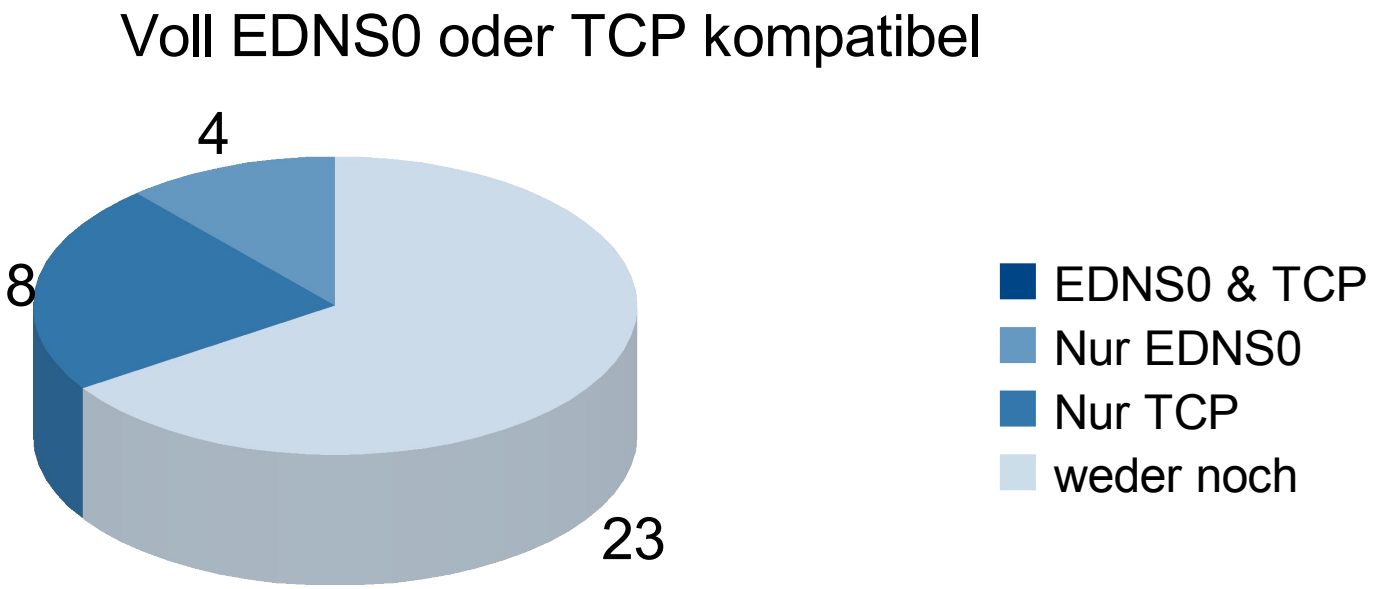
- Hauptprobleme:
  - Pakete wurden abgeschnitten
  - TC-Bit wurde nicht gesetzt oder weitergeleitet

Testergebnisse
TCP-Unterstützung



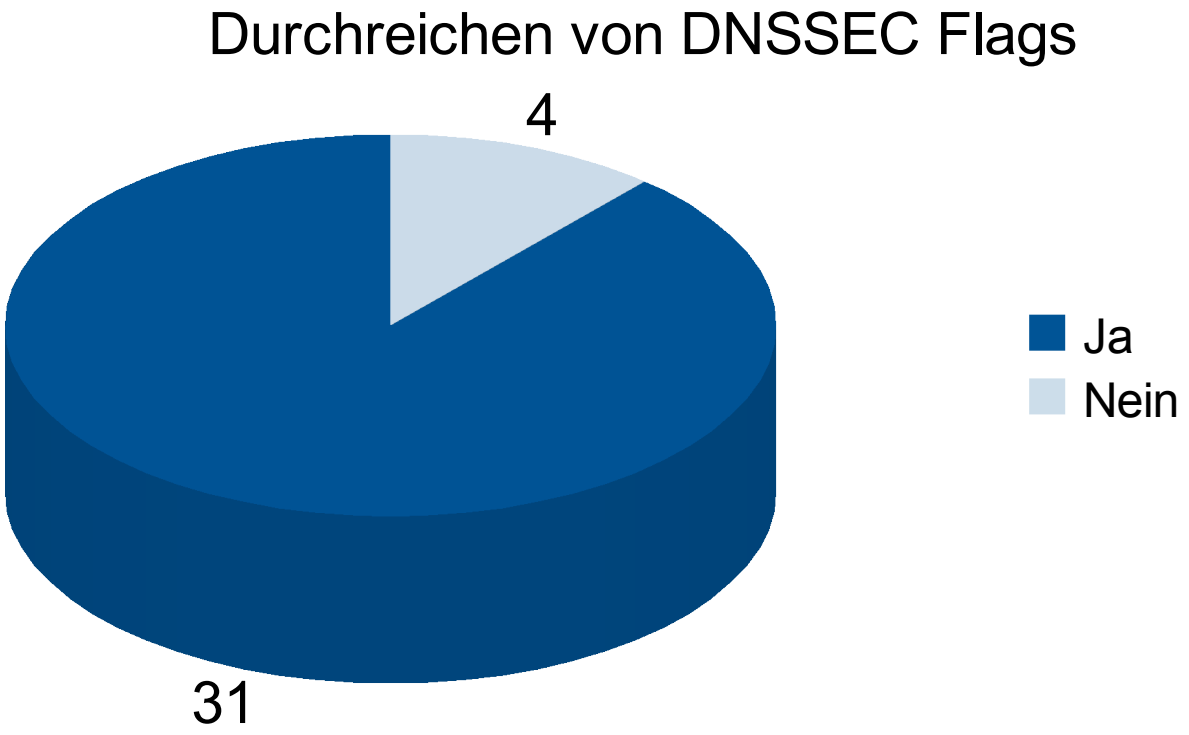
- Nur wenige DNS-Proxies der Heimrouter unterstützen TCP

Testergebnisse
EDNS0 oder TCP Kompatibilität



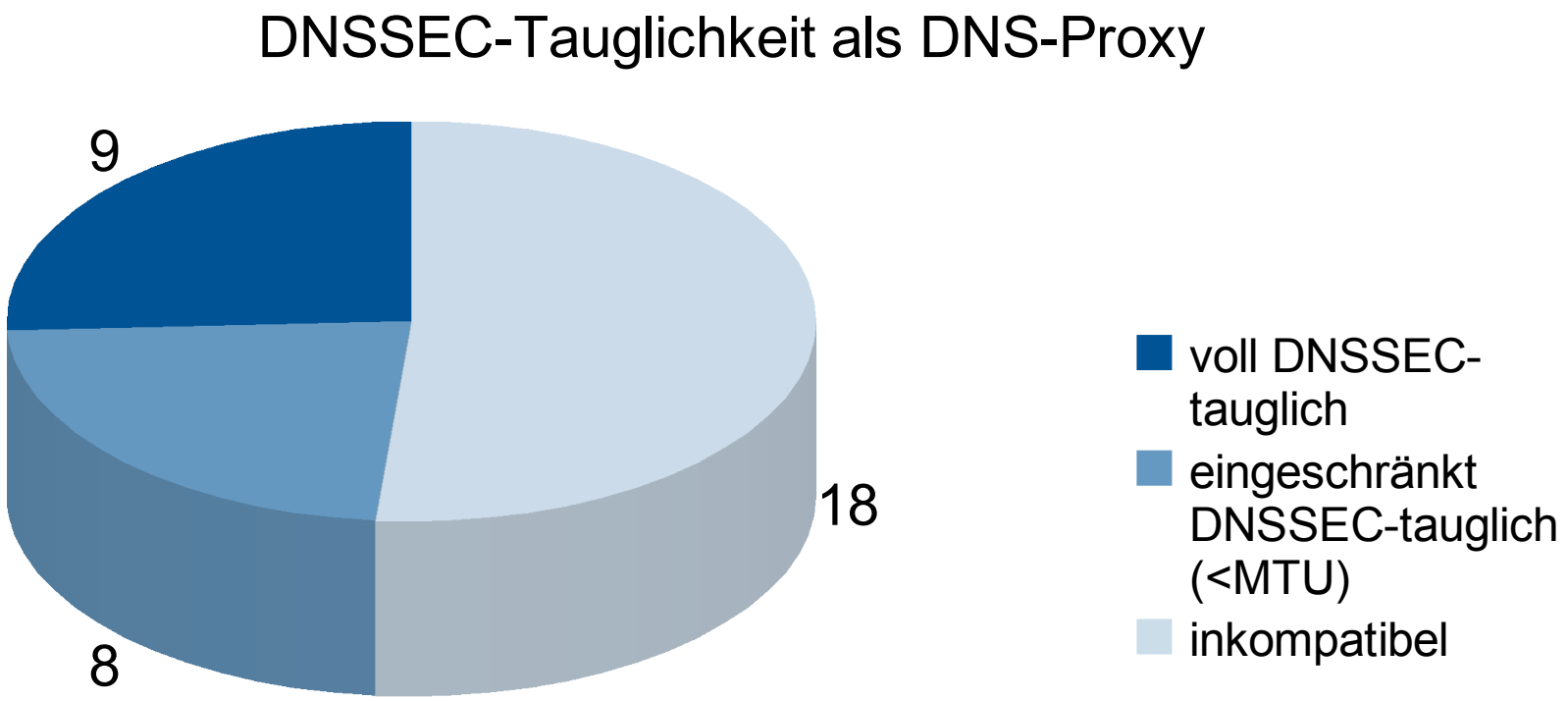
- kein Gerät war sowohl vollständig mit EDNS0 als auch mit TCP kompatibel

Testergebnisse
Kompatibilität DNSSEC-Flags



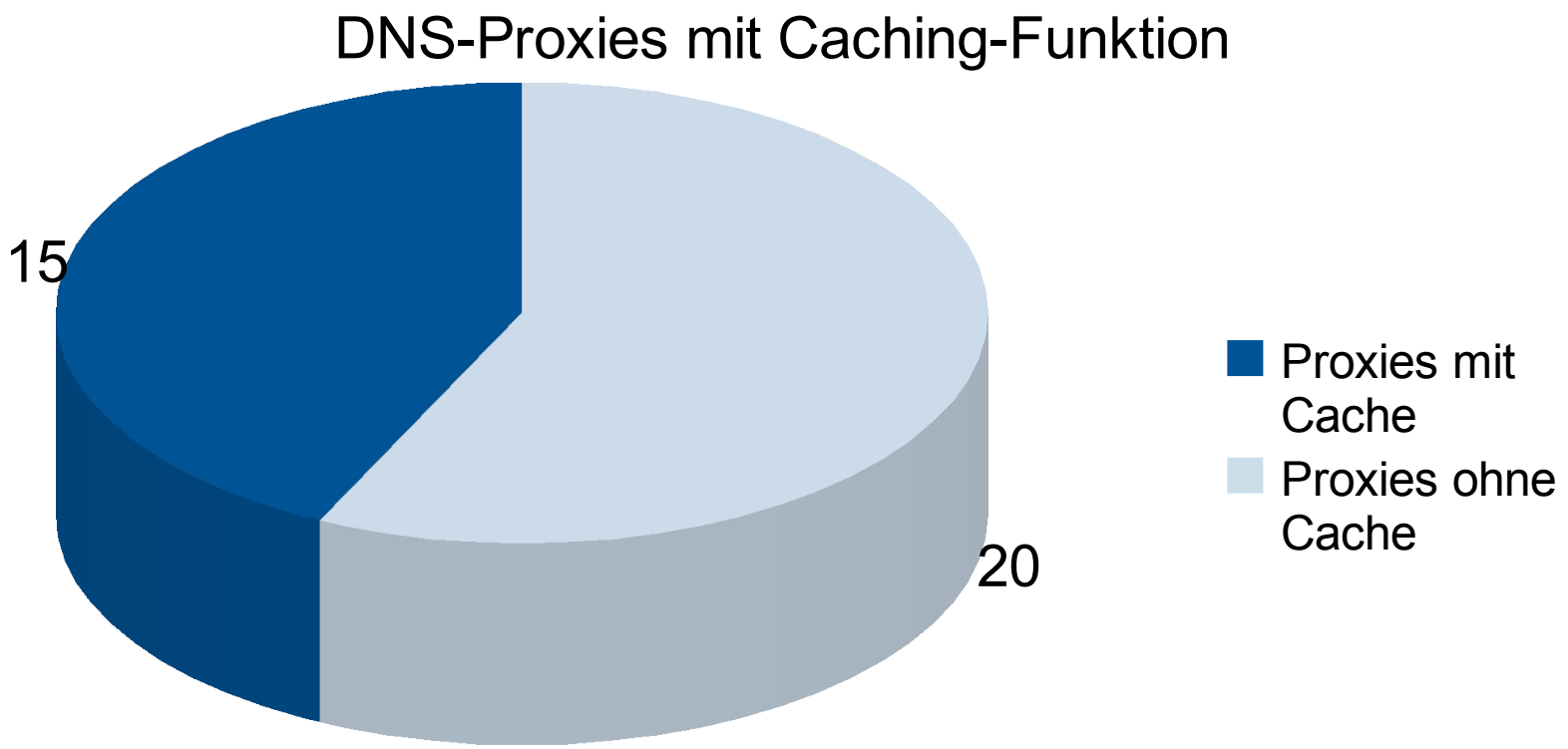
- Die meisten Geräte sind kompatibel mit den DNSSEC-Flags
- 3 Geräte verfälschen jedoch die Flags
- 1 Gerät lieferte „Connection Timeout“ bei gesetztem AD- oder CD-Bit zurück

Testergebnisse
Gesamtergebnis Proxy



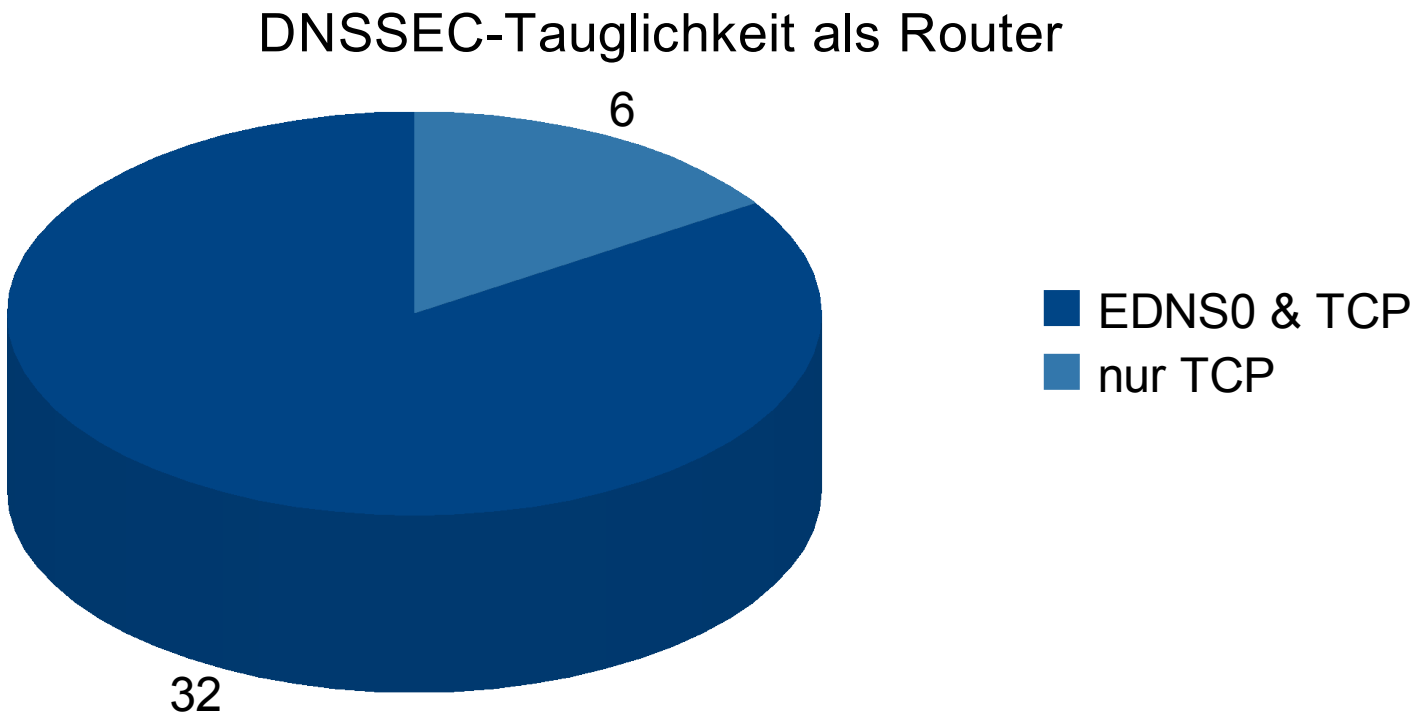
- Nur 9 von 38 getesteten Geräten / Firmwareständen sind bei Nutzung des eingebauten DNS-Proxies voll kompatibel mit DNSSEC
- Weitere 8 sind eingeschränkt kompatibel (Antwortpakete < MTU-Größe)

Testergebnisse
Proxy & Caching



- Proxies mit Caching-Funktion weisen Fehlverhalten bei DNSSEC-Abfragen auf, wenn zuvor eine Abfrage ohne DNSSEC-Flags erfolgt ist

Testergebnisse
Gesamtergebnis Router



- Alle getesteten Geräte sind bei Umgehung des eingebauten DNS-Proxies DNSSEC kompatibel
- Bei 6 der getesteten Geräten erfolgt jedoch ein Fallback auf TCP, da EDNS0-Pakete nicht in allen Fällen korrekt geroutet werden

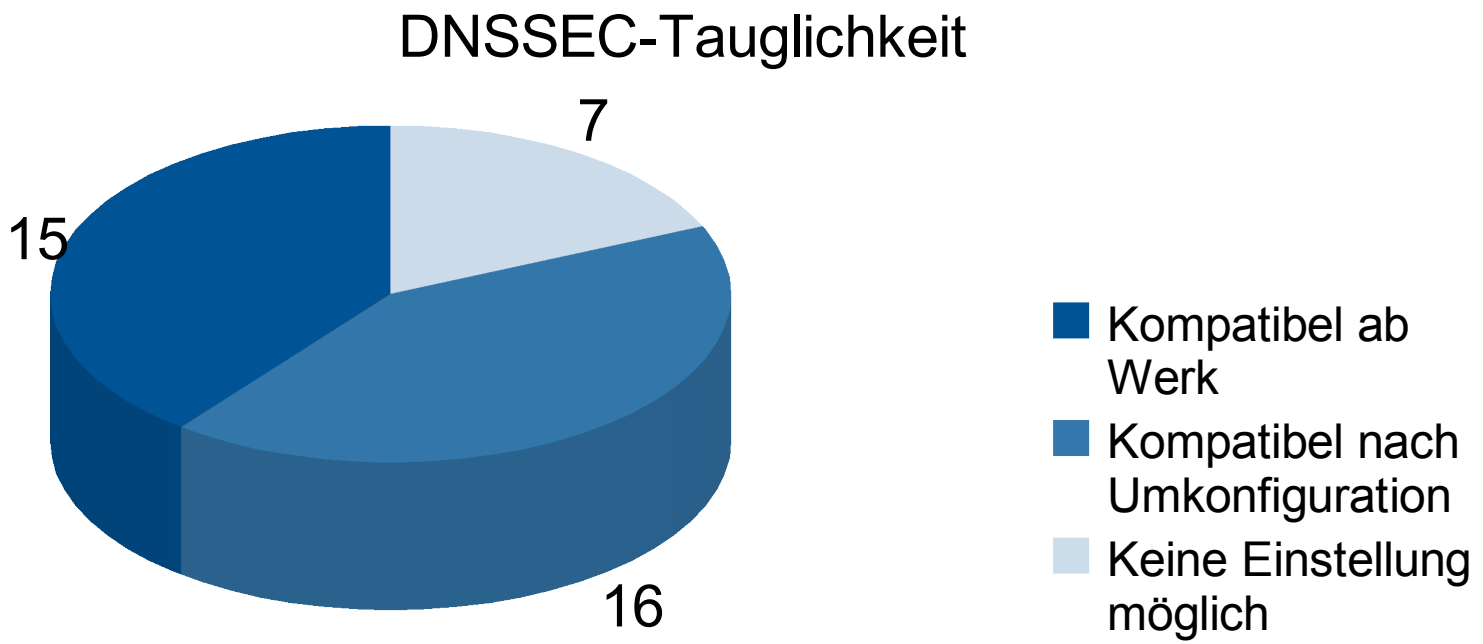
Testergebnisse
Manuelle Konfiguration der DHCP-Nameservereinträge

- Manuelle Konfigurationsmöglichkeit der per DHCP übermittelten Nameserver:

	Per DHCP übermittelter DNS-Server manuell einstellbar	Per DHCP übermittelter DNS-Server nicht manuell einstellbar
Proxy DNSSEC tauglich	9 (Defaultwert Proxy: 9)	0
Proxy eingeschränkt DNSSEC tauglich	7 (Defaultwert Proxy: 5)	1 (Defaultwert Proxy)
Proxy nicht DNSSEC tauglich	11 (Defaultwert Proxy: 10)	7 (Defaultwert Proxy: 6)
Unvollständige Proxy-Implementierung	2 (Defaultwert Proxy: 1)	1 (Keine DHCP-Übermittlung)

- Bei 7 der nicht DNSSEC Proxy-fähigen Geräte lässt sich der per DHCP übermittelte Nameserver nicht manuell einstellen

Testergebnisse
DNSSEC-Tauglichkeit



- 15 Router sind ab Werk DNSSEC kompatibel, da entweder der Proxy DNSSEC unterstützt oder per DHCP die ISP Nameserver ausgeliefert werden
- 16 Router können DNSSEC kompatibel konfiguriert werden
- 7 Router bieten keine Konfigurationsoption für die per DHCP übermittelten Nameserver

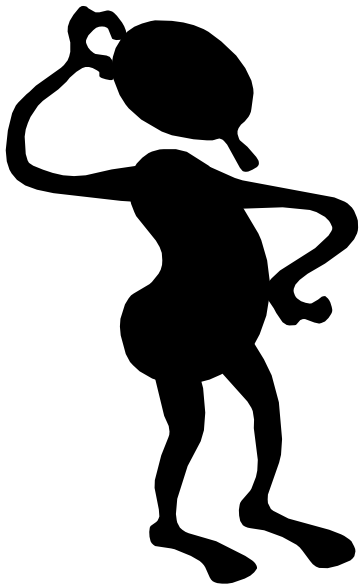
Zusammenfassung

- 9 von 38 Geräten können als DNS-Proxy im Zusammenhang mit DNSSEC ohne Einschränkung verwendet werden.
- 5 dieser Geräte verwenden die Implementierung DNSMASQ.
- Die DNS-Proxies 8 weiterer Geräte sind eingeschränkt DNSSEC tauglich (bei Antwortpaketen < MTU-Größe).
- Die mangelnde Unterstützung der anderen Geräte liegt in den meisten Fällen an fehlendem EDNS0-Support in Verbindung mit gleichzeitig nicht vorhandenem TCP-Support.
- Alle getesteten Geräte sind bei Umgehung des eingebauten DNS-Proxies DNSSEC kompatibel. Allerdings ist bei 7 Geräten eine manuelle Konfiguration der DNS-Server auf jedem angeschlossenen Gerät erforderlich, da der eingebaute DHCP-Server nicht entsprechend konfiguriert werden kann.

Vergleich mit den .se und .uk Studien

	.se	.uk	.de
EDNS0 kompatibel	3/10	4/22	4/35
TCP-Support	3/10	1/22	8/35
DNSSEC-Flag Support	7/10	16/22	31/35
DNSSEC kompatibel als Router	-	24/24	38/38
DNSSEC kompatibel ab Werk	3/12 (25%)	6/24 (25%)	15/38 (39%)
DNSSEC kompatibel nach Umkonfiguration	-	9/24 (38%)	16/38 (42%)

Vielen Dank für die Aufmerksamkeit!



Fragen?

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Thorsten Dietrich
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5947
Fax: +49 (0)22899-10-9582-5947

Thorsten.Dietrich@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de