DNSSEC

ISPA Academy, DNSSEC Workshop, 21.11.2012
Otmar Lendl <lendl@nic.at>

Programm

- Warum DNSSEC
- Wie funktioniert DNSSEC
- Internationaler Stand der Dinge
- Technische Probleme
- Policy Implikationen

Danke an Michael Braunöder, Olaf Kolkman, Phil Regnauld, … für die Erlaubnis, aus ihren Slides zu zitieren.

Vorstellungsrunde

- Otmar Lendl
  - Ehemals Ping/Eunet/KQ/Eunet/…
  - Seit 2002 bei nic.at
  - Seit 2008 Teamleader CERT.at
- Teilnehmer?
  - Techies?
  - Produktmanager?
  - GF?
- Das ist ein Workshop, kein Kino.

3

DNS: Was ist das?

- Global, distributed Database
- Input: Domain name
- Output: Resource Record **Sets**
  - A, AAAA — IP addresses
  - MX — Mail routing
  - CNAME — Aliasing
  - NS — Delegation
  - PTR, NAPTR, SRV,
  - RRSIG, DS, NSEC, NSEC3
- Transport: mainly UDP
- Lots of caching

4

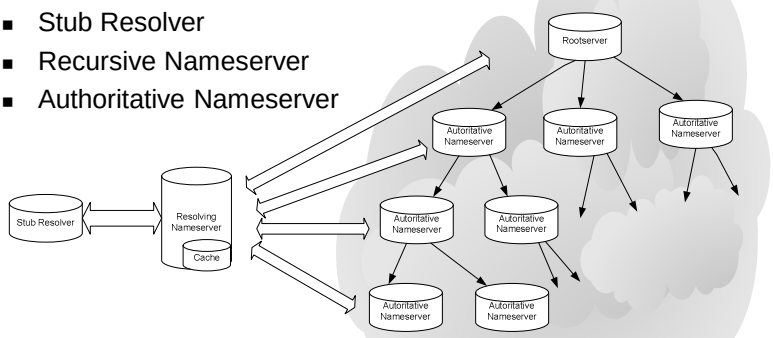
Integrität des DNS: Wozu?

- DoS
- Man-in-the-middle almost *everything*
  - Phishing
  - Email hijacking
- Password reset emails
- Software Updates
- SSL and PKI for the rescue?
  - How do users react to X.509 errors?
  - CA email-loop
  - CA whois lookup
- Für den Enduser ist „DNS kaputt“ nicht von „Internet kaputt“ unterscheidbar.

5

Mitspieler

- Stub Resolver
- Recursive Nameserver
- Authoritative Nameserver

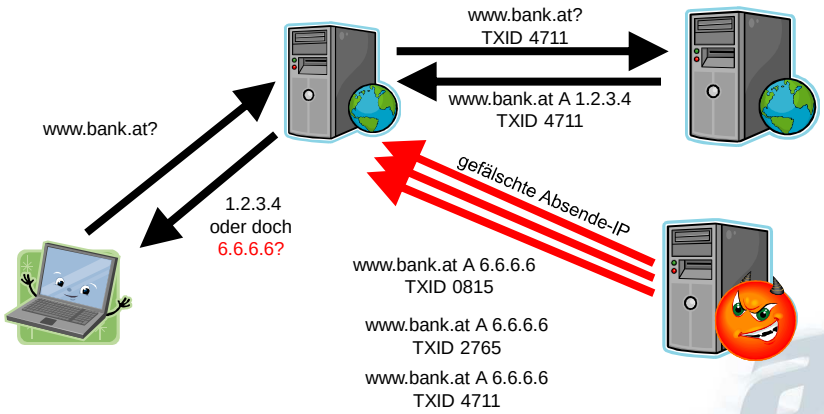


Resolution ist nur das halbe Spiel: Provisioning ist auch wichtig!

Ausführliche Gefahrenanalyse in RFC 3833.

6

DNS Cache Poisoning



7

Cache Poisoning (on-path)

- Trival und weit verbreitet
- Politische Gründe
  - Iran, China, …
  - „DNS-Sperren“
- Geld
  - NX-Domain monetizing

8

Cache Poisoning (off-path)

- Das ist nichts neues.
  - Kashpureff
  - Triviale Query-ID
  - Parallele Anfragen
- Berechnungen zur Erfolgswahrscheinlichkeit in RFC 5452

Security?

This is the safety net

```
$ dig cert.at MX
[…]
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8861
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;cert.at.                       IN      MX
```

16 bits of entropy might have been enough in 1987, but not in 2008.

Pre-Kaminsky

- An attack needs to match
  - Question section
  - The ID field
  - IP address of the nameserver queried
  - IP address / port from which the query was sent
- How often can an attack take place?
  - Each query from a recursor starts a race.
  - Forcing a query helps the attacker
  - The cache limits attacks to once per Time-To-Live for the same query

11

Attacking www.example.org

```
;; QUESTION SECTION:
;345678.example.org.          IN      A

;; ANSWER SECTION:
345678.example.org.  3600     IN      A       192.0.2.1

;; AUTHORITY SECTION:
example.org.         100000   IN      NS      ns1.evil.net.
example.org.         100000   IN      NS      ns2.evil.net.
```

Neue Nameserver für example.org

Source: IETF namedroppers list. (P. Koch, T. Finch)

12

Oder ...

```
;; QUESTION SECTION:
;345678.www.example.org.            A

;; AUTHORITY SECTION:
www.example.org.     NS ns1.evil.net.
www.example.org.     NS ns2.evil.net.
```

Zonecut bei www.example.org

13

... oder ...

```
;; QUESTION SECTION:
;345678.example.org.          IN    A

;; ANSWER SECTION:
345678.example.org.      CNAME www.example.org.
www.example.org.         A     192.0.2.80  ; evil
```

CNAME chaining auf www.example.org

14

Die Story geht weiter

- Amir Herzberg / Haya Shulman 2012
  - Effekte von NATs auf Port-Randomization
  - Ausnutzen von Fragementation

15

DNSSEC

- DNS Security Extension
- Paul Vixie:
  „DNSSEC is an Internet Standard meaning that it came from IETF, took years longer than it should have, has some features that almost nobody now remembers the reason for, and lacks some features that almost everybody wishes it had. So, it‘s a lot like IPv6 or IPSEC. And yet, it works.“

16

DNSSEC

- Details zum Nachlesen:
  - RFC4033, “DNS Security Introduction and Requirements” (2005)
  - RFC4034, “Resource Records for the DNS Security Extensions”
  - RFC4035, “Protocol Modifications for the DNS Security Extensions”
  - RFC5011, “Automated Updates of DNS Security (DNSSEC) Trust Anchors“
  - RFC5155, “DNS Security (DNSSEC) Hashed Authenticated Denial of Existence” (2008)
- 1. Versuch war schon RFC 2535 (1999)

17

Welche Security?

- Confidentiality
  - Kann wer mitlesen?
- Integrity
  - Stimmt das, was ich bekommen habe?
- Availability
  - Bekomme ich überhaupt eine Antwort?

DNSSEC betrifft ausschließlich „Integrity“!

18

Grundidee

- Kompatible Erweiterung des DNS
- Public Key Kryptografie Signaturen innerhalb der DNS Antworten
- Schutz der Daten, nicht Schutz des Transports
- Delegationshierarchie des DNS wird auch zur Trust-Hierarchie
- Hat mit X.509 **nichts** zu tun.

19

New Resource Records

- Three Public key crypto related RRs
  - RRSIG — Signature over RRset made using private key
  - DNSKEY — Public key, needed for verifying a RRSIG
  - DS — Delegation Signer; 'Pointer' for building chains of authentication
- Two RR for internal consistency
  - NSEC — Indicates which name is the next one in the zone and which typecodes are available for the current name.
  - NSEC3 — NSEC++

20

RRSIG – Signature

- 16 bits - type covered
- 8 bits - algorithm
- 8 bits - nr. labels covered
- 32 bits - original TTL
- 32 bit - signature expiration
- 32 bit - signature inception
- 16 bit - key tag
- signer's name

RRSIGs gelten nicht ewig!

Absolute Zeit

```
nlnetlabs.nl.  3600 IN  RRSIG   A 5  2 3600  (
            20050611144523 20050511144523  3112 nlnetlabs.nl.
            VJ+8ijXvbrTLeoAiEk/qMrdudRnYZM1VlqhN
            vhYuAcYKe2X/jqYfMfjfSUrmhPo+0/GOZjW
            66DJubZPmNSYXw== )
```


DNSKEY – Public Key

- 16 bits: FLAGS
- 8 bits: protocol
- 8 bits: algorithm
- N*32 bits: public key

```
nlnetlabs.nl. 3600 IN DNSKEY  256 3 5 (
          AQOvhvXXU61Pr8sCwELcqqq1g4JJ
          CALG4C9EtraBKVd+vGIF/unwigfLOA
          O3nHp/cgGrG6gJYe8OWKYNgq3kDChN)
```

Delegation Signer (DS)

- Delegation Signer (DS) RR indicates that:
  - delegated zone is digitally signed
  - indicated key is used for the delegated zone
- Parent is authorative for the DS of the child's zone
  - Not for the NS record delegating the child's zone!
  - DS **should not** be in the child's zone
  - **ACHTUNG**: DNSSEC hinter non-DNSSEC-aware Recursor macht Probleme.

DS – Key of Subdomain

- 16 bits: key tag
- 8 bits: algorithm
- 8 bits: digest type
- 20 bytes: SHA-1 Digest

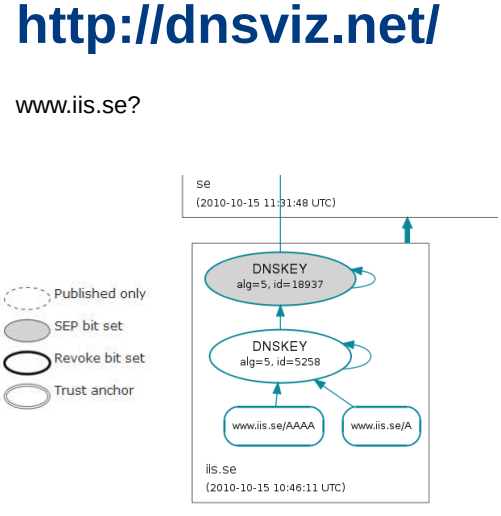
```
$ORIGIN nlnetlabs.nl.
lab.nlnetlabs.nl.   3600 IN   NS  ns.lab.nlnetlabs.nl
lab.nlnetlabs.nl.   3600 IN   DS  3112   5  1 (
                                   239af98b923c023371b52
                                   1g23b92da12f42162b1a9
                                 )
```

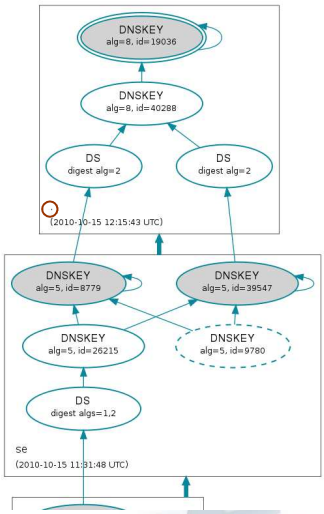
Nyckelsigneringsnyckel

- Lange Schlüssel
  - Sicherer -> weniger Schlüsselwechsel notwendig (weniger Interaktion mit übergeordneter Stelle (Registry, IANA) notwendig -> weniger Fehlermöglichkeiten
  - Signieren dauert länger
  - Das signierte Zonefile wird größer
- Kurze Schlüssel
  - Weniger sicher -> häufigere Schlüsselwechsel notwendig (mehr Interaktion mit übergeordneter Stelle notwendig -> mehr Fehlermöglichkeiten
  - Signieren geht schneller
  - Das signierte Zonefile wird kleiner
- Lösung: Key Signing Key + Zone Signing Key

http://dnsviz.net/

www.iis.se?





Problem: Beweis von Nicht-Existenz

- Wie kann man beweisen dass etwas nicht existiert (und das möglichst für den Client überprüfbar)?
  - generelles, signiertes NXDOMAIN nicht möglich (Replay-Attacke)
  - offline generieren aller möglichen Anfragen und signieren der möglichen Antworten nicht praktikabel
  - On-the-fly Signierung der Antworten bietet DoS-Potential und Sicherheitsrisiko (Private Schlüssel auf allen Nameservern)
- Lösung: Man beweist die Löcher.
  - Einfach: NSEC
  - Zone enumeration problem, daher NSEC3

NSEC – Proof of non-existance

- FQDN: Next Name in Zone
- N*32 bit map: RRTypes present

```
www.nlnetlabs.nl. 3600 IN   NSEC z.nlnetlabs.nl. A RRSIG NSEC
```

NSEC Records

- NSEC RR provides proof of non-existence
- Not only for names, but also for RR-Types
- If the servers response is Name Error (NXDOMAIN):
  - One or more NSEC RRs indicate that the name or a wildcard expansion does not exist
- If the servers response is NOERROR:
  - And empty answer section
  - The NSEC proves that the QTYPE did not exist
- More than one NSEC may be required in response
  - Wildcards
- NSEC records are generated by tools
  - Tools also order the zone

29

NSEC Walk

- NSEC records allow for zone enumeration
- Providing privacy was not a requirement at the time
- Zone enumeration is a deployment barrier

- Solution is developed: NSEC3
  - RFC 5155
  - Complicated piece of protocol work
  - Hard to troubleshoot
  - Only to be used over Delegation Centric Zones
  - Opt-out Feature

30

DNSSEC Packets

- DO
  - DNSSEC OK (EDNS0 OPT header) to indicate client support for DNSSEC options
  - EDNS0 is required for DNSSEC
- CD
  - “Don’t check signatures for me, just give me the raw DNSSEC records”
- AD
  - Authenticated Answer

31

Deployment Server-side

- Key management
  - Generate keys
  - Add DNSKEY records
- Sign zone
  - Signing & serving need not be performed on same machine
  - Signing system can be offline
- Make sure authoritative nameservers handle DNSSEC
- Communicate your keys to parent zone

32

Deployment Client-side

- Stub-Resolver speaks DNSSEC
  - Inefficient
  - Slow rollout
  - Upsides in User-Interface
- Recursor does DNSSEC Validation
  - Need a way to secure last hop
  - Huge multiplier possibilities
- Secure Entry Points?
  - Signed Root helps

33

2010: Das Jahr in dem „.“ signiert wurde

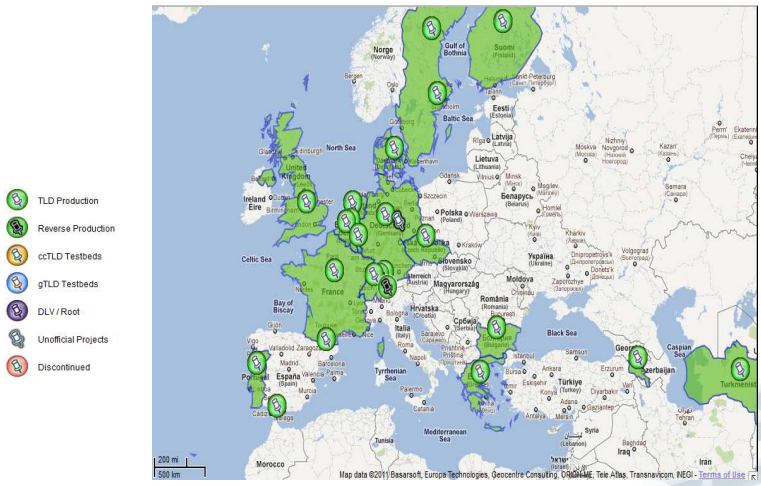
- Langer (politischer) Streit um „wer hat die Keys der Root“
- 3. Juni 2009: Einigung
  - http://www.icann.org/en/announcements/announcement-2-03jun09-en.htm
  - ICANN hat KSK
  - DoC macht weiterhin Freigabe von Changes
  - Versign hält den ZSK und signiert
- http://www.root-dnssec.org/
- Root ist seit 15. Juli 2010 signiert.

34

Deployment-Statistiken?

- http://www.internetsociety.org/deploy360/dnssec/statistics/
- http://secspider.cs.ucla.edu/
- http://scoreboard.verisignlabs.com/
- http://www.huque.com/app/dnsstat/
- https://xs.powerdns.com/dnssec-nl-graph/
- http://www.xelerance.com/dnssec/
- https://www.dnssec-deployment.org/

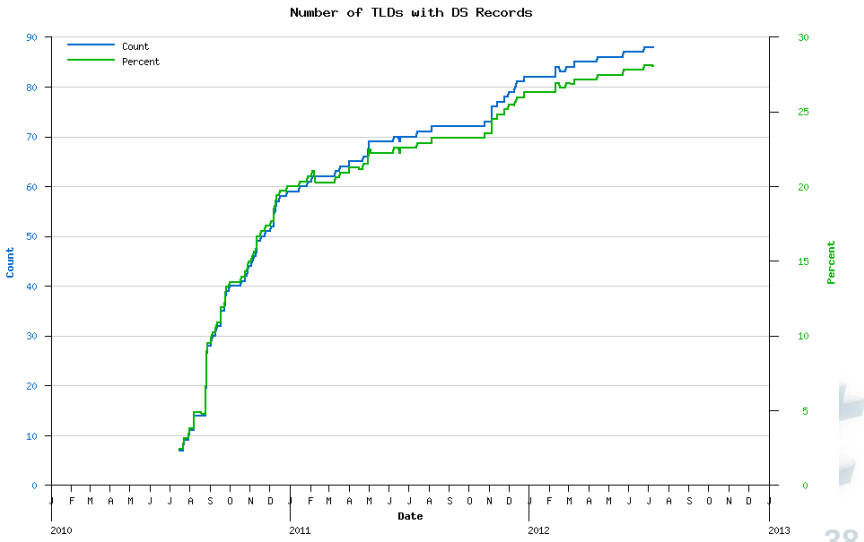
Status 2011/09



Quelle: Paul Wouters, http://www.xelerance.com/dnssec/

Animiert

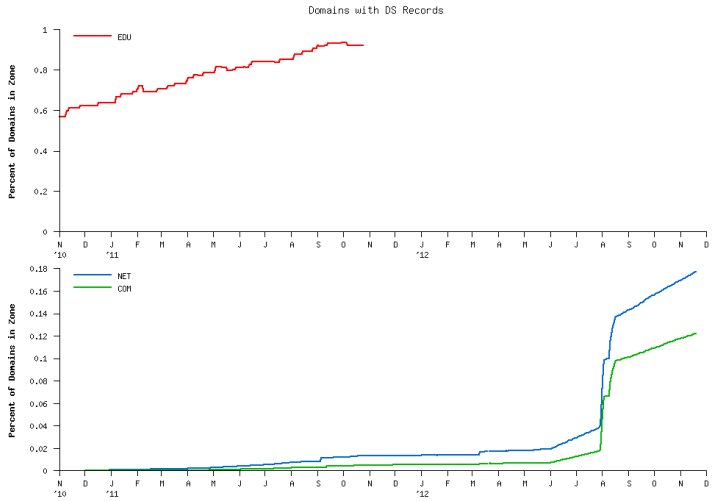
37



38

nic.at
the austrian registry

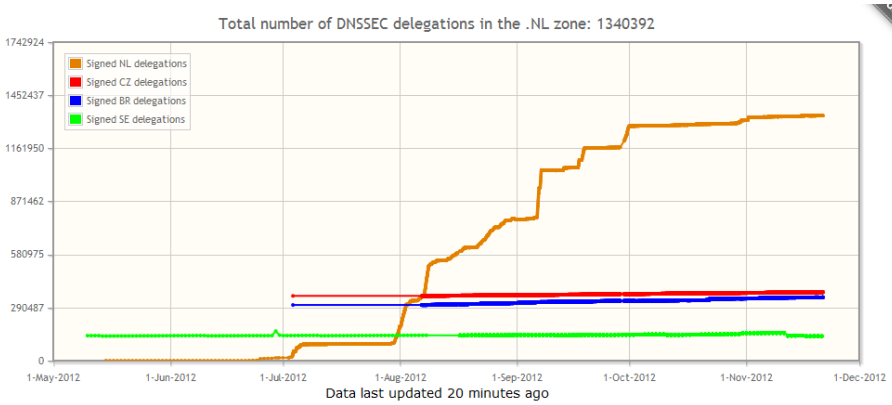
http://scoreboard.verisignlabs.com/percent-trace.png



39

nic.at
the austrian registry

ccTLDs:



https://xs.powerdns.com/dnssec-nl-graph/

40

Policy Side

- Das Protokoll ist komplex, aber beherrschbar
- Die Software wird laufend besser

- Aber: Welche Grundannahmen des DNS-Operating kollidieren mit DNSSEC?

41

Sicherheit vs. Verfügbarkeit

- Plain DNS ist robust
  - Sehr fehlertolerant
  - Oft komplett auf Autopilot
- DNSSEC ist spröde
  - Ein falsches Bit und die Zone ist offline.
  - Kompetentes Operating nötig.
  - DNSSEC nicht unüberlegt einführen!
  - Fehler werden passieren.

42

Wen hat es schon erwischt?

- Diverse .gov Domains
- .arpa (Juni 2010)
- mozilla.org (September 2011)
- .uk (September 2011)
- .be (Oktober 2011)
- .th (November 2011)
- .fr (Februar + März 2011)
- ripe.net / 0.a.2.ip6.arpa (April 2011)
- ip6.arpa (16. Mai 2011)
- Fortsetzung folgt bestimmt

43

Caching

- Bekanntes Problem:
  - Vor Änderungen TTL runtersetzen
- Mit DNSSEC deutlich böser:
  - Bei allen Änderungen (key rollover, …) muss man bedenken, welche alte DS und RRSIG Records noch in den Caches sind.
  - DNSSEC abschalten geht nicht einfach so.

44

Registrarmodell

- Registry
- Registrar
- Registrant

- Wo ist da der Nameserverbetreiber?

45

Woher kommt der DS Record?

- Wer erzeugt den DNSKEY?
- Wer kann mit der Registry sprechen?

- Technisch einfach:
  - Erweiterung von EPP (RFC5910)
- Aber sonst?
  - Rechtliches (Haftung!)
  - Process?
  - Soll die Registry gemeldete DS testen?

46

Registrarwechsel?

- Unterstützt der neue DNSSEC?
- Rolle für die Registry?
  - DNSSEC Support vorschreiben?
  - Transfer verhindern?
  - Anderweitig reingreifen?

47

NS-Operator Wechsel

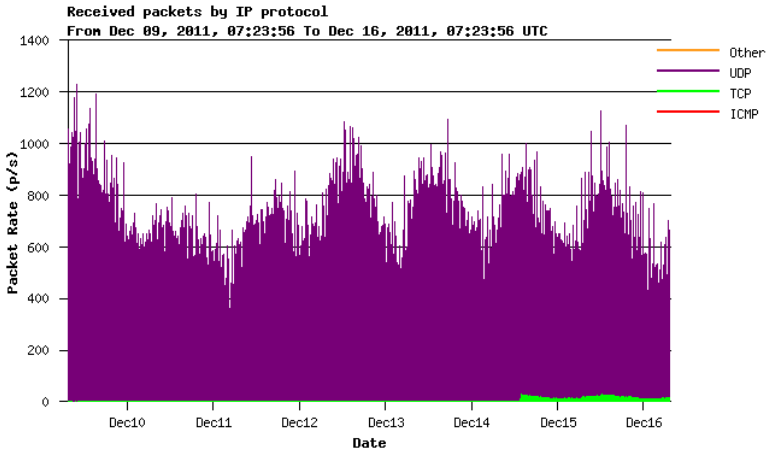
- NICHT Registrar-Wechsel!
- Ziel: Zone durchgehend signiert
  - Das ist NICHT trivial.
  - Geht ohne Kooperation des alten nicht

48

NS Change

- Step 1:
  - Losing and Gaining include both of sets of ZSK keys in their DNSKEY RRset.
  - Losing DNSKEY RRSET:
    - Losing KSK
    - Losing ZSK
    - Gaining ZSK
  - Gaining DNSKEY RRSET:
    - Losing ZSK
    - Gaining KSK
    - Gaining ZSK
- Step 2:
  - Parent adds Gaining KSK to DS, listing both KSKs
- Step 3: (actual transfer) (wait at least 1 DS TTL)
  - Parent updates NS from losing NS-set to gaining NS-set.

Packet Sizes



DNSSEC für den NS-Betreiber

- Software support?
- Wie groß wird das Zonefile?
- Wo signiere ich?
- Key-Management
- Automatisieren!
- Security der private keys?
  - Anforderungen wie an eine CA?
  - HSM
  - Pure Software-Lösungen
- Notfallsplanung nötig, da komplexe Abhängigkeiten.

51

Warnung!

- Schlüsselverwaltung ist Neuland für den typischen ISP / Registrar / Webhoster.
- Manuelle Prozesse funktionieren nicht!
- Gute Tools nötig
- Auch für debugging
- Schulungen!

52

Emergency Procedures

- Key Compromise
  - Emergency Rollover
- Probleme im Zonefile?
  - Siehe .se
  - Zonefiles in Reserve
- Notfallsplanung nötig, da komplexe Abhängigkeiten.

53

Kommerziell?

- Erfahrungen aus Schweden
  - Mehr Geld dafür verlangen funktioniert nicht.
- Tschechien
  - Einfach für alle Kunden aufdrehen.
- USA / .gov
  - Vorgeschrieben.
- Neue TLDs
  - ICANN verlangt DNSSEC support.

54

Business-case?

- DNSSEC ist kein Selbstläufer
- Kosten/Nutzen
  - Typische Privatdomain
  - e-Commerce
- Was kann ich an DNSSEC in Zukunft anhängen?
  - Ersatz für X.509?
  - ….

55

IETF DANE

- RFC 6394 (Use Cases)
  - CA Constraints
    - Welche CA sind zu erwarten?
  - Service Certificate Constraints
    - Welches Certificate/CA ist zu erwarten?
  - Trust Anchor Assertion and Domain-Issued Certificates
    - Selfsigned / Non-wellknown CA Certificate
  - Delegated Services
    - Outsourcing restrictions
- RFC 6698 (Protocol)

56

Recursors

- Last am Server
- Helpdesk Schulung
- Debugging Tools
- Was tun, wenn wichtige Zone Probleme mit DNSSEC hat?

57

Zusammenfassung

- Manipulationen des DNS sind **böse**
  - Siehe „ A brief History of DNS Hijacking“ auf https://www.icann.org/en/news/in-focus/dnssec/presentations
- Cache Poisioning ist **ein** Vektor dafür
  - Wer Software von vor 2008 einsetzt ist massiv gefährdet
  - Aktueller Recursor mit source port randomization ist gut geschützt
  - DNSSEC kann hier den Sack zumachen
- Aber …

58

Das DNS ist mehr als Port 53

- Fast alle Angriffe auf das DNS in den letzten Jahren waren
  - auf der Provisionierungsseite,
    - Registrar, Registry, …
  - on-path attacks
    - China, Iran, ..
  - oder am Client.
    - DNSChanger, Conficker, …
- Inklusive dem gelegentlich genannten Vorfall in Brasilien.
  - https://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil

Fragen?

Otmar Lendl
lendl@nic.at / lendl@cert.at