ISPA Academy

# DNSSEC

## in der Praxis

Datum:
21.11.2012

Michael Braunöder
R&D

ISPA Academy

## Überblick

- Lessons learned
- Wie kann ich DNSSEC verwenden?
- DNSSEC in .at

## Lessons learned

- Software: möglichst aktuelle Versionen benutzen
  - Weniger Bugs
    - z.B. Bind 9.8.1: 21 DNSSEC-related Bugfixes
  - Bedienbarkeit verbessert
    - z.B. Bind 9.6 -> 9.7 „DNSSEC for Humans“
- Testen, testen, testen



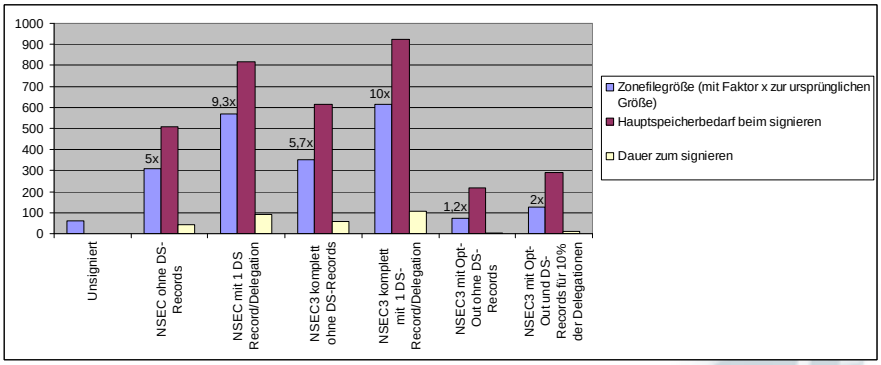
ISPA Academy

## Lessons learned

- Hardware: höhere CPU und Memory Anforderungen
- Alle Slave-NS müssen DNSSEC unterstützen
- Firewall: DNS verwendet auch Port 53/TCP
- Saubere Delegationen:
  - Achtung: domain.at + sub.domain.at auf selben Nameserver ohne NS –Records
- Möglichst Default-Einstellungen verwenden
- Zeit auf allen NS synchron halten (NTP)

# Zonefilegröße

Ausgangsfile: Zone mit ca. 60MB




5



# Software

- Nameserversoftware
  - Bind ab Version 9.6
  - NSD ab Version 3.1
  - Unbound  seit Version 1.0
  - PowerDNS seit Version 3.0 (autoritativ)
  - Windows Server 2003 (Commandline, kein GUI)

6

## Software

- Signieren
  - Nameserver-Utils (bind-utils, ldns-utils)
  - Im Nameserver selbst (Bind, PowerDNS)
  - OpenDNSSEC
  - Hardwarelösung
    - Secure64, Xelerance, …
- Monitoring/Debugging
  - Nagios/Icinga Plugins
  - Webinterface z.b: http://dnsviz.net





## Wer ist schon signiert?

- 316 TLDs in the root zone in total
- 105 TLDs are signed;
- 96 TLDs have trust anchors published as DS records in the root zone;
  - com, net, org, de, at, eu, uk, cz, se, …
- 3 TLDs have trust anchors published in the ISC DLV Repository.

## Validieren

- http://www.root-dnssec.org/
- Notwendige Schritte
  - Root-Key am Resolving-NS hinzufügen
  - Valdierung aktivieren
  - http://test.dnssec-or-not.net





## Validieren – Bind >= 9.7

- named.conf

```
options { dnssec-validation yes;
          dnssec-enable yes;
        }

managed-keys { "." initial-key 257 3 8
"AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVV
LOyQbSEW0O8gcCjF
[…]
fwhYB4N7knNnulq QxA+Uk1ihz0="; };
```

## Signieren

- Zone vorab signieren
- Dynamische Updates, Bind signiert wenn Update eintrifft
- On-the-fly Signierung (PowerDNS, Bind ab 9.9)
- Bump-in-the-wire Lösungen
  - Hard- oder Software





## Beispiel: Signieren mit Bind-utils

- KSK erzeugen

```
dnssec-keygen –a RSASHA1 –b 2048 –f KSK
dnssec-test.at
```

- ZSK erzeugen

```
dnssec-keygen –a RSASHA1 –b 1024 dnssec-
test.at
```

- Zone signieren

```
dnssec-signzone –S –o dnssec-test.at
dnssec-test.at.db
```

## Beispiel: Signieren on-the-fly

- Bind ab Version 9.9

```
zone "test.at" {
        type master;
        file "/etc/bind/test.at";
        key-directory "/etc/bind/keys";
        auto-dnssec maintain;
        inline-signing yes;
};
```

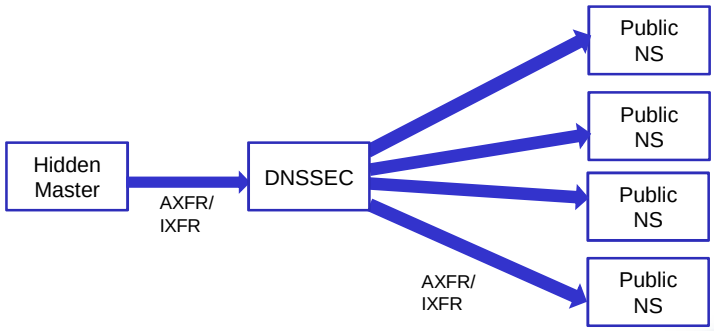




## Bump-in-the-wire

- Lösung, die in ein bestehendes Setup eingeklinkt wird
  - definierter Eingang
    - AXFR
  - Policy wird definiert
    - Keyhandling passiert automatisch
  - definierter Ausgang
    - Notify + AXFR
    - Script
- Hardware oder Software: z.B. opendnssec.org

## Bump-in-the-wire








## DNSSEC für .at

## DNSSEC für .at

- Internes Projekt seit >4 Jahren
- DNSSEC-Testbed
  - von 12.2010 – 12.2011
- DNSSEC in Produktion
  - .at signiert seit 12.2011
  - Verfügbar für Registrare seit 29.2.2011
    - auch im Testsystem

17



## EPP

- RFC 5910 „Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)" implementiert
  - Nachfolger von RFC 4310: secDNS-1.1
  - nur DS-Data Interface
  - nur Syntaxchecks, keine Inhaltschecks
  - nic.at EPP-Toolkit angepasst

18

## Whois

- DNSSEC-Daten werden im Whois angezeigt:

```
DNSSEC:Signed
DS Key Tag 1:54135
Algorithm 1:5
Digest Type 1:1
Digest 1:225F055ACB65C8B60AD18B3640062E8C23A5FD89
DS Key Tag 2:54135
Algorithm 2:5
Digest Type 2:2
Digest
2:6CDE2DE97F1D07B23134440F19682E7519ADDAE180E20B1B1E
C52E7F58B2831D
```





## Web

- DNSSEC Unterstützung für
  - Registrarweb
  - Endkundenweb

## Transferproblem

- Problem:
  - Transfer einer signierte Domain zu neuen Registrar
  - Neuer Registrar bemerkt nicht, dass Domain signiert ist und schickt Nameserver-Update
  - NS-Update wird durchgeführt, DS-Record in .AT-Zone bleibt bestehen -> Validierung der Domain schlägt fehl





## Transferproblem: nic.at Lösung

- Unterscheidung DNSSEC-/Nicht-DNSSEC-Registrar
  - „Mascherl“ im Registrar-Web
  - Default: Nicht-DNSSEC
- Bei Transfer von DNSSEC- zu Nicht-DNSSEC-Registrar werden die DS-Records automatisch entfernt
- Bei Transfer von DNSSEC- zu DNSSEC-Registrar bleiben diese bestehen

Fragen? Diskussion?

Michael Braunöder <mib@nic.at>