Eco – DNSSEC Workshop

DNSSEC – Vertrauen ins DNS

Lutz Donnerhacke

```
dig NAPTR 1.6.5.3.7.5.1.4.6.3.9.4.e164.arpa. +dnssec
```

DNS Security

- Klassische Public-Key Signaturen: RRSIG
- Signaturen der Nichtexistenz: NSEC*3*
- Signaturen der Wildcards: extra RRSIG
- Verteilung der Schlüssel: DNSKEY
- Zertifikate entlang der Hierarchie: DS
- Zertifikate außerhalb der Hierarchie: DLV
- Datenübertragung: TSig und SIG(0)
- Bits zur Abfrage, Korrektheit, Eigenprüfung

Cool Stuff

- SSH – Zentraladministration statt known_hosts
- SSL/HTTPS – Zertifikate kostenfrei statt CAs
- VPN/IPSec – Public Keys aktuell halten
- OpenPGP – Public Keys aktuell halten
- VoIP – e164.arpa ist signiert
- Spamschutz – Domainkeys, SPF etc. validierbar
- Schutz vor Pharming, Poisoning

Was DNSSEC wirklich kann

- Admin: Falsche Daten in der Zone
  - Keine Hilfe möglich
- Dienstleister: Falsche Daten bei der Registry
  - Keine Hilfe möglich
- MitM: Pakete abfangen und ändern
  - Änderung wird erkannt
  - Datenwiederherstellung ist nicht möglich

Was DNSSEC wirklich kann

- ID-Raten: Schneller andere antworten
  - Schutz: Angreifer werden erkannt und abgewehrt
- Poisoning: Falsche Antworten cachen lassen
  - Schutz: Angreifer werden erkannt und abgewehrt
- DoS: Vorspiegelung der Nichtexistenz
  - Schutz: Angreifer werden erkannt und abgewehrt
- Wildcards: Vorspiegelung der Existenz
  - Schutz: Angreifer werden erkannt und abgewehrt

Was DNSSEC wirklich kann

- Redirects: Falsche Server konfigurieren
  - Schutz: Angreifer werden erkannt und abgewehrt
- ABER
  - Aktuelle Implementationen prüfen im Nachgang, d.h. Ermittlung der richtigen Daten nicht möglich
  - Anstatt auf den falschen Server zu gelangen, kann die Applikation nicht mehr kommunizieren
  - Kein Protokollfehler, sondern Validierungfehler

Was DNSSEC wirklich kann

- Kommunikation zwischen DNS-Servern
  - TSIG / SIG(0) für Integritätsnachweis
- Schutz der Kommunikationsinhalte (P2P, IM, ...)
  - Kein Schutz vorhanden
- Schutz vor Ausspähung
  - Passiv: Kein Schutz bei zone transfers
  - Aktiv: NSEC *ermöglicht* zone enumeration
  - Aktiv: NSEC3 verhindert zone enumeration

Auswirkungen von DNSSEC

- Verbesserung der Cacheperformance
  - Theoretisch: NSEC-Nutzung für Negativcaching
  - Praktisch: Im Protokoll verboten
  - Getestet: Substantielle Anfrageersparnis 30-70%
- Loadbalancing, Contentdistribution
  - *Verhindert* Geocaching
- (double-)NAT wegen Adressüberschneidung
  - *Unterbindet* Umschreibungen

Auswirkungen von DNSSEC auf innovative Geschäftsmodelle

- Sitefinder
  - *Verhindert* Abgreifen von Suchseiten
  - Erkennt keine transparenten Proxies
- Fastflux, DynDNS
  - Erschwert schnelle Änderungen
- Flippthelerdomains
  - Keine Auswirkung

Auswirkungen von DNSSEC im Domaingeschäft

- DNSSEC als Mehrwert
  - Zusätzliche Einnahmen vs. Deployment
- Domainübernahmen
  - Kein Schutz vor unberechtigten Übernahmen
  - Keine Probleme bei berechtigten Übernahmen
- Abschaltung von DNSSEC
  - Unkooperatives Abschalten kann wochenlange Downtimes generieren (bis zur Kooperation)

Rechtsfolgen von DNSSEC

- DNSSEC ist eine fortgeschrittene Signatur
  - Grundsätzlich der Unterschrift gleichgestellt
  - Signierte Records als Beweismittel verwertbar
  - Administratorhaftung im Kundenverhältnis klären
- Zone nicht signiert und Kunde fehlgeleitet
  - Rechtsfolgen erst Jahre später
  - Anbieterverpflichtung zum Kunden(selbst)schutz
  - Onlinebanking via Russland: Bank wird haften!

Maintenance – Tägliche Arbeiten

- Signaturen laufen aus: Nächtlich neu signieren
- Seriennummer muss *automatisch* erhöht werden
- Notfallplan: kompromittierte Schlüssel
- Datenpakete werden zu groß: EDNS0, Firewalls
- Zeitsynchonisation nötig
- Zone walking: Sind Ihre Zonen *so* öffentlich?
- Regelmäßige Schlüsselwechsel: DS aktualisieren

Zentralisierung als Kompromiss

- Einsatz validierender rekursiver Resolver
- Stub-Resolver der letzten Meile bekommen nur korrekt validierte Angaben oder SERVFAIL
- Sicherheit auf der letzte Meile zwingend nötig

➔ Aufbrechen des Ende-Ende-Prinzips

- *Intelligentere* Resolver können aber Rohdaten anfordern und selbst validieren

DNSSEC – Verbreitung

- Derzeit ca. 3000 signierte Domains
- Signierte TLDs: bg, br, cz, pr, se, (org, fr, ru, at)
- Top: 709 ru, 526 com, 416 br, 339 arpa, 262 de
- Produktiv vorhanden:
  - Signierte Root von IKS (IANA 2009)
  - Öffentliche DLVs von IKS und ISC
  - Remote Signierung Services für schnellen Start
  - Vor allem die Rückwärtsauflösung ist validierbar

DNSSEC – Vertrauen bilden

Fragen!