Einsatz von DNSSEC in der Domain .de

8. DFN-CERT Workshop
„Sicherheit in vernetzten Systemen“
15./16. Mai 2001

Marcos Sanz
sanz@denic.de

DENIC eG
Wiesenhüttenplatz 26
D-60329 Frankfurt am Main
Tel. +49 69 27235-0
Fax +49 69 27235-235
E-Mail info@denic.de
http://www.denic.de

Stefan Kelm
kelm@secorvo.de

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455
E-Mail info@secorvo.de
http://www.secorvo.de

Agenda

- **Einleitung**
- **1. Teil:**
  Anforderungen an ein sicheres Top-Level-DNS
- **2. Teil:**
  Schlüsselmanagement für DNSSEC bei DENIC
- **Ergebnisse und Ausblick**

Einleitung

- **Erstellung einer Studie zum Thema DNSSEC**
  - **Welche rechtlichen, gesetzlichen und organisatorischen Anforderungen werden an die Sicherheit des DNS gestellt?**
  - **Welche Aufgaben fallen bei der organisatorischen Einbindung in das bereits bestehende Umfeld an?**
  - **Wie gestaltet sich die technische Konzeption bei der Software-Umstellung von Nameservern auf DNSSEC?**
  - **Welche rechtlichen Rahmenbedingungen sind bei der Umsetzung zu berücksichtigen?**
- **Zeitraum**
  - **Juli 2000 - Oktober 2000**
  - **danach: europäische Arbeitsgruppentreffen**

DENIC de

secorvo security consulting

Anforderungen an ein sicheres Top-Level-DNS

- **Sicheres DNS vs DNSSEC**
  - **Anforderungskatalog: DNSSEC bei DENIC**
    - **rechtliche Anforderungen**
      - Registrierung
      - Datenschutz
      - vertragliche Anforderungen
    - **Grundschutzanforderungen**
      - Infrastruktur
      - Server
    - **Besondere Anforderungen an DNS**
    - **Sonstige Anforderungen**

DENIC de

secorvo security consulting

Registrierung von Domains

- Wettbewerbliche und kennzeichenrechtliche Ansprüche, z.B.:
  - §§ 14 und 15 MarkenG
    - Verbot der Verwendung identischer oder ähnlicher Zeichen
    - OLG Frankfurt - „ambiente.de“
    - LG Magdeburg - „foris.de“
  - § 1 UWG
    - Verstoß gegen strafrechtliche oder gewerberechtliche Vorschriften
    - OLG Hamburg - „goldenjackpot.com“
  - § 12 BGB
    - Verletzung des Namensrechts
    - OLG Mannheim - „heidelberg.de“

Registrierung von Domains

- Gebotene und zumutbare Maßnahmen
  - Keine Prüfungspflicht vor Registrierung
  - Aber Prüfungspflicht bei späterer Kenntnis
  - Beschränkung der Prüfung auf offensichtliche Rechtsverstöße
  - Problem: Was ist offensichtlich?
    - Muß ein rechtskräftiges Urteil vorliegen?
    - Reicht Kenntnisnahme in mündlicher Verhandlung?
    - Was ist mit Kennzeichen, die allen bekannt sind?
- Schiedsstellen zu Lösung dieses Problems
- Kündigung aus wichtigem Grund

Datenschutz

- Zulässigkeit der Speicherung und Übermittlung personenbezogener Daten (z.B.: whois)
  - Einwilligung des Kunden
  - § 28 BDSG: Interessenabwägung
- Problem: Einwilligung des admin-c
  - Gefordert für Übermittlung der E-Mail-Adresse
  - Falls admin-c nicht mit Domaininhaber identisch
    - Woher weiß DENIC, daß admin-c zugestimmt hat?
    - Schriftform i.d.R. erforderlich
- Weitere Anforderungen
  - Verpflichtung auf das Datengeheimnis (§ 5 BDSG)
  - Technische und organisatorische Maßnahmen (§ 9 BDSG)

Vertragliche Anforderungen

- Vereinbarungen mit Kunden
  - Aufgaben von DENIC gemäß § 2 AGB
    - Registrierung der Domain
    - Übernahme in öffentliches Register (whois)
    - Dispute-Eintrag
  - Weitere Aufgaben gemäß Statut
    - Betrieb des Primary-Nameservers
    - Bereitstellung von Datenbankdiensten (whois)
- Entzug einer Domain
  - vorher rechtmäßige Kündigung des Vertrags
  - liegt ein Kündigungsgrund vor ?

Vertragliche Anforderungen

- Haftung von DENIC
  - Haftungsausschluß für leichte Fahrlässigkeit
    - Grundsatz: Haftungsausschluß unzulässig, falls der Verletzte auf die Einhaltung von Sorgfaltspflichten vertrauen darf
  - Haftungsbeschränkung der Höhe nach
    - Grundsatz: Angemessenes Verhältnis zur typischen Schadensrisiko
- Maßnahmen zur Haftungsreduzierung
  - Versicherung
  - Service Level Agreement (SLA) mit dem Kunden
  - Vertrag mit ICANN

DENIC de

secorvo security consulting

Übergeordnete Grundschutzanforderungen

- Organisation
- Personal
- Notfallvorsorge-Konzept
- Datensicherungskonzept
- Computer-Virenschutzkonzept
- Kryptokonzept
- Behandlung von Sicherheitsvorfällen

- vgl. BSI-Grundschutzhandbuch (GSHB)

DENIC de

secorvo security consulting

Bes. Anforderungen an DNS

- DNSSEC
  - Signatur der Zone
  - DNSSEC-Fähigkeit der Nameserver
  - Schlüsselmanagement
  - Caching
- Zonentransfers
  - Sicherer Zonentransfer
  - Verhinderung nichtautorisierter Zonentransfers
  - Beschränkung der Transfers
- Zonenupdate
  - Integrität der Zone
  - Maximaldauer, Offline-Zonenupdate

DENIC .de

secorvo security consulting

Sonstige Anforderungen

- Lastreserve
- Konnektivität
- Besonderes LAN-Segment
- Schutz durch Firewall
- Synchronisation der Uhren

DENIC .de

secorvo security consulting

Das Problem

- DNSSEC basiert auf der Public Key-Technologie...
  - RRs sind digital signiert
  - Transaktionen können digital signiert sein
  - Antworten des Servers können authentisiert werden
  - dynamische Updates können digital signiert werden
- ...wurde aber nicht mit PKI-Prozessen konzipiert
- es fehlen insbesondere Konzepte für
  - Schlüsselmanagement
  - „Zertifizierung“
  - Kommunikation

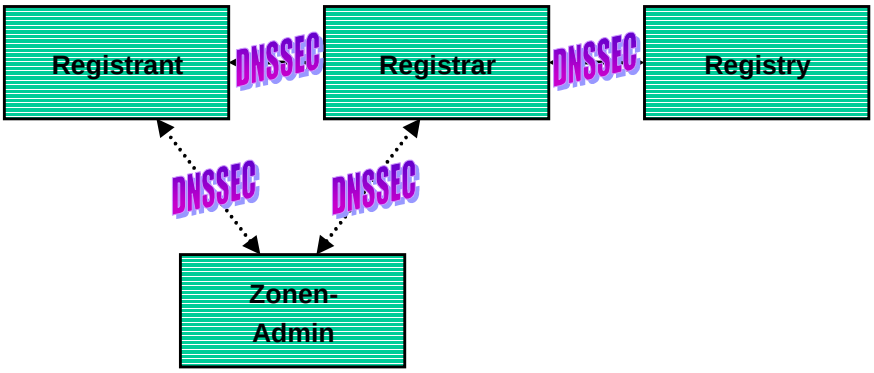
PKI-Prozesse

- Die wesentlichen Prozesse einer PKI
  - Schlüsselgenerierung
  - Schlüsselzertifizierung
  - Schlüsselverteilung
  - Schlüsselrückruf / Schlüsselsperrung
  - Schlüsselwechsel
  - Schlüsselspeicherung
  - Schlüsselanwendung
  - Key Recovery
- Trennung der PKI-Teilnehmer
  - CA, RA, Verzeichnisse, TSA, ...
  - Endteilnehmer (Benutzer vs. Server)

Bsp: Schlüsselzertifizierung

- DNSSEC kennt keine Zertifizierung nach X.509
  - Eine Zertifizierung nach DNSSEC ist die Signierung des KEY-RRs einer untergeordneten (delegierten) Zone
- Überprüfung des Schlüsselinhabers ?
  - Identität des KEY-Inhabers
  - „Personalisierung“
- Gültigkeitsdauer
  - Signatur vs. TTL
  - keine Sperrung von Zertifikaten !
- zentrale Frage:
  - wo werden KEY und SIG gespeichert ???

Wo DNSSEC ?



drei „Problembereiche“

- technische Ausgestaltung der DNSSEC-Spec
  - grundlegende Verfahren zur Signaturerzeugung und -verifikation sind vorhanden
  - dennoch: Spezifikation nicht sehr stabil
  - und: mangelnde Implementation
- organisatorische Umsetzung des PKI-Konzepts
  - Zertifizierung
  - Kommunikation zwischen Teilnehmern („out-of-band“)
  - keine Trennung zwischen Nameserver und Resolver
- Performanz der Systeme
  - Netzwerk, Nameserver und Resolver
  - Server: Zugriff auf Schlüssel off-line vs. on-line

DENIC de

secorvo security consulting

Eine DNSSEC-PKI ?

- Sicherheits- und Betriebskonzept
- Ressourcenplanung
- Gültigkeitsmodell
  - Festlegen der einzelnen Gültigkeitszeiträume
- Policy
  - Richtlinien für die Zertifizierung
    - z.B.: wer darf zertifiziert werden?
    - wer zertifiziert?
  - Aussagen über die Qualität
  - Aussagen über die Gültigkeit von Zertifikaten
  - Bsp: Resolver-Policy [RFC 2535, 6.3.1]

DENIC de

secorvo security consulting

Eine DNSSEC-PKI ?

- Einhalten der Policy
- laufender Betrieb der Zertifizierung
  - möglicher Ablauf
    - Zonenschlüssel erzeugen
    - Senden an „parent zone“
    - SIG-RRs erzeugen und an „child zone“ übermitteln
    - NXT und SIG(NXT) erzeugen
- Überprüfung der Identitäten
  - Zonenadministrator = CA-Administrator ?
  - Aussage der Signatur ?
- Automatisierung von Abläufen, z.B. durch Skripte
  - was passiert mit ungültigen Signaturen und den entsprechenden RRs ?

Eine DNSSEC-PKI ?

- Administration der Zonen
  - jede Schlüsseländerung erfordert Kommunikation zwischen zwei Zonen
    - Re-Zertifizierung ?
  - „NULL-Schlüssel“ ?

offene Fragen

- Win2K und DNSSEC?
- Providerwechsel (CHPROV)?
- Performanz?
  - CPU, RAM, HDD, Netzanbindung, ...
- „Kontrolle“ von signierten Zonen?
- Kompromittierung von Schlüsseln?
- Resolver und DNSSEC?
- Wechsel des DNSSEC-Status?
- „Lücken“ im Zertifizierungspfad?
- Root-Server & DNSSEC?

DENIC de

secorvo security consulting

Fazit

- DNSSEC gewinnt an Bedeutung
  - viele offene Fragen sind identifiziert und werden adressiert
  - Einführung von DNSSEC ist unproblematisch,
  - ...aber der laufende Betrieb !
- Einführungskonzept
  - schrittweise Nutzung von DNSSEC
  - Einrichten von „Schattenzonen“ (.de.de) ?
  - Zusammenarbeit mit einigen Zonenadministratoren
  - langsame Ausdehnung
  - Kooperation mit anderen Gruppen, z.B. NLnet Labs
- Empfehlung
  - Beantwortung der Fragen innerhalb eines DFN-Projektes

DENIC de

secorvo security consulting

Empfehlung

- **Bearbeitung von Fragestellungen innerhalb eines langfristigen Projektes**
  - **Schlüsselmanagement („think PKI“)**
  - **Delegierung von Aufgaben**
    - **Verträge / Haftung**
  - **Skalierbarkeit / Performanz**
  - **Interoperabilität (BINDv9 vs. Windows 2000)**
  - **Resolver-Unterstützung**
  - **reale Anwendungen (z.B. SSH über DNSSEC)**
  - **gesicherte und ungesicherte Zonen**
  - **Automatisierung von Abläufen**
  - **Erstellung einer DNSSEC-Policy**
    - **PKI, Betriebskonzept , Roll-out Konzept, Vorfallsbearbeitung, ...**

DENIC eG
Wiesenhüttenplatz 26
D-60329 Frankfurt am Main

Tel. +49 69 27235-0
Fax +49 69 27235-235
E-Mail info@denic.de
http://www.denic.de

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455
E-Mail info@secorvo.de
http://www.secorvo.de