DNSSEC-Erweiterungen aus Registrarsicht

...es geht einfach! InterNetX

Volker Janzen, Senior Developer

janzen@internetx.de

Geschichte

- 1998 Gründung in Regensburg
- 2001 Übernahme von PSI-USA, Inc.
  Seitdem ICANN akkreditierter Registrar
- 2005 InterNetX gehört zum Teil der
  United Internet AG

Domains

- Verwaltung von mehr als 2,9 Millionen Domains
- Mehr als 300 ccTLDs und gTLDs im Portfolio
- Größtes DENIC-Mitglied
- Akkreditierung bei ICANN und zahlreichen Registrys rund um den Globus

Server

- Innovative Server-Lösungen für alle Business-Anforderungen
  - First-Class Data-Center in München
  - Hosting von über 1.400 Servern
  - Server-Housing

AutoDNS (1)

- Inhouse Software-Entwicklung
- Domainverwaltungs-Software in drei Sprachen (DE, EN, ES)

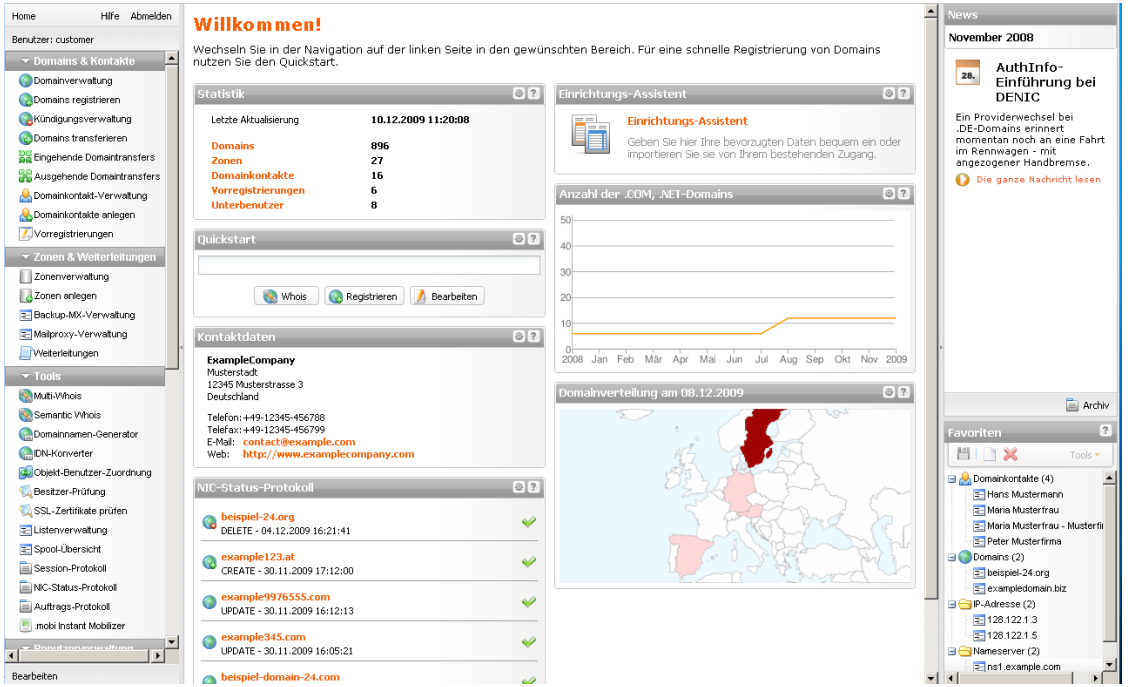
für Domainer

für Reseller

für Registrare

AutoDNS (2)

- Einheitliche Schnittstelle zu allen Registrys
  - Web-Interface
  - Key-Value-Schnittstelle
  - XML-Schnittstelle



AutoDNS XML

```
[…]
   <domain>
    <name>meindnssec.de</name>
    <ownerc>1234567</ownerc>
    <adminc>1234567</adminc>
    <techc>1222467</techc>
    <zonec>1222467</zonec>
    <nserver>
        [...]
    </nserver>
    <dnssec>
        <flags>257</flags>
        <protocol>3</protocol>
        <algorithm>5</algorithm>
        <publickey>[...]</publickey>
    </dnssec>
   </domain>
[…]
```

Welche Möglichkeiten bieten die Registrys DNSSEC zu verwenden?

DENIC RRI

- DNSKEY
- Proprietäres Protokoll (RRI oder MRIv2)
- DENIC DNSSEC Testbed
  - Komplett implementiert bei InterNetX
  - Nutzung durch InterNetX Testkunden
  - Teilnahme auch mit Registrar AutoDNS möglich
  - Tests für Providerwechsel willkommen

DENIC RRI

```
[...]
<dnsentry:dnsentry
xmlns:dnsentry="http://registry.denic.de/dnsentry/1.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="dnsentry:DNSKEY">
  <dnsentry:owner>meindnssec.de.</dnsentry:owner>
  <dnsentry:rdata>
     <dnsentry:flags>257</dnsentry:flags>
     <dnsentry:protocol>3</dnsentry:protocol>
     <dnsentry:algorithm>5</dnsentry:algorithm>
     <dnsentry:publicKey>[...]</dnsentry:publicKey>
  </dnsentry:rdata>
</dnsentry:dnsentry>
[...]
```

EPP nach RFC (1)

- Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)
- RFC 4310 (November 2005)
  - DS (Delegation Signer) Daten, optional mit DNSKEY Daten
- **.SE** hat DNSSEC im Produktivbetrieb
- **.ORG** will Ende Juni mit DNSSEC starten

EPP nach RFC (2)

- **.CH / .LI** : produktiv
- **.EU** hat Testbed gestartet
- **.NET** möchte im Q4/2010 starten
- Weitere Registrys bieten DNSSEC
- RFC 5910 im Mai veröffentlicht

EPP (RFC 4310)

```
<extension>
   <secDNS:update urgent="1"
    xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.0"
    xsi:schemaLocation="urn:ietf:params:xml:ns:secDNS-1.0
    secDNS-1.0.xsd">
    <secDNS:chg>
       <secDNS:dsData>
          <secDNS:keyTag>12345</secDNS:keyTag>
          <secDNS:alg>3</secDNS:alg>
          <secDNS:digestType>1</secDNS:digestType>
             <secDNS:digest>[...]</secDNS:digest>
       </secDNS:dsData>
    </secDNS:chg>
   </secDNS:update>
</extension>
```

EPP (RFC 5910)

```
<extension>
   <secDNS:update xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
    <secDNS:rem>
        <secDNS:dsData>
            <secDNS:keyTag>12345</secDNS:keyTag>
            <secDNS:alg>3</secDNS:alg>
            <secDNS:digestType>1</secDNS:digestType>
            <secDNS:digest>38EC35D5B3A34B33C99B</secDNS:digest>
        </secDNS:dsData>
    </secDNS:rem>
    <secDNS:add>
        <secDNS:dsData>
            <secDNS:keyTag>12346</secDNS:keyTag>
            <secDNS:alg>3</secDNS:alg>
            <secDNS:digestType>1</secDNS:digestType>
            <secDNS:digest>38EC35D5B3A34B44C39B</secDNS:digest>
        </secDNS:dsData>
    </secDNS:add>
   </secDNS:update>
</extension>
```

EPP extended

- EPP definiert einen Standard zur Erweiterung mit neue Kommandos und Parametern
- .CZ verwendet Nameservergruppen und Keysets für die DS/DNSKEY Einträge

Die Kommunikation mit der Registry macht aber nur einen Teil des Ganzen aus...

Nameserver

- Wir verwalten ca. 1,5 Millionen Zonen
- Hohe Anforderungen an Nameserver-Software
  - Datenbankgestützte Nameserver zur effizienten Verwaltung.
  - Änderungen müssen ohne große Verzögerung aktiv werden.
  - PowerDNS hat eine erste Testversion mit DNSSEC. Noch nicht optimal.

Sonstige Probleme

- Wie funktioniert ein (Emergency) Key Rollover für 1,5 Millionen Zonen?
- Keine definierte Schnittstelle, um Änderungen an der Signierung der Zone an die Registry weiterzugeben.

Ende

InterNetX

Gibt es noch Fragen?

janzen@internetx.de