DNSSEC-Einführung in .bund.de

Thorsten Dietrich

Bundesamt für Sicherheit in der Informationstechnik

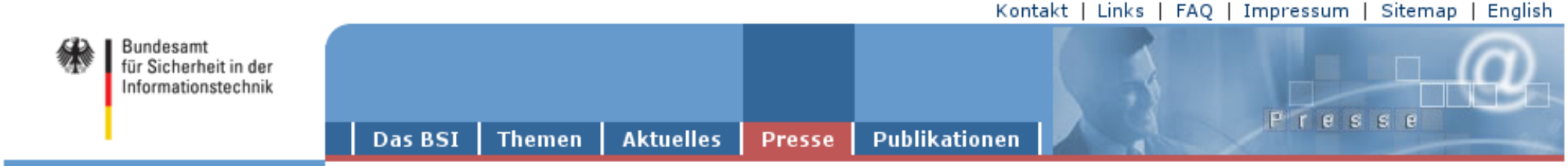
3. DNSSEC-Testbed Meeting / 16. Juni 2010

Inhalt

- Signierung .bund.de:
  - Status
  - Betriebsparameter
  - Erfahrungswerte
- DNSSEC-Validierung im Informationsverbund Berlin-Bonn (IVBB)
- Ausblick

Bundesamt
für Sicherheit in der
Informationstechnik

DNSSEC-Signierung .bund.de



Startseite › Presse › Verbesserung der Sicherheit des Domain-Name-Systems (DNS)

Verbesserung der Sicherheit des Domain-Name-Systems (DNS)

DNSSEC-Signierung der Domain ".bund.de" und BSI-Studie zur DNSSEC-Tauglichkeit von Internetzugangsroutern

Bonn, 03.05.2010.
Seit dem 7. April 2010 stehen die Einträge der Domain ".bund.de" kryptographisch signiert zur Verfügung. Der zur Überprüfung der Signaturen erforderliche Schlüssel ist seit dem 29. April 2010 in der von der DENIC Domain Verwaltungs- und Betriebsgesellschaft eG bereitgestellten Testumgebung veröffentlicht. Er kann außerdem auf der Webseite des Bundesamts für Sicherheit in der Informationstechnik (BSI) heruntergeladen werden. DNSSEC-Signierung der Domain bund.de (txt, 383 Byte) Nutzern der Testumgebung wird damit bereits heute bei der Namensauflösung die Validierung der Einträge mit der Endung ".bund.de" ermöglicht. Eine Signierung weiterer Domains der Bundesverwaltung ist geplant. Die Bundesverwaltung beteiligt sich somit aktiv an der Testumgebung für die DNS-Sicherheitserweiterung DNSSEC (Domain Name Security Extensions) und nimmt hier eine Vorreiterrolle ein.

Im Jahr 2008 wurde in dem für das Internet wichtigen Dienst Domain Name System (DNS) eine Schwachstelle entdeckt, die es Angreifern potenziell ermöglicht, den Internetverkehr von Anwendern umzulenken, Daten mitzulesen und Inhalte zu manipulieren. Die Ausnutzung der Schwachstelle wurde seitdem erschwert, ist aber nicht geschlossen.

Um das Domain Name System nachhaltig zu verbessern, empfiehlt das BSI die Einführung der DNS-Erweiterung DNSSEC, bei der die DNS-Einträge mittels kryptographischer Verfahren auf ihre Gültigkeit geprüft werden. Mit DNSSEC können die bekannten Sicherheitslücken geschlossen und Manipulationen erschwert werden.

Status

- .bund.de seit 07. April 2010 DNSSEC signiert:
  - ;; ANSWER SECTION:
  - www.bund.de. 12643 IN A 77.87.229.48
  - www.bund.de. 12643 IN RRSIG A 7 3 21600 20100620130201 20100610130201 44432 bund.de. lgs7/c5G5diA4iBqnR9miTavl9jGzxSy4r/pvvx1OQEW0rjT6JrKPUMY ykjsMgP9c1Okvcw+7zxOavNL79DC1k28GMBz1UUkjs8Zw0t+NjgAzKmk mWAGeakLkXFigUIOShkTQnRxNZJ1Ka5OU0FoPKZarIXC6/y/77Pem+IM yJg=
- Veröffentlichung des Schlüssels:
  - Seit Anfang Mai im .de – Testbed
  - Seit Mitte Mai im ISC DLV Repository
  - Auf der Webseite des BSI
    - bund.de. IN DNSKEY 257 3 7 AwEAAbZnEv+KqU91sE0PCtMdwiwh0zKswH9+UjBt+dW4WWgJId026HkA AD6glfOKH9lQajhvvQ5BBcolVCdcAgpI9I9IY0UnLeQJjNbxjHwLMxDr DK9Vj9cgbEntU5BLIjn3Gbk5XXem9z6eXrFKQdilS/kc75qrJz/GZNOB 0CGcXuhsUXvL3cLxpvv7i+KNKYwFnSyOmNwD43V4Nq6IsETccpEyhpY1 oKfspfqKIwYz+zRj1ruEc4Jhr5enEsKcath40mxFIMYkU+VGL974hZbj EuRRs+8oWgdGhy3kB8Ayp+UYwQMy72zZbcAp9aAt2dzCiq6pOtF+7asV dual/7aYov8=

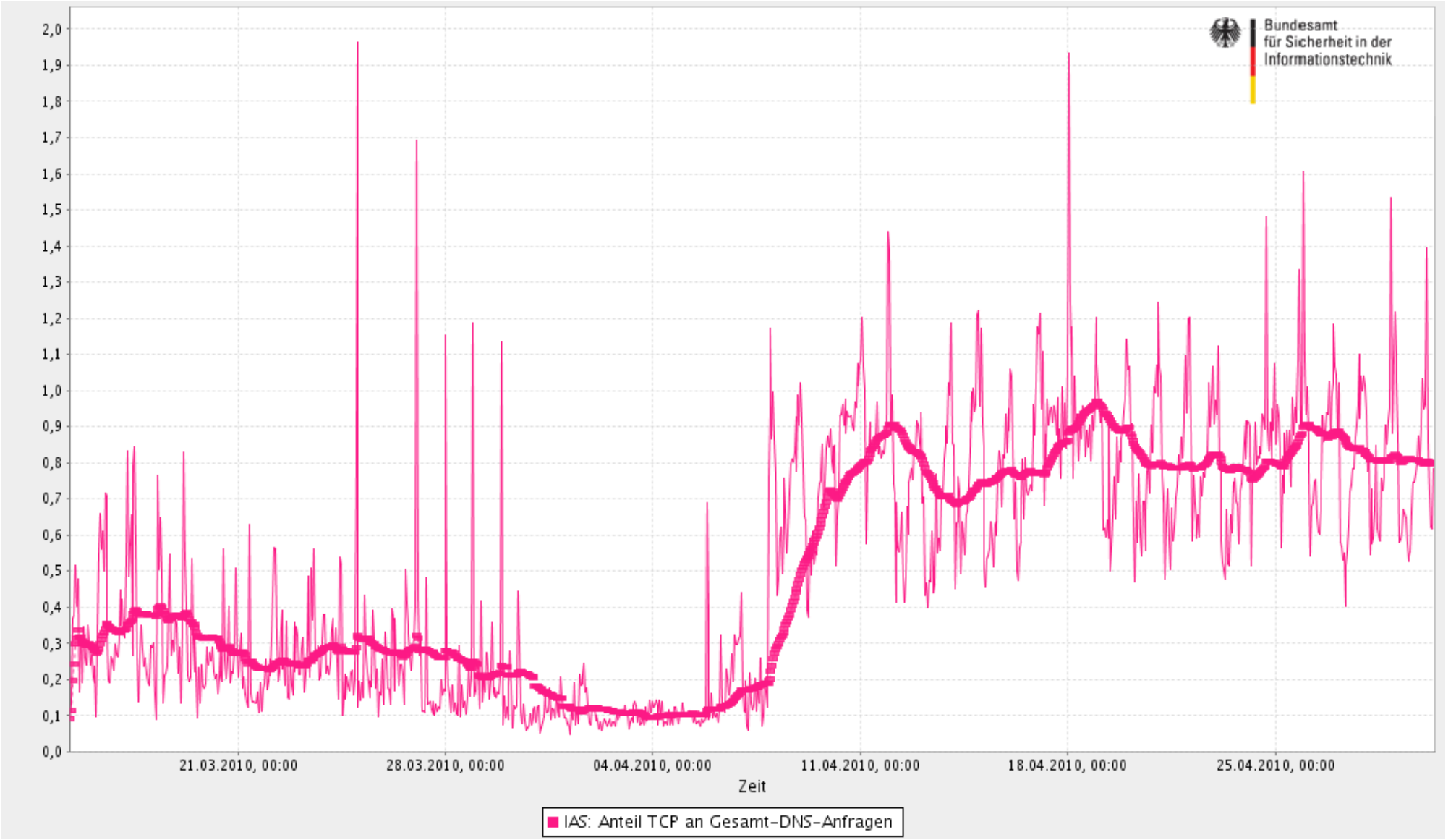
Betriebsparameter

- 4 Nameserver
- Serversoftware: Bind
- Signatur-Algorithmus: RSASHA1 mit NSEC3
- Signierungsparameter:
  - Gültigkeit der Signaturen: 10 Tage
  - ZSK mit 1024 bit Schlüssellänge
  - KSK mit 2048 bit Schlüssellänge
  - ZSK-Rollover: alle 90 Tage, Pre-Publish
  - KSK-Rollover: alle 360 Tage, Pre-Publish

Erfahrungswerte

- CPU-Last:
  - keine signifikanten Auswirkungen auf produktiven Systemen
  - Älteres System: Anstieg CPU-Last von 2% auf 3%
- Transfervolumen:
  - Anstieg um Faktor 5,5 (durch Auslieferung von Signaturen)
- 60,4% der Abfragen erfolgen mit gesetztem DO-Bit
- 0,89% der Abfragen erfolgen über TCP
- 1,04% Truncated Responses

Anteil TCP-Abfragen an DNS-Abfragen insgesamt



DNSSEC-Validierung im Informationsverbund Berlin-Bonn (IVBB)

Betriebserfahrungen

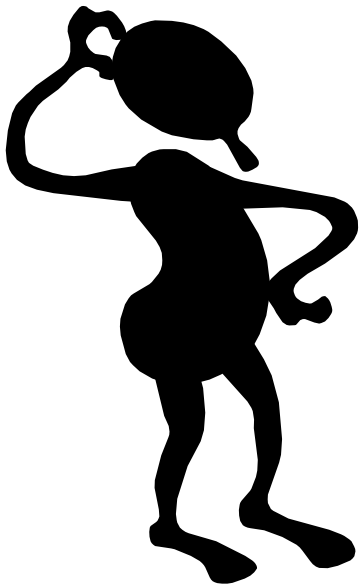
- Serversoftware: Bind
- Validierung seit Mitte April unter Nutzung des ISC DLV Repositories

- Erfahrungen bisher:
  - Vereinzelt Beobachtung von nicht validierbaren Domains aufgrund von abgelaufenen Signaturen (TLD-Endungen .bg, .br, .ARPA, .cz)
  - Fehlerbehebung erfolgte i.d.R. nach wenigen Tagen
  - Beispiel für Domain mit z. Zeit abgelaufener Signatur: eu2009.cz

Ausblick

- Ausweitung der Signierung auf weitere Domains der Bundesverwaltung
- Bereitstellung einer DNSSEC - FAQ für verschiedene Zielgruppen

Vielen Dank für die Aufmerksamkeit!



Fragen?

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Thorsten Dietrich
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5947
Fax: +49 (0)22899-10-9582-5947

Thorsten.Dietrich@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de