Internetdagarna 2005-10-24--25

Agenda

- Aktiviteter fram till produktion
- Koppling mellan certifikat, domän och administratör
- Vilken support kan DNS-operatörer och domännamnsinnehavare få
- NIC-SE:s testresolvrar
- Förväntade effekter

DNSSEC – hur fungerar det?

- Med stöd av digitala signaturer
  - Verifiera vilken namnserver ett svar kommer ifrån
  - Verifiera att informationen är intakt
  - Förhindra manipulering av informationen under transport
- DNS ger möjlighet att distribuera data eftersom DNS är världens största distribuerade databas
- DNSSEC gör att vi kan lita på att data inte är förändrat, men, vi kan inte avgöra om data är korrekt
- Kräver
  - Standarder som omsätts i teknik och utveckling av verktyg för administration

Aktiviteter fram till produktion

- Projektet startade 1999, förstudie publicerades 2000
- Flera workshops har ägt rum, 1999, 2000, 2002, 2005
- Projektet övergick till NIC-SE för fortsatt arbete 2004
- Medverkan i utvecklingen till standard inom IETF
- Utveckling av tekniska verktyg för registryfunktionen
- Informationsspridning till berörda intressenter
- Signering av zonfil
- Förstärkt skydd av kunddata
- Nyckelhanteringsverktyg
- Etc.

DNSSEC – aktiviteter 2005

1. Ny programvara hos namnserveroperatörerna för .se (juni)
2. Signerad se-zon i produktion (september)
3. Utveckling av rutiner och procedurer kring nyckeladministration i .se-zonen. Nyckelhantering mot kunder, definiera ansvarsfrågan. (januari)
4. Signera viktig svensk DNS-infrastruktur (?)
5. Säker DNS-uppslagning hos svenska Internetoperatörer (?)
6. Testverksamhet - informationsträffar med potentiella testdeltagare (löpande)
7. Workshop – utbildning (Q2)
8. Lansering av DNSSEC som tjänst (2006)

DNSSEC – andra aktörer

- Förutom NIC-SE finns följande:
  - Ripe NCC (reverse DNS, in-addr-arpa)
  - Verisign (.net)
  - PIR (.org)
  - Affilias (.info)
  - Nederländerna,SIDN (.nl)
  - På den amerikanska marknaden finansieras en hel del från Department of Homeland Security.

DNSSEC – Begränsat marknadstryck - Starkt myndighetstryck

- PTS säger att de kommer att främja användningen av DNSSEC genom att:

  - ❑ delta i de projekt som branschen driver avseende försök med DNSSEC.
  - ❑ delta i internationellt samarbete för att driva på användandet av DNSSEC.
  - ❑ påverka administratörer av toppdomäner som används i Sverige så att de erbjuder DNSSEC.
  - ❑ påverka namnserveroperatörerna så att de erbjuder DNSSEC till sina kunder.
  - ❑ PTS anser att ***domännamnsadministratörerna ska ta ansvar för att ta fram praktiskt fungerande lösningar för hur hantering av nycklar och certifikat för krypteringen i DNSSEC ska ske***.

Ur rapporten PTS-ER-2005:7 ISSN 1650-9862 Strategi för att säkra Internets infrastruktur

DNSSEC - tjänster

- Nyckeldistribution – från registry till domäninnehavare
- Signering
  - Av zoner
  - Av poster i zoner

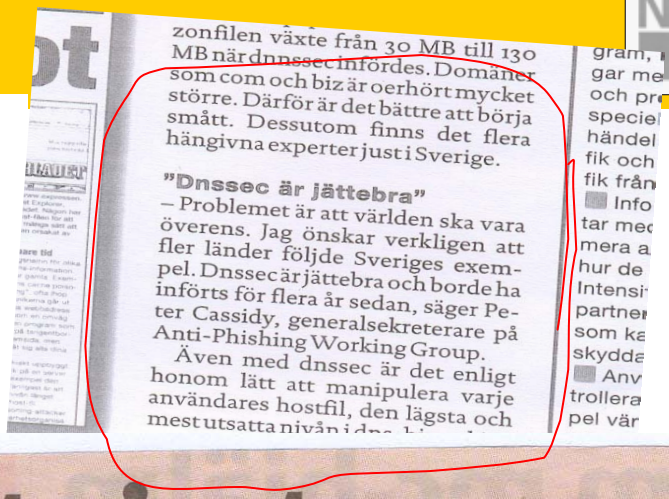
Koppling domän, certifikat, administratör

- En användare registrerar ett domännamn och signerar den egna DNS-informationen i sin zon (antingen själv, eller genom sin namnserveroperatör)
- Användaren måste identifiera sig mot .se:s nyckelhanteringssystem (hur det ska ske är ännu inte slutligt avgjort)
- NIC-SE signerar domäninnehavarens nyckel med .se:s nyckel.
- Verifiering av användarens identitet och innehav av aktuell domän görs innan nyckeln signeras.
- Genom att .se:s nyckel finns publicerad på ett säkert sätt kan vem som helst verifiera signaturer på DNS-frågor i .se förutsatt att:
  - ❑ Zonen man frågat efter är signerad
  - ❑ Operatörernas namnservrar har stöd för DNSSEC

Förväntade effekter – vad DNSSEC hanterar

- Dataintegritet
  - Ingen ska kunna ändra i ett DNS-svar under överföringen utan att det upptäcks
- Autentisering
  - Svaret kommer från rätt server

Förväntade effekter


zonfilen växte från 30 MB till 130 MB när dnssec infördes. Domäner som com och biz är oerhört mycket större. Därför är det bättre att börja smått. Dessutom finns det flera hängivna experter just i Sverige.

"Dnssec är jättebra"

– Problemet är att världen ska vara överens. Jag önskar verkligen att fler länder följde Sveriges exempel. Dnssec är jättebra och borde ha införts för flera år sedan, säger Peter Cassidy, generalsekreterare på Anti-Phishing Working Group.

Även med dnssec är det enligt honom lätt att manipulera varje användares hostfil, den lägsta och


SVERIGES STÖRSTA WEBBPLATS INOM IT

Skriv ut Tipsa Kommentera Lyssna

Där satt den

Nic-se testar säkrare internet med hjälp av dnssec-protokoll

2005-09-23 07:11

Utvecklingen har ta ska internet bli säk toppdomänen som dnssec.

Av Mikael Ricknäs

Det finns ett antal tek dagens internet. En av domännamnssystemet kopplingen mellan dom

Likt många tekniker s

IDG Köp & Sälj
Säljes/Bytes:
Motorola Razr v3
Bytes mot k75

Dagens erbjudande
Här är bästa budgetdatorn
Pris: 30 kr
Del 3: Topprank av sökmotorer
Pris: 30 kr


Så luras nätpiraterna – utan att du vet om det

kommer att få betydligt mer av i Sverige, säger Johan Mårtensson, chef för Sveriges IT-incidentcentrum hos Post- och telestyrelsen (PTS).

Den nya bedrägerimetoden hoppar över e-postinslaget. Du loggar in rätt, men via bedragarnas sätt att lura servrarna så styrs din begäran rätt i gapet på bedragarnas falska sida. Nic-se, som administrerar den svenska huvuddomänen .se, håller som första land i världen på att installera ett nytt säkerhetssystem som ska försvara domännamnssystemet. TT

CS

FREDAGEN DEN 7 OKTOBER 2005 NR 97

DAGENS PRODUKT

8 GB på ett litet kort

Nästa stora hot

Efter phishing kommer pharming

SÄKERHET Nästa stora bedragartrend från USA kallas pharming och går ut på att lura de servrar på internet som styr surfaren till rätt hemsida. När fenomenet når Sverige kan det drabba användarna långt värre än nätdagens phishingförsök mot Nordea.

Attackerare

DNS Caching Server

Attackerarens namnserver

Kund

Så här fungerar pharming

AFTONBLADET

Flera exempel på senare tid

Förväntade effekter – vad DNSSEC INTE hanterar

- Konfidentialitet
  - Ingen kryptering av frågor och svar
- Åtkomstkontroll
  - Grundfilosofin i DNS är att alla uppgifter som läggs i databasen skall vara allmänt åtkomliga

  (Viss åtkomstkontroll sker vid överföring av zoner)

Förväntade effekter – DNSSEC som möjliggörare

- DNSSEC kan användas för distribution av nycklar till IPSec för säker kommunikation och VPN-tunnlar.
- DNSSEC kan användas för distribution av certifikat säkrare elektronisk post, t.ex PGP eller S/MIME.
- Hantering av servernycklar till SSH kan underlättas och göras säkrare med DNSSEC.
- Distribution av certifikat till TLS/SSL, dvs. servercertifikat i webbläsare, kan göras mer flexibel och leverantörsoberoende med hjälp av DNSSEC.

DNSSEC

- Grundstandarder - DNS
  - RFC 1034 Domain names - concepts and facilities. P.V. Mockapetris. Nov-01-1987. (Format: TXT=129180 bytes) (Obsoletes RFC0973, RFC0882, RFC0883) (Updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC2065, RFC2181, RFC2308, RFC2535) (Also STD0013) (Status: STANDARD)
  - RFC 1035 Domain names - implementation and specification. P.V. Mockapetris. Nov-01-1987. (Format: TXT=125626 bytes) (Obsoletes RFC0973, RFC0882, RFC0883) (Updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC1995, RFC1996, RFC2065, RFC2136, RFC2181, RFC2137, RFC2308, RFC2535, RFC2845, RFC3425, RFC3658) (Also STD0013) (Status: STANDARD)

DNSSEC – nya standarder

- DNSSEC – nya standarder
  - RFC 4033 DNS Security Introduction and Requirements.
    R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005. (Format: TXT=52445 bytes) (Obsoletes RFC2535, RFC3008, RFC3090, RFC3445, RFC3655, RFC3658, RFC3755, RFC3757, RFC3845) (Updates RFC1034, RFC1035, RFC2136, RFC2181, RFC2308, RFC3225, RFC3007, RFC3597, RFC3226)
  - RFC 4034 Resource Records for the DNS Security Extensions.
    R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005. (Format: TXT=63879 bytes) (Obsoletes RFC2535, RFC3008, RFC3090, RFC3445, RFC3655, RFC3658, RFC3755, RFC3757, RFC3845) (Updates RFC1034, RFC1035, RFC2136, RFC2181, RFC2308, RFC3225, RFC3007, RFC3597, RFC3226)
  - RFC 4035 Protocol Modifications for the DNS Security Extensions.
    R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005. (Format: TXT=130589 bytes) (Obsoletes RFC2535, RFC3008, RFC3090, RFC3445, RFC3655, RFC3658, RFC3755, RFC3757, RFC3845) (Updates RFC1034, RFC1035, RFC2136, RFC2181, RFC2308, RFC3225, RFC3007, RFC3597, RFC3226)

Frågor?

dnssec-info@nic.se

http://dnssec.nic.se