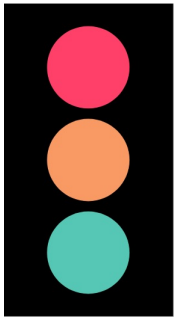
DNSViz

DNSSEC inom sektorn



Zonemaster

SUNET SOC

Om mig

- Erik ”Berra” Bergström
- berra@sunet.se
- SUNET NOC
- NORDUnet/SUNET från 2015
- DNSSEC från 2008

SUNET SOC

flashback...

Zonemaster

- 98 domäner testade SUNET-dagarna HT 2020 med zonemaster
- https://zonemaster.iis.se/

SUNET SOC

DNSSEC & MSB

Myndigheten för samhällsskydd och beredskap

- MSB författningssamling, MSBFS 2020:7

- 4 Kap 8 § - Myndigheten ska använda Domain Name System Security Extensions (DNSSEC) avseende samtliga domännamn som myndigheten registrerat i domännamnssystemet (DNS)

- https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-7-foreskrifter-om-sakerhetsatgarder-i-informationssystem-for-statliga-myndigheter.pdf

SUNET SOC

flashback...

Zonemaster

- 98 domäner testade SUNET-dagarna HT 2020 med zonemaster
- 30 domäner med fel

SUNET SOC

flashback...

Zonemaster

- 98 domäner testade SUNET-dagarna HT 2020 med zonemaster
- 30 domäner med fel
- 54 domäner saknade DNSSEC

SUNET SOC

Nutid!

Zonemaster

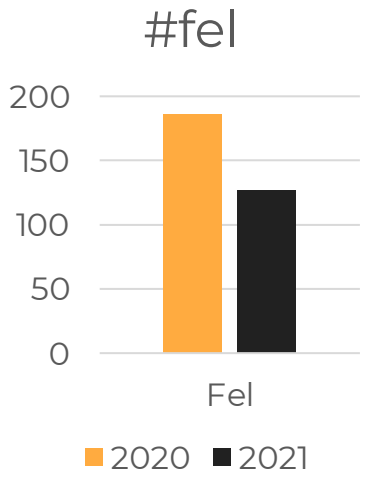
- Samma 98 domäner testades igen med zonemaster

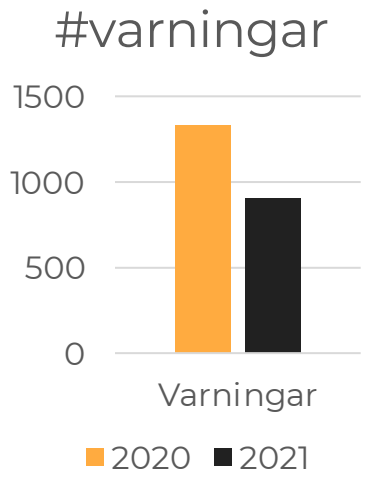
SUNET SOC

Nutid!

Zonemaster

- Samma 98 domäner testades igen med zonemaster
- 9 domäner fick färre fel, 25 domäner fick färre varningar





SUNET SOC

Zonemaster

Nutid!

- 4 domäner har aktiverat DNSSEC (Applåder!)
    - kkh.se, konstnarsnamnden.se, raa.se, skansen.se

SUNET SOC

DNSSEC nutid!

Zonemaster

- Totalt antal fel angående DNSSEC: 57 st
- Totalt antal varningar angående DNSSEC: 704 st

- Totalt antal unika fel per domän: 14 st
- Totalt antal unika varningar per domän: 48 st

- Domäner med fel: 7 st
- Domäner med varningar: 33 st

SUNET SOC

DNSSEC nutid!

Zonemaster

- Vanligaste felen och varningarna:

- Man kör fortfarande SHA1 på sina DS-poster
- Mindre nycklar än rekommenderat
- Extra DS poster som pekar på en DNSKEY som inte finns

SUNET SOC

DNS(SEC) verktyg

- https://zonemaster.iis.se/
- Zonemaster finns som CLI och man kan installera det på sin egna dator.
- https://github.com/zonemaster/zonemaster/

```
# zonemaster-cli --json sunet.se | jq '.[] | select(.level == "WARNING"
and .module == "DNSSEC") | .tag' | sort -u
"DNSKEY_SMALLER_THAN_REC"
"DS_ALGO_SHA1_DEPRECATED"
```

SUNET SOC

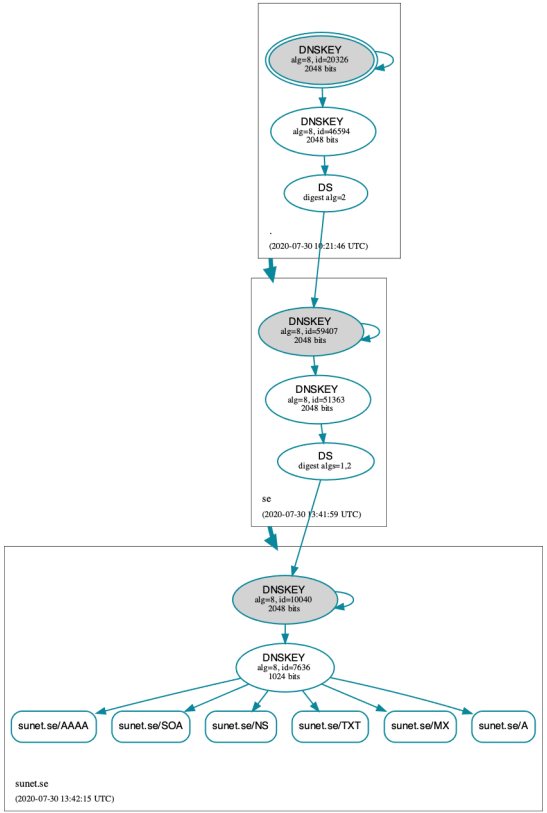
DNS(SEC) verktyg

- dig +trace +dnssec sunet.se

SUNET SOC

DNS(SEC) verktyg

- https://dnsviz.net

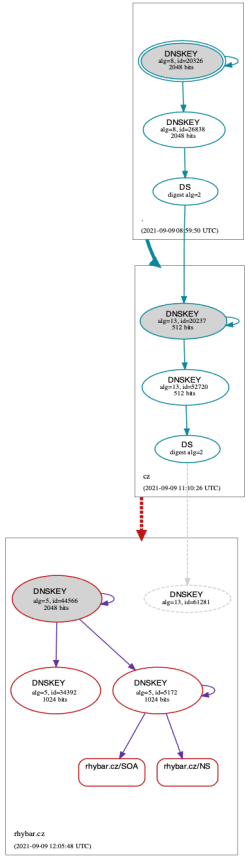


SUNET SOC

DNS(SEC) verktyg

- https://dnsviz.net

- dnssec-failed.org
- rhybar.cz



SUNET SOC

DNSSEC setup

- Så hur gör man?

SUNET SOC

DNSSEC setup

- Så hur gör man?
- RFC2535, RFC4033, RFC6781, RFC8624…
- KSK/ZSK, RRSIG, DNSKEY, DS, NSEC/NSEC3, CDNSKEY, CDS…

SUNET SOC

DNSSEC setup

- bind9.16

```
zone ”sunet.se." {
 ...
 dnssec-policy "default";
};

rndc reconfig
```

Klart!

SUNET SOC

DNSSEC setup

```
# dig @localhost sunet.se DNSKEY | dnssec-dsfromkey -f - sunet.se
sunet.se. IN DS 10040 8 2
D4450B9DF9CAE67849EA7CB620D96743F92A9893487DA045825B28C854A9CABC
```

OBS! Vänta minst en (max) TTL innan man publicerar DS.

Automatisk (via CDS) publicering hos .se. (tar 3 dagar)

SUNET SOC

DNSSEC setup

- Om man inte har tur och kör senaste bind 9

```
dnssec-keygen -a ECDSAP256SHA256 sunet.se
dnssec-keygen -a ECDSAP256SHA256 -f KSK sunet.se

options {
 …
key-directory "/var/bind/keys";
}
zone ”sunet.se." {
 ...
inline-signing yes;
auto-dnssec maintain;
};
```

SUNET SOC

RFC8624

- Vilka algoritmer bör man använda?
- För **DNSKEY**
  - RSASHA256 eller ECDSAP256SHA256
- För **DS**
  - SHA-256

SUNET SOC

SUNET & DNS

- Bistå med råd och hjälp
- Sekundär: sunic.sunet.se

SUNET SOC

Mer läsning

- https://internetstiftelsen.se/domaner/domannamnsbranschen/teknik/dnssec/

- https://internetstiftelsen.se/domaner/domannamnsbranschen/teknik/automatiserad-dnssec/

SUNET SOC

Tack!

Frågestund?

It's not DNS
There's no way it's DNS
It was BGP

SUNET SOC