

Applications & DNS

What could possible go wrong?

*"Snakes. Why did it
have to be snakes?"
– Indiana Jones*

*"Applications. Why did it
have to be applications?"*

– me

Very dangerous – you go first!

What is this talk about?

Applications depend on DNS

Applications require DNS

Applications require DNSSEC

Why DNS?

DNS works pretty well

Fast

Scalable

Robust

Secure
(with DNSSEC)

What applications?

Since the dawn of time...

Host Address Lookup

A & AAAA

Mail Exchange

MX



Mail Sender Policy

SPF via TXT

Domain Message Signatures

DKIM via TXT

Email Authentication Policy

DMARC via TXT



kirei

SSH Authentication

SSHFP

Authentication for SMTP

TLSA

Certificate Issuing Constraints

CAA

What happens
when DNS breaks?

A & AAAA wrong \Rightarrow

No connections

SPF wrong ⇒

Outbound mail not accepted

MX or
TLSA for SMTP wrong \Rightarrow
Inbound mail failure

CAA wrong \Rightarrow

No new certificates issued

So, what do you do?

Inventory

– find out what's cooking

<https://hardenize.com>

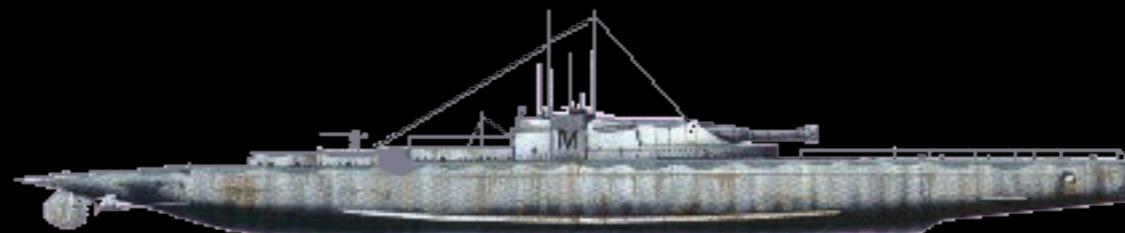
<https://zonemaster.se>

<http://dnsviz.net>

Detect breakage

– early warning systems

Monitor!



<https://keychest.net>

Local Zonemaster

Generic Monitoring Apps

Nagios, Icinga, Sensu, Zabbix, ...

Prevent breakage

Automate deployment
or face the consequences

New SSH key
⇒ SSHFP updated

New DKIM key
⇒ DKIM TXT updated

New certificate for SMTP
⇒ TLSA updated

SURFnet danish

TLSA

hash-slinger

TLSA, SSHFP, IPSECKEY

Update live data
using Dynamic DNS

Generate zone files using automation software

Puppet, Ansible, SaltStack, ...

It is worth it?

Technical Summary:

Automate. Monitor.

Executive Summary:

Maintain your DNS carefully