Applications & DNS

What could possible go wrong?

Nordic Domain Days 2017

kirei

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

"Applications. Why did it have to be applications?"
– me

kirei

Very dangerous – you go first!

What is this talk about?

kirei

Applications depend on DNS

Applications require DNS

Applications require DNSSEC

kirei

Why DNS?

kirei

DNS works pretty well

Fast

Scalable

Robust

Secure

(with DNSSEC)

What applications?

kirei

Since the dawn of time…

Host Address Lookup

A & AAAA

Mail Exchange

MX

Ingredients: Pork with Ham, Salt, Water, Modified Potato Starch, Sugar, Sodium Nitrite
SPAM®
Classic
U.S. INSPECTED AND PASSED BY DEPARTMENT OF AGRICULTURE
Serving Suggestion
NET WT 12 OZ (340g)

Mail Sender Policy

SPF via TXT

kirei

Domain Message Signatures

DKIM via TXT

Email Authentication Policy

DMARC via TXT

SSH Authentication

SSHFP

Authentication for SMTP

TLSA

Certificate Issuing Constraints

CAA

What happens when DNS breaks?

kirei

A & AAAA wrong ⇒

No connections

SPF wrong ⇒

Outbound mail not accepted

MX or
TLSA for SMTP wrong ⇒

Inbound mail failure

CAA wrong ⇒

No new certificates issued

So, what do you do?

Inventory

– find out what's cooking

https://hardenize.com

https://zonemaster.se

http://dnsviz.net

kirei

Detect breakage

– early warning systems

Monitor!

https://keychest.net

kirei

Local Zonemaster

kirei

Generic Monitoring Apps

Nagios, Icinga, Sensu, Zabbix, …

kirei

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

kirei