Switching to DNSSEC Won't Cause the Sky to Fall in

Similar to the character Chicken Little who hysterically believes the world is coming to an end, some Internet Service Providers (ISP) mistakenly believe that validating Domain Name System Security Extensions (DNSSEC) may deliver imminent disaster to their technical systems and customers.

However, as a number of New Zealand ISPs have proved, offering DNSSEC validation can sometimes just be a simple matter of flicking the switch.

DNSSEC have been developed to improve the security of the Domain Name System (DNS) and provide increased protection for activities such as browsing the Internet and email. DNSSEC is in the process of being rolled out internationally.

Technical Specialist for Palmerston North-based ISP *Inspire* Dave Mill says he and his team decided to configure their DNS resolvers for DNSSEC validation in July 2011.

"DNSSEC has been pushed at NZNOG (New Zealand Network Operators' Group) conferences for a while and three or four years ago we realised that all the tools were out there and we had everything we needed to just do it. So we did it," he said.

"It was a good thing for us to try and the sky didn't fall in when we flicked the switch. We checked our reports, turned it on and it just works. We knew that it was good for us to do and it was good for our customers, so we went ahead."

Senior Network Engineer Michael Fincham had similar motivations when he offered DNSSEC validation for the ISP *Unleash*.

"The motivation was essentially that I like DNSSEC and think it's important. We had just switched to using `Unbound' as a recursor and I wanted to enable it as early as possible so we escaped needing to make a "big" change by switching on validation once DNSSEC signed zones were more commonplace," Mr Fincham said.

"Enabling validation is easy. In Unbound it's a matter of a one-liner configuration change and running the bundled tool to retrieve the root keys. 'Unbound' makes the setup process straightforward and has a reputation as a generally excellent choice of recursive resolver.

"We're yet to run in to any situations where "invalid" zones have caused problems for our customers."

While *Inspire* went down the road of configuring one DNS resolver for DNSSEC validation, monitoring it for issues for a week's duration, and then configuring the remaining DNS resolvers, Mr Mills said that in retrospect a better approach would have been to just turn them all on simultaneously, which is what *Unleash* did.

DNS Specialist at New Zealand Domain Name Registry Limited Sebastian Castro says enabling validation on all the resolvers at once is a better approach because queries aim to be equally distributed amongst different servers.

“Doing it all at once stops process confusion and won’t cause breakage,” Mr Castro said.

“If they haven’t already done so, ISPs should configure their DNS resolvers for DNSSEC validation because it isn’t hard and there isn’t much excuse why not to. There are great tools to implement it (such as Unbound, Bind and PowerDNS), as well as tools for testing, the best of which are offered through VeriSign and Sandia National Laboratories.”

Mr Mills admits that being a smaller ISP probably made DNSSEC validation a bit easier for *Inspire*, but that there are so many resources available that larger ISPs should also flick the switch, enable DNSSEC and conform to best practice guidelines.

“There are a whole lot of tools out there so there is no real reason for others not to go down the same route we did. In three years we’ve had no issues whatsoever having to do with DNSSEC,” he says.

“Unbound is incredibly easy to turn on. But no matter what system you use, it’s easy. VeriSign will test it works and that your tools are doing what they say they are doing. “

For his part, Mr Fincham advocates for all recursors to perform validation, and for all zones to be signed.

“Practically speaking, though, whether it makes sense for a given "ISP" to enable validation will be a function of their environment and customer requirements,” he said.

In New Zealand, the Domain Name Commission (DNC) recommends that Registrants looking to deploy DNSSEC look for Registrars who are DNSSEC-friendly on the .nz Authorised Registrars list. This list also identifies Registrars who may not meet the criteria to be deemed DNSSEC Friendly but can accept and submit DS Records to the .nz Registry on behalf of Registrants.

Two commonly used tools to test if a website is DNSSEC-friendly or not is http://test.dnssec-or-not.com/ and dnsvis.net

Recent Asia Pacific Network Information Centre (APNIC) research confirms that along with Inspire and Unleash, FLIP, Voyager, Megatel and DTS also protect their customers with DNSSEC validation.