Back to Article

DNSSEC Deployment Heads North
By Sean Michael Kerner
October 7, 2009

TORONTO -- The global movement toward a more secure DNS infrastructure has gained another convert. The dot ca (.ca) country code Top Level Domain (ccTLD) now has an open public DNSSEC testbed to help secure the more than 1.2 million domains it manages.

The move was formally announced at the SecTor security conference underway in Toronto.

The move by dot ca places it in good company, joining other top level domains like .org in beginning to prove out and test DNSSEC in its infrastructure. Moving to DNSSEC on a global basis is a key security effort that could ultimately make the Internet safer for all.

DNSSEC provides cryptographic authentication of DNS information to ensure integrity and authenticity. The need for better DNS security became a big IT issue in mid-2008 when the Internet was rocked by the revelation that the Domain Name System (DNS), one of the core infrastructures of the Internet, was vulnerable to cache poisoning attack.

Vendors rushed out patches to the DNS vulnerability, although experts have suggested that DNSSEC is the ultimate solution to the problem. DNSSEC is a technology that has been available since at least 2004, but it is only now that adoption is growing.

Norm Ritchie, CIO of the Canadian Internet Registration Authority (CIRA), told the SecTor audience that now is the right time to test out DNSSEC. Ritchie noted that other countries and top-level domains are now testing it out and there is a lot of momentum in the global networking community for the effort.

According to Ritchie, the goal of the dot ca DNSSEC testbed is to get feedback on the process and the system ahead of a full scale deployment sometime in 2010.

The dot ca testbed is now in what Ritchie described as a 'friends and family' phase for all interested parties. Ritchie was hoping that those in the SecTor audience would be among the interested parties.

CIRA is using the services of DNSSEC vendor Xelerance in its testbed. Paul Wouters of Xelerance explained to attendees how both simple and complex it can be to actually get a dot ca domain ready for DNSSEC.

For users to enable their PCs and networks to accept DNSSEC secured domains, Wouters explained that all users need to do is to point to a DNSSEC activated DNS resolver. Wouters added that for the SecTor wireless network, such a DNS resolver was in place, meaning users were already benefiting from any DNSSEC protected domains.

For domain holders and DNS administrators, the process is a little more involved. Wouters said that with open source BIND DNS version 9.6 or higher, there are included tools to help users generate DNSSEC encryption keys.

Once a key has been generated, the user must visit the CIRA DNSSEC testbed site and manually activate the key on the dot ca servers.

While the process might seem straightforward, Wouters warned that there are risks.

"The problem with DNSSEC is if you make a mistake, your domain is gone," Wouters said. "So we've added a domain check procedure to make sure everything is okay."