Safeguarding your Domain Name with Domain Name System Security Extensions (DNSSEC)

Date : 26 Sep 2017

Organisation : Hong Kong Internet Registration Corporation Limited (HKIRC)

Writer : Mr. Leo Lam, Chief Executive Officer of HKIRC

Handling with Care – Safeguarding your Domain Name with Domain Name System Security Extensions (DNSSEC)

According to statistics disclosed by the Hong Kong Computer Emergency Response Team Coordination Centre, the number of security incident reports increased by over 23% to 6,058 reported cases in 2016 compared with 2015. The Hong Kong Police Force also revealed that in 2016, financial losses due to computer crime cases amounted to HK$2.3 billion, which recorded an increase of over 25% from the previous year. These alarming numbers remind us the crucial role of Internet security in operating our business during this digital era.

Many companies likely have some levels of digital security measures in place and that include antivirus or network security solutions. In fact, there is also a fundamental way to protect your business from cyber security threats through your website. That is where Domain Name System Security Extensions (DNSSEC) comes to play.

Many attacks targeted the Domain Name System (DNS) which is one of the basic building blocks of the Internet that translates domain names into numerical IP addresses and serves as a phone book for the Internet.

Leveraging DNSSEC as a "remedy" for the inherent flaw of DNS protocol

DNSSEC was created as an Internet security standard by the Internet Engineering Task Force (IETF) in 1997 and was adopted as the corner stone of DNS security, when a fundamental flaw was discovered in the DNS protocol in 2008, which allowed malicious hackers to inject bad data into a name server's cache.

DNSSEC was designed to conduct data origin authentication and ensure data integrity through the Key Pairs and Digital Signatures technologies. Key pairs are like keys on a safe deposit box, where you will need to use two keys simultaneously in order to open a safe deposit box. With key pairing technology, each DNS query can be verified via the "Chain-of-trust" and conduct data origin authentication. Digital signatures are also used to verify the unique identity of a DNS record. By verifying the signature with the DNS record, DNSSEC will be able to ensure data integrity.

Though DNSSEC has been effective, the adoption rate in Asia-Pacific region is comparatively low at the moment. This is because the implementation of DNSSEC requires additional monetary investments, public awareness, takes time and requires relevant expertise. Hence, corporations which adopt DNSSEC have mainly been those which require collection and storage of confidential data, like personal details, financial or transaction records, intellectual property, etc., from industries ranging from financial and banking, e-commerce, to Internet Service Providers and social media platform service providers.

Tapping on HKIRC for DNSSEC adoption

Internet security, with a relatively hefty price tag and resource investment, small and medium enterprises domain names are often left vulnerable to spoofing attacks. In order to help the local business community tackle such threats, Hong Kong Internet Registration Corporation Limited (HKIRC) has collaborated with related parties and Internet stakeholders, striving for more collaboration on DNSSEC enablement and development. The DNSSEC enabled service will be made available to the public soon. As a result, it will greatly improve the security and integrity of Internet communications and transaction data records protecting business and end users transacting on .hk domain names.

Calling for industry-wide collaboration to ensure better internet security

As a global financial hub, securing administration of domain name infrastructure in Hong Kong is crucial to the Internet community. The development of DNSSEC for.hk will bring more collaboration within the Internet community to embrace the technology for better Internet security. It is important for domain registrars, resellers and related parties in Hong Kong to collaborate and plan ahead for DNSSEC deployment in their development schedule. By working together, we could further our commitment to foster a safe Internet environment on a secured DNS for .hk -- a core part of Internet's global addressing system in the Internet world.