

DNSSEC - Are You Ready?

Devoteam Genesis AG, Your Partner for IP Address-, DNS- and DHCP Management Solutions

We all know and use DNS, the Domain Name System. Less well known, however, is the latent danger underlying DNS. In the early days of the Internet, security aspects hardly played a role for fundamental protocols and services like name resolution, web-sites and sending mail. In the rather simply configured DNS there are also no technologies implemented to prevent misuse of this service. DNSSEC, the abbreviation for DNS Security Extensions, is now going to add the missing security to the name service.

Since 1 February 2010 it has been possible to register signed .ch and .li domains with Switch. Here DNSSEC is an extension of DNS, which guarantees the authenticity and integrity of DNS responses. In professional circles it is considered as the solution for the «cache poisoning» problem. DNSSEC mainly concerns «external» DNS servers which are responsible for Internet resolution.

What this means specifically for your DNS server environment, why DNSSEC is important and how Devoteam Genesis can help you with all DNSSEC questions can be found out here!

We plan, realise and run solutions in the areas of IT service management, IT security management and IP management. We provide our customers with «best practice» complete solutions from one single source and here we work closely together with our partners of many years. Our main area of expertise is the management of IP addresses, DNS and DHCP services. Devoteam Genesis AG has offered IP management solutions for more than 10 years and has an experienced team of IP, DNS and DHCP specialists who have realised successful national and international IT projects.

Our DNSSEC consultancy package includes:

- Introduction and technical overview of DNSSEC
- Brief analysis of external DNS
- Rough preparation of a proposed DNSSEC solution
- Creation of a final report
- Presentation of the final report and the proposed solution
- Q & A

Package price 4990.00 CHF excl. VAT.

Be ready for DNSSEC! Get in touch with us. We will be happy to give you advice without obligation regarding DNSSEC in your environment and to show you possible solutions.

Ostermundigen +41 31 560 35 35
 Zürich +41 44 455 60 81
 Carouge +41 22 732 16 27
 Support +41 31 560 35 40

OVERVIEW

Devoteam Genesis AG

- founded 1996
- 40 employees in Switzerland
- since 2007 member of the Devoteam Group

Offices

Ostermundigen, Zurich, Carouge

Training Centre

Ostermundigen

Devoteam Group

- founded 1995
- with 4500 employees
- in 23 countries
- 2008 revenues € 460 million

Our IP Management Offer

- IP address management solutions
- DNS/DHCP management and appliance solutions
- DNS training
- IPv6 training



What is DNSSEC?

DNSSEC is an extension of the Domain Name System (DNS) which ensures the genuineness (authenticity) and completeness (integrity) of the data from DNS responses. DNSSEC is a type of insurance which guarantees that Internet users arrive only at the website which they looked up.

Why is DNSSEC important?

DNS is not safe! The DNS protocol does not encrypt data. This is not provided with DNSSEC either. The role of DNS is to ensure as quick as possible and efficient name resolution. But the data integrity of the DNS responses has to be guaranteed. This was not always the case in the past. DNSSEC is now an extension of the DNS protocol which, according to the latest knowledge, provides the best protection against «cache poisoning» attacks.

What is the target of DNSSEC?

Imagine someone manages to make changes in your telephone directory without you noticing. Do you have the chance to find out if the available numbers are wrong? No! On the Internet such a scenario is equally possible. If an attacker managed, for example, to smuggle false data into the server of your provider (cache poisoning), when you visit www.devoteam.ch you would be taken to another website. It is best not to imagine what could happen if the fake website is that of your bank.

Is it difficult to implement DNSSEC?

The implementation itself is not difficult. But it is necessary to use the latest DNS server versions. What is difficult, however, is the manual maintenance of zones signed with DNSSEC because every change requires «resigning» of the zone. The biggest challenge here is key management. But there are already products available today which automate the complete management and maintenance of DNSSEC-signed zones. As well as the technical aspect, organisational points also have to be considered, however.

What advantages do I have with DNSSEC?

As the person responsible for DNS, being certain of having done everything possible to protect your own company and its customers from «cache poisoning» attacks and their consequences, as an Internet user greater security in the future!

Do I definitely have to introduce DNSSEC?

From a purely technical perspective it's not necessary for the moment. DNSSEC is entirely compatible with the existing DNS. A zone signed with DNSSEC simply contains additional information. This means the zone is also correspondingly bigger. With banks and other companies such as online shops which run web platforms with sensitive data the question has to be answered with a definite yes, however. Ultimately the answer to the question also depends on how DNSSEC spreads in the coming years.

What can DNSSEC not do?

DNSSEC does not encrypt data. All DNS resource records can be viewed unencrypted. DNSSEC does not protect against DOS or DDOS attacks either.

What do I have to do next?

Our consultancy package gives you the opportunity to understand DNSSEC, shows possible solutions and what it would mean to introduce DNSSEC into your environment. This is mainly with a view to external DNS servers which can be seen on the Internet. You will find out more about running a DNSSEC solution and, as well as important information, you will also receive an evaluation of the necessary expenditure.

Whenever
you **need us,**
we are **there for you.**
That's a promise!

