CyTRAP Labs GmbH

Roentgenstrasse 49 Street
CH-8005 Zuerich Zip Code
Switzerland Country

+41(0)44 272 1876 Voice
+41(0)76 200 7778 Cell

www.CyTRAP.eu URL
info@CyTRAP.eu E-Mail

675961 VAT

DNSSEC– What is holding it up?

2008-06-24

This information outlines some data from 2006 where we already discussed the DNSSEC challenge.

DNSSEC - will the Trust Anchor Repository (TAR) make a difference?

DNSSEC - judging from the lack of existing deployments is it economically attractive?

CyTRAP Labs GmbH

2) 12 Jul 2006 - You are concerned about the DNS infrastructure? - here is what you can do to better manage your risks
Recently we pointed out that the Internet infrastructure represents a high risk regarding the reliability and dependability of networks.
Unfortunately, things do not look very rosy, see related stories. NIST has provided some specific suggestions what you should do to reduce your risk regarding the DNS server and related matters. Because of the functional impacts of attacks on the DNS, we thought you might be interested to know that you must do the following jobs to reduce your risks:

*** Implement appropriate system and network security controls for securing the DNS hosting environment, such as operating system and application patching, process isolation, and network fault tolerance.
*** Protect DNS transactions such as the update of DNS name resolution data and data replication that involve DNS nodes within the organization's control. The transactions should be protected using hash-based message authentication codes based on shared secrets, as outlined in the IETF TSIG specification. Message authentication codes (MACs) are cryptographic functions that provide assurance to the receiver of data that the sender of the data is truly the sender and that the data has not been modified since it was authenticated. A hash function is a one-way function that produces a short representation of a longer message and is used to determine whether or not data has been changed after it was transmitted.
*** Protect the ubiquitous DNS query/response transaction that could involve any DNS node in the global Internet using digital signatures based on asymmetric cryptography, as outlined in IETF's **DNSSEC** specification.
*** Enforce content control of DNS name resolution data using a set of integrity constraints that are able to provide the right balance between performance and integrity of the DNS system.

NIST recommends that organizations secure their DNS name server through the deployment of the **DNSSEC** for zone information. A zone may be either an entire domain or a domain with one or more sub-domains. A zone is a configurable entity within a name server under which information on all Internet resources pertaining to a domain and a selected set of sub-domains is described. Zones are administrative building blocks of the DNS name space, just as domains are the structural building blocks.
Protection approaches for DNS software include choice of version, installation of patches, running the version with restricted privileges, restricting other applications in the execution environment, dedicating

instances for each function, controlling the set of hosts where software is installed, placing the software properly within the network, and limiting information exposure by logical/physical partitioning of zone file data or running two name server software instances for different client classes. The latest version of name server software should be used.
<http://freebies.weburb.org/newsservice/link/4054/http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf>

CITATION
NIST Special Publication (SP 800-81) (2006-05). Secure Domain Name System (DNS) Deployment Guide. Washington, DC: The National Institute of Standards and Technology (NIST).
Finally organizations should:
- Install a **DNSSEC**-capable name server implementation.
- Check zone file(s) for any possible integrity errors. NIST SP 800-81 details the technical steps that a DNS administrator can take in generating a zone file to keep network exposure to a minimum. This process should be done prior to signing a zone to authenticate security. Network information that should be kept absolutely private should not be published in DNS at all.
- Generate an asymmetric key pair for each zone and include them in the zone file. The **DNSSEC** specifies generation and verification of digital signatures using asymmetric keys. This requires generation of a public key-private key pair. Although the **DNSSEC** specification requires the use of just one key pair, experience from pilot implementations suggests that at least two different types of keys are needed for easier routine security administration operations such as key rollover (changing of keys) and zone re-signing. NIST SP 800-81 provides guidance on the use of NIST-approved algorithms for digital signatures and for hash algorithms to be used as part of the algorithms suite for generating digital signatures.
- Sign the zone. The process for signing a zone file consists of generating a hash, generating a signature, and capturing the signature information in a file.
- Load the signed zone onto the server.
- Configure name servers that deploy **DNSSEC**-signed zones or query-signed zones to perform **DNSSEC** processing. NIST SP 800-81 discusses the mechanisms involved in the **DNSSEC** approach, the operations that those mechanisms entail, and a secure way of performing those operations by using checklists.
There is much more but you can find that important information in the Related Link provided
RELATED STORIES:
Infrastructure - Is your firm ready for an attack against its cabling

infrastructure?
- http://security.weburb.dk/frame/show/news/4026
Infrastructure - why is DNS something you should be concerned about?
- http://security.weburb.dk/frame/show/news/4052
Internet infrastructure - where are we going?
- http://security.weburb.dk/frame/show/news/4021

~~~~~~~~~~~~~~~~~~~~~~~~~~~~

2) 10 Aug 2006 - Best practice to limit DNS vulnerabilities
On of the Internet's fundamental building blocks is the distributed host information database. It is responsible for translating names into:
- addresses,
- routing mail to its proper destination, and even
- listing phone numbers (with the new ENUM standard)

But this database has to be protected.
There are several steps and deployment best practices that organizations can follow to reduce the risk of becoming a victim of an attack exploiting the address DNS vulnerabilities, such as:

1) if possible, split external name servers into authoritative name servers and forwarders,
2) on external authoritative name servers, disable recursion while on forwarders, allow only queries from your internal address space.
3) if the authoritative name servers and forwarders cannot be split, recursion must be restricted as much as possible; accordingly, only permit recursive queries if the come from the firm's internal address space
4) using secure appliances instead of systems based on general-purpose servers and operating software applications is a must
5) making sure that the server is running on the latest version of the domain name server software us required
6) traffic to and from external name servers must be filtered by using either either firewall- or router-based filters, which will help in ensuring that only authorized traffic is allowed between the organization's name servers and the internet.
<http://freebies.weburb.org/newsservice/link/4055/http://www.infoblox.com/library/dns_resources.cfm>

As the document in the related story shows, we are often too ignorant regarding the DNS and, thereby, making the organizations infrastructure assets vulnerable against various types of attacks.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

CyTRAP Labs GmbH

RELATED STORIES:
Trend - Infrastructure and cabling
- http://security.weburb.dk/frame/show/news/4017
You are concerned about the DNS infrastructure? - here is what you can do to better manage your risks
- http://security.weburb.dk/frame/show/news/4054

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~