Disturbance of the Name Service for .de Domains on May, 12th 2010

Joerg Schweiger

<schweiger@denic.de>

ICANN / ccNSO Meeting, Cartagena, December 2010

Outline

1. Impact
2. Chronology of the incident from an external perspective
3. Incident handling
   - Analysis
   - Confining and fixing the bug
4. Follow-up actions and respective status

Impact

What happened?

12 of DENIC's 16 name server locations loaded a zone file that contained only about one third of the .de domain records

Effect

- ➔ NXDOMAIN replies for domains that did actually existing
- ➔ Undeliverable e-mails
- ➔ Effects on various other applications (using the DNS)

„Proclaimer“ : Other zones served and cooperation partner weren‘t effected!

Chronology of the incident from an external perspective

… DENIC received calls from the community that "*something's wrong with the internet*" and thus initially became aware of the problem

➔ count ZERO of incident handling

•00:00 + 1 hour

… Exclusively correct answers were given again,

… although service capacity was not yet fully restored

•00:00 + 2 hours

… The entire capacity / performance was restored

•00:00 + 3.5 hours

… The standard zone data provision process (including the most up-to-date data)

was fully restored

Incident handling

Step 1: Analysis

The Incident handling team was summoned immediately to analyse, confine and fix the problem

¿ A root server problem ?	No, but we were seeing a disproportionate number of NX replies! →
¿ Does a bug in the registration software result in a "corrupt" database ?	No!
¿ Was a corrupt zone file generated ?	No!
¿ Was the check guarding the copy operation from the zone generating server to the zone distribution server negative ?	No!
¿ Was the plausibility check negative that verifies if the copy of the zone file is authentic (MD5 hash)?	No!
¿ Is there any bug in the protocol software that will have an impact on the zone file loading at the distributed remote name server locations ?	No!

¿ **…if not so, what actually *did* happen ?**

Root cause

We conducted a **project** to innovate our name server architecture resulting in a successive roll-out processes of **new equipment to the name server locations**.

For duration of the parallel operation of "old" and "new" name server locations, we **adopted the zone distribution process**.

To serve as data source for the new locations the correctly generated, plausibility-checked and securely transmitted **zone file is copied** once **again**, from one directory of the zone distribution server to another.

This copy failed … because of insufficient disk space !

… and wasn't observed because the particular server had not yet been integrated into the standard monitoring for the transition period !

Incident handling

Step 2: Confining and Fixing the Bug

1. Eliminate the storage problem
2. Successively shut down and restart the locations using the latest intact predecessor version of the zone file
3. Re-establish the standard process

Follow-up actions and status (1)

Ad-hoc Measures	Status
• Implement and deploy a MD5 check of the copying process on the distribution server and • Implement a switch to interrupt automatic processing in case of faulty results	done
• Integrate the respective server in the standard hard disk monitoring	done
• Script for deleting outdated zone files from the distribution server	done

Follow-up actions and status (2)

Medium-termed Actions	Status
• Provide a "backup zone" at each name server location and implement an automated rollback mechanism to activate the backup zone or	under test
• Install a stand-by server for each location to run an old (1 day) zone to switch to in case of an emergency (corrupt new zone)	under test

Incident Handling	Status
• Envision potential security incidents and respective optimized counter action plans	30 Dec 2010
• Fast and efficient mechanisms to summon the incident handling team	30 Dec 2010
• Implement emergency switches “name server locations on / off"	done
• Review DNS monitoring functionalities	31 Dec 2010

Follow-up actions and status (3)

Process Improvement	Status
• Live-up to the defined change-/ release management processes	On-going
• Leverage of a professional service management and configuration management database tool	done
• Define an incident response process	done
• Review crisis communication	done
• Recruit an "Information Security Officer"	done

Quality Assurance Measures	Status
• IT operations audit	1st quarter 2011

Questions / Comments

?

Joerg Schweiger
schweiger@denic.de
+49 69 27235 -455

Process to publishing a zone