Swedish Post and Telecom Agency (PTS)
Internet security division
Attn: Camilla Grimelund Thomsen
Box 5398
SE-103 91 Stockholm
Sweden

Stockholm, November 12, 2009

Information regarding the disruption of the domain name system under the Swedish top-level domain .se (Your reference document number 09-9940)

In a statement dated October 14, 2009, PTS requested information regarding the disruption on October 12, 2009 in the domain name system under the top-level domain .se. In its statement, PTS requested that .SE submit information and account for a number of points, as presented below.

1. **A full description of the circumstances regarding the disruption on October 12, 2009, which shall include the cause and scope of the disruption.**

.SE's response: In conjunction with scheduled maintenance work on the evening of Monday, October 12, 2009, a defective zone file was distributed at 9:39 p.m. The cause of the problem was a defective program update, which was not detected despite .SE's test procedures and controls. The updated software was missing the trailing dot in .se. In such cases, the Bind program automatically adds ".se" to all domain names. This resulted in all domain names in the .se zone being changed so as to read **domainname.se.se.**

As a result of a well-functioning monitoring system, .SE immediately detected the defect, troubleshooting commenced and a new file containing DNS information (a zone file) was produced and distributed within an hour.

After 30 minutes, the crisis management organisation was aware of conditions and could follow the recovery work, while working in parallel on spreading information.

The cause of the incident was a number of coinciding events and circumstances, which when combined, resulted in the defective software being applied. The process leading

from the development to the application of new and changed software can generally be described as follows:

During the development process, every altered system component is tested in a separate development environment. The tests consist of manual function tests with test cases that are adapted to the system changed that occurred and shall be implemented by two independent developers. Prior to the delivery of a release, the entire integrated production system is tested using automated function tests with predefined test cases, known as pure tests. Following an approved test, the release is delivered to the commissioning organization.

During the incident in question, the manual function tests performed on the concerned program modules for zone generation failed, and the test was only performed by one developer (not two, as stipulated by the procedures). The automatic tests do not encompass zone generation either, which rendered the defect more difficult to detect.

The commissioning organization performs routine function tests and specific tests of the new functionality commissioned as part of the acceptance tests. These are limited to that which can be performed by way of the interactive user interfaces offered by the system. The commissioner subsequently approves the delivery and grants authorization for activation.

The commissioning organization does not test the zone generation and thus did not detect the defect during this phase either.

The operating organization performs an installation in a test stage pursuant to the documentation delivered by the development division. This documentation specifies the program corrections and new functions contained in the release. The document also specifies what program packages shall be installed in what server platforms and what configuration changes shall be made. In addition, the package must include instructions regarding the preparations that shall be made (such as what services are to be turned off and the temporary unplugging of surveillance), how to perform the installation (installing the package and launching services), what tests to perform following the installation and launch, and the routines for backtracking if problems arise. In addition, the commissioning organization performs a number of basic function tests to verify that the system's components are cooperating.

The documentation that was delivered with the release in question did not contain any specific tests for the validity of the zone file, or any specific actions to stop zone distribution during the work. The documentation was also missing a description of the changes that were made to the zone generation program.

The operation division's own routine tests do not encompass loading and testing the generated zone file to ensure its validity and thus the defect went undetected during this phase as well.

Activation in the production environment takes place on a scheduled and announced service occasion. On this occasion, one person from the development department must assist the responsible operations technician. Activation is carried out following the same documentation as for the test installation.

In this case, activation was carried out following the same documentation as in the test stage. Accordingly, no specific test of the zone file's validity was performed, nor was the scheduled zone distribution stopped. The automatic blocks that prevent unusually large changes to the zone file were deployed. Following a visual inspection of the generated data during which the missing dot was not detected, a decision was made to force the distribution of the defective zone file. Accordingly, the defective information was published via .SE's slave server operator.

The zone generator is a particularly critical component of .SE's operations, which .SE's technicians are aware of. An aggravating circumstance of the incident was that a senior system administrator had fallen acutely ill, which caused a less experienced system administrator to implement the activation of the new release. According to the applicable routines, the change should not have been implemented with only one system administrator on-site.

Another contributing factor was that the system administrator who performed the change was not familiar with the specifics of how the zone signing functioned and did not have access to the machine that conducts the zone signing. Accordingly, a decision was also made to distribute a zone file with the correct information, but with an incorrect SOA signature for .se. Given the circumstances, this was the right decision and one which enabled the contamination of the cache in the name-resolver program to be stopped.

2. **A description of the implications of the aforementioned disruption, such as its affect on the domain name system and the implications for various players, including name-server operators, domain-name holders and end users.**

.SE's response: Overall, the time of day, the scarce monitoring of our system, .SE's crisis-management contingency, the speed at which corrections were made and our strong contacts with name-server operators in Sweden were to our advantage and resulted in the implications of the aforementioned incident being far less severe than they could have been.

The defective information that was distributed resulted in complications regarding accessibility to all .se domains during the period in which the defective information was published. At the same time, the information in the name-resolver services was cached on the Internet for a certain period of time, and for many end users, everything functioned as usual. In .SE's opinion, the implications for domain-name holders and end users were mild, while efforts were required on the part of name-server operators (ISPs, registrars och web hosting providers) and probably resulted in activities in the form of trouble shooting and customer support.

.SE has not received any formal complaints or damage claims.

The defect was successively detected and corrected during the evening, and by 1:00 a.m. on Tuesday, October 13, the .se zone was fully functioning. However, defective information remained cached in the name-resolver services, which was beyond the control of .SE. Name-resolver services that requested .se domains during the period in which the defective zone was published (approximately 9:40 p.m. – 10:50 p.m. CEST[1],) received failure responses that remained cached for up to one day. Requests regarding the .se zone itself, such as DNS directors and SOA posts, were cached for up to two days. Residual effects from the event could also theoretically have occurred for up to 48 hours. However, according to .SE's monitoring and trouble shooting, all visible residual effects were ended as early as 24 hours later.

Slightly more than an hour after the incident, an interim zone was published. The interim zone had the correct zone information but contained an invalid DNSSEC signature. Accordingly, the contamination of the cache in the name-resolver software stopped. During the period in which the interim zone was published (approximately 10:50 p.m. – 00:55 a.m. CEST), Internet users mainly received the correct response, with the exception of cases in which the name resolver required SOA DNSSEC validation for .se. These situations led to request denials as well as implementation dependence.

3. **Detailed description of the actions taken by .SE concerning the incident. This description shall include the actions taken by .SE to reduce the implications of the disruption and whether routines were in place to manage the incident and, if so, if these can be described or if a statement can be attached.**

.SE's response: One of the first actions is presented in response two above, namely the distribution of an interim zone to immediately stop the contamination of the cache in the name-resolver software. Through direct contacts with several major Swedish Internet operators, the effects of the disruption were minimized since these operators manually purged the name-resolver services' caches as soon as the interim zone was published, thus avoiding the protracted effects that the matter could have resulted in.

.SE also backtracked to a previous version of the zone generation script. Documentation is available concerning routines for the management of backtracks, incidents and more extensive crises. Incident-management routines applicable to the event concerned are described in brief as follows:

The office and production operating environments are monitored and any alerts can be automatically received from .SE's monitoring system or by someone reporting a defect through customer service, an emergency telephone number or e-mail.

Automatic alerts are always sent SMS to .SE's emergency telephone number. Depending on the nature of the warning, alerts can also be sent to other people in the organization through other channels, such as e-mail. During normal office hours, incidents are generally managed by technical operation personnel. After normal office hours, incidents are handled by on-call personnel. The party handling the alert makes an assessment

[1] Central European Summer Time

based on the type of alert, statistics and personal inspections. When in doubt, other parties are contacted for consultation. If this occurs after normal working hours, people from the on-call group are those primarily contacted. Depending on the results of the assessment, the following functions may be contacted:

- In the case of issues stemming from the distribution of zone files in which .SE's partners must be notified, the on-call personnel for .SE's slave server operations shall be contacted.
- In the case of matters that require administrative/legal counsel, the appropriate member of .SE's management shall be contacted.
- In the case of security-related matters, .SE's quality and security manger shall be contacted.

When an incident is deemed to have the potential to lead to a crisis, .SE's crisis-management plan is activated. The crisis-management team makes a preliminary assessment of the nature of the crisis. The crisis-management team subsequently follows the instructions specified in the crisis-management plan. The crisis-management team decides what functions are to actively work with the team, taking into account the current scenario, meaning what work groups shall be drafted. Those who are not affected by the crisis return to their regular tasks. A task manager is appointed and leaves the crisis-management team to activate the crisis plan and head the operational management of the crisis. This involves assembling the resources necessary to manage the crisis, inform them of the situation and perform an analysis of the incident according to a checklist. The task manager reports the results of the analysis to the crisis-management team.

During the incident on October 12, the technical personnel in question were already on-site due to scheduled maintenance work, and the cause of the event was thus promptly identified and a correction was initiated essentially immediately. Accordingly, .SE categorizes the event as a serious incident rather than a crisis situation.

4. **A description of the information regarding the disruption submitted by .SE to the concerned players (such as name-server operators, domain-name holders and end users) and when and how this took place.**

.SE's response:
October 12
In conjunction with the activation of the crisis plan at 11:06 p.m., a number of activities were initiated including the dissemination of information.

At 11:06 p.m., the security manager notifies the information manager and customer service manager of the events and tells them to prepare for contact with the press and customers, respectively. Ongoing contact with the information manager is maintained until 1:00 a.m.

At 11:10 p.m., .SE's CEO contacts *Aftonbladet* newspaper; at 11:16 p.m., the TT news service is contacted; and at 11:45 p.m., *Expressen* is notified. The reasoning behind this is that the information will reach domain-name holders and end-users quicker through the media than if .SE uses resources posting the information on its website.

At 11:27 p.m., the security manager notifies the crisis management team of the status of the events by e-mail.

At 11:33 p.m., the CEO notifies the Board of Directors of the status of the incident by e-mail.

At 12:12 a.m., the security manager notifies .SE's DNS reference group, which included most major Swedish name-server operators, of the status of the incident.

At 1:05 a.m., the security manager advises the crisis-management team that the problem has been resolved and announces a return to standard operations.

October 13
At 7:02 a.m., internal information is distributed to notify customer service staff and other personnel. All press contact is referred to the information manager or CEO.

At 7:11 a.m., brief information is provided to the Swedish Post and Telecom Agency, the supervising authority.

At 8:24 a.m., information is sent to the DNS reference group list with advice on how to purge the resolvers.

At 8:30 a.m., a scheduled status meeting is held with the concerned members of the crisis-management team to obtain as much information as possible, and an internal investigation headed by the security manager is initiated.

At 9:31 a.m., the information is compiled in a document that is distributed internally and posted on .SE's website.

At 9:30 a.m., the information is sent to the SOF group by e-mail.

At 9:48 a.m., brief information is sent to .SE's registrars in Swedish.

At 10:17 a.m., brief information is sent to .SE's registrars in English.

At 11:19 a.m., supplementary information is sent to PTS.

October 14
Detailed information regarding the incident is posted on .SE's website and sent to .SE's registrars and to the DNS reference group.

October 15
Detailed information regarding the incident is sent to CENTR Full Members.
PTS is updated regarding the information that was sent to Registrars and DNS operators.

5. **A description of future measures that .SE plans to implement to avoid similar disruptions from occurring.**

.SE's response: The most urgent actions taken were naturally to investigate the incident on October 12. An internal investigation commenced immediately on the morning of October 13. Two separate external investigations were subsequently initiated: one technically oriented investigation and one more focused on organization, responsibilities and routines. The IT operations group was reinforced with a temporary senior operations technician.

One thing we established early on is that we are lacking channels for reaching ISPs/web hosting providers and resolver operators located outside of Sweden. Therefore we have started a global improvement initiative aiming at finding forms of creating a possibility to get this kind of contact information to all the large operators around the world, if need be. We have started discussions with various parties on this issue.

Furthermore, .SE has distributed a generic request to all concerned players for suggestions for internal and external improvement measures. Submitted suggestions are being compiled, analyzed and prioritized. We are working on the formulation of an action plan based on these suggested measures and those improvement proposals that have surfaced in both the internal and external inquiries. Our routines have also been tightened up.

This work is being coordinated by .SE's security manger. A steering group has been appointed to make decisions regarding prioritizations and establishing who is responsible for implementing actions. Specific resources have been allocated for the additional expenses caused by the incident. The incident and the management thereof eill continue to be discussed in .SE's Board of Directors at a meeting on November 23.

We welcome a meeting with PTS representatives if so desired, for a more comprehensive review of the actions taken and will be taken.

Danny Aerts,
CEO