Philosophy behind the workflow documentation effort

- The general workflow should be efficient but very flexible
- Where large amounts of very typical, more or less equal incidents occur, create a very specificic workflow, much less flexible, but possibly much more efficient. Think about open relays, portscans.

Different actors within CERT-NL

- CERT-NL officer on duty (1 week shift)
- CERT-NL backoffice staff (2 persons parttime)

The CERT-NL octopus within SURFnet

CERT-NL staff have direct access to:

- Site Security Contacts (customers)
- Customer interface (SURFnet Account Management)
- SARA (the day-to-day management of the SURFnet backbone)
- Escalation path (CERT-NL Steering Group, consisting of the chair and both the SURFnet managing directors

---

General procedure

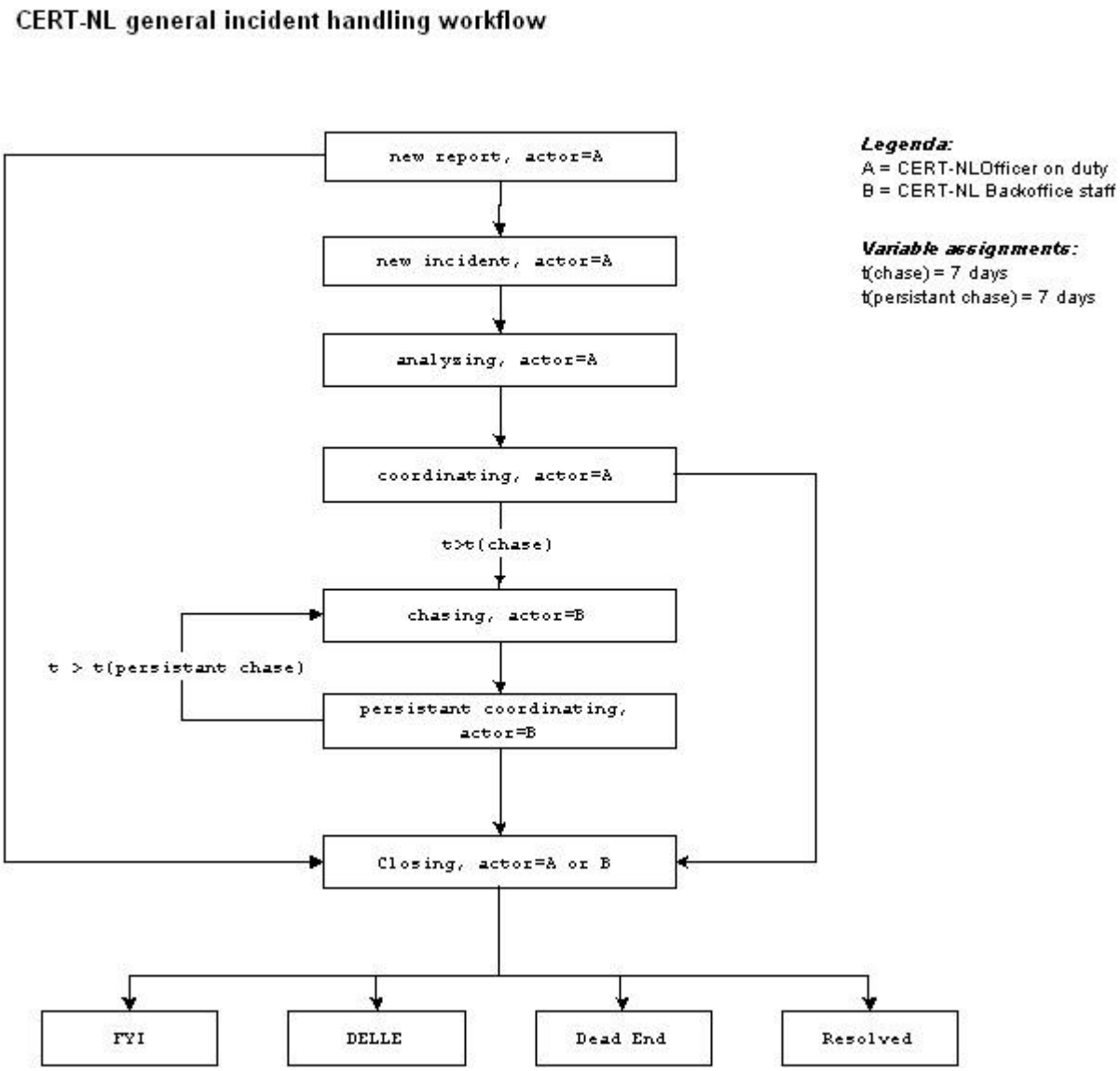

Figure 1: CERT-NL general workflow

Try-out diagrams:

State-event diagram

Process-diagram

Open relay procedure

CERT-NL does not handle spam issues as such, though when we receive complaints about SURFnet users sending out spam we will pass the complaint on to the Site Security Contact. These type of incidents are NOT security incidents, but a complaint has been filed, so something properly needs to be done with it. Let the Site Security Contact handle it. When an open relay is found, this does consist a security incident (Denial of Service of the MTA, usually). CERT-NL has a specific procedure to deal with open mailrelays at customers' sites that consists of three stages, each stage involving persons higher up the contact-person hierarchy:

1st stage: contact the Site Security contact

The Site Security Contact is informed about the open relay and asked to close it. This is done using a standard template containing all the nessecary information needed: what is the problem, why solve it, pointers to how to close open relays. Someone lacking the specific knowledge should be able to close an open relay this way.

2nd stage: contact the Site Security contact again and Cc: the general customer contact person (ICP)

The Site Security Contact either did not respond or did not close the open relay. A notification stating "The open relay is still open, please close it within (n) days, otherwise SURFnet will start filtering port 25 on your connection except for the mailhosts in the mx-records of the primary domain of the organization"

3rd stage: contact the Site Security Contact, the ICP and the general manager of the computing department of the customer

Still no response, the relay is still open, SURFnet will filter as promised until the problem has gone away.

Notes:

- A lot of SURFnet customers have decentralized mailinfrastructures, in which faculties have their own MTAs. These MTAs will be affected by the suggested filtering method
- The 3rd stage has never needed to be used

CERT-NL open relay incident handling workflow

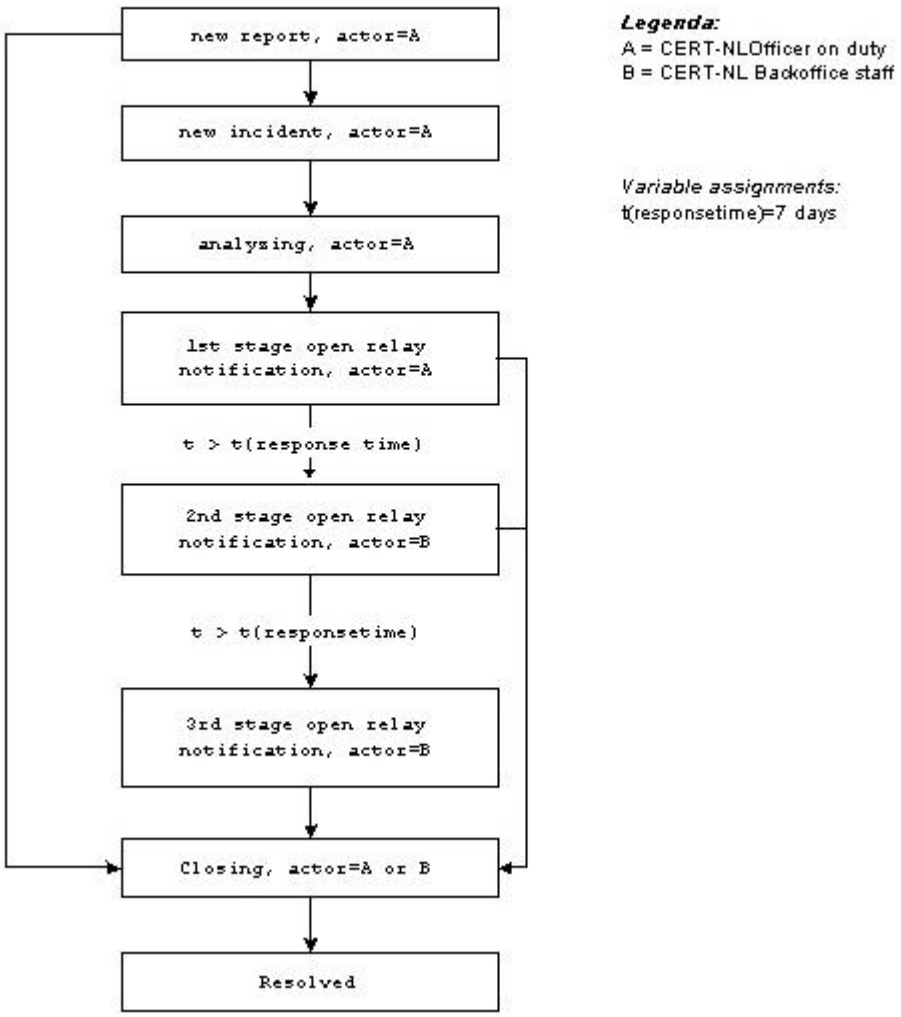

Figure 1: CERT-NL open relay incident workflow

Back to the table of contents

The actors