

Emergency Backup Infrastructures for CSIRTs

How will CSIRTs face a network breakdown ?

Gilles ANDRÉ

gilles.andre@certa.ssi.gouv.fr

CERTA

Background

Emergency Backup Infrastructures for CSIRTs

- whatever happen we need to be able to keep in touch
- the network we use to keep in touch might collapse
- thus we need another (backup) network

Purpose of the project

Emergency Backup Infrastructures for CSIRTs

To identify in general terms, the potential threats to the European communication infrastructure. To identify alternative methods of communication that will enable information to be passed between CSIRTs with experiment as an objective.

Threat assessment

Emergency Backup Infrastructures for CSIRTs

- first thoughts about such a backup infrastructure came from the fear that both Internet *and* phone network collapse at the same time ;
- we investigated about the probability of such an event.

Threat assesment : both phone and Internet collapsed

Emergency Backup Infrastructures for CSIRTs

- it had already happen ...
 - because of physical failure due mainly to weather related events (storms, floods, tornados, blizzard, ...) or human failure (digging the street and cut a cable, ...)
 - at a local level (district, town, region, ...)
 - could be solved at a local level (no need for a coordination with other CSIRTs to manage the outcomes of a storm ...)

Threat assesment : whole Europe out of network ?

Emergency Backup Infrastructures for CSIRTs

- while a breakdown can happen in a significant part of Europe, yet we couldn't define a scenario where the attack would be so huge that all means of communication between CSIRTs are disabled
- anyway if such a problem should occur, then CSIRT coordination might a secondary importance regarding the situation
- your input is welcome

Threat assesment : without phone *or* without Internet

Emergency Backup Infrastructures for CSIRTs

our analysis is for the moment :

- the threat analysis for a breakdown of both phone and Internet is to be continued
- a failure of phone *or* Internet for a significant period of time is far more probable
- we should study first how to react to such a risk

Alternative methods communication

Emergency Backup Infrastructures for CSIRTs

There are known solutions to the identified risk :

- phone failure :
 - voice over IP, ...
- Internet failure :
 - modems, ...

But trusted introducer does not take into account these contact information.

Proposal

Emergency Backup Infrastructures for CSIRTs

- identify standard backup solution
- identify the benefit and risk of these solution
- agree on common protocols
- propose an upgrade of trusted introducer information
- ongoing process of threat assesment