Il servizio GARR-CERT

Roberto Cecchini

II Incontro di GARR-B

Napoli, 17-18 Gennaio 2000

GARR-CERT

- Il servizio
  - istituito nel Marzo 1999, pienamente operativo da Giugno 1999;
  - 8 unità: 2 a tempo pieno e 6 a tempo parziale.
- Gli utenti sono tutte le istituzioni afferenti alla rete GARR.
- I compiti
  - rispondere alle segnalazioni di incidenti, avvertire ed assistere gli utenti coinvolti e seguire gli sviluppi;
    - politica di riservatezza
  - diffondere informazioni sulle vulnerabilità più comuni e sugli strumenti di sicurezza da adottare;
  - controllare periodicamente "lo stato di salute" dell'utenza per le vulnerabilità più gravi o più comuni;
  - gestire corsi di aggiornamento tecnico;
  - provare strumenti esistenti, e svilupparne di nuovi per esigenze specifiche.

Chi siamo

- Membri
  - Roberto Cecchini (coordinatore) <Roberto.Cecchini@fi.infn.it>
  - Claudio Allocchio <Claudio.Allocchio@elettra.trieste.it>
  - Paolo Amendola <Paolo.Amendola@ba.infn.it>
  - Luca dell'Agnello <luca.dellagnello@cnaf.infn.it>
  - Francesco Gennai <Francesco.Gennai@iat.cnr.it>
  - Enrico Morandi <Enrico.Morandi@fi.infn.it>
  - Francesco Palmieri <fpalmier@unina.it>
  - Andrea Pinzani <Andrea.Pinzani@fi.infn.it>
- Chiavi PGP

```
Type  bits        keyID      Date       User ID
RSA   1024       0x0C5C2A09 1995/10/21 Claudio Allocchio
RSA   1024       0x12DA1A6D 1998/06/26 Paolo Amendola
RSA   2048       0x22646D49 1999/03/09 Luca dell'Agnello
RSA   1024       0x5BA9D271 1997/11/25 Roberto Cecchini
RSA   1024       0x839FFA81 1999/06/22 Enrico Morandi
DSS   4096/1024  0xD96E620F 1998/12/25 Francesco Palmieri
RSA   1024       0x829622DD 1999/09/10 Andrea Pinzani
```

Procedura di gestione incidenti

- **http://www.cert.garr.it/incidenti.php3**
  (approvata dall'OTS GARR il 20/12/99)
  1. GARR-CERT invia una comunicazione di apertura incidente ai responsabili locali coinvolti e all'APM;
  2. se il problema non viene risolto GARR-CERT invia all'APM la richiesta di filtraggio sul router di connessione alla rete GARR;
  3. se l'APM non interviene entro i tempi richiesti, GARR-CERT invia al GARR-NOC la richiesta di filtraggio sul router di accesso al GARR.
- Tempi di intervento richiesti:
  - open mail relay: **3 giorni**;
  - nodi origine di azioni ostili (*port scan*, attacchi, ecc.): **1 giorno**;
  - router utilizzati per attacchi DoS (ad es. *smurf*) perché erroneamente configurati: **1 ora**.

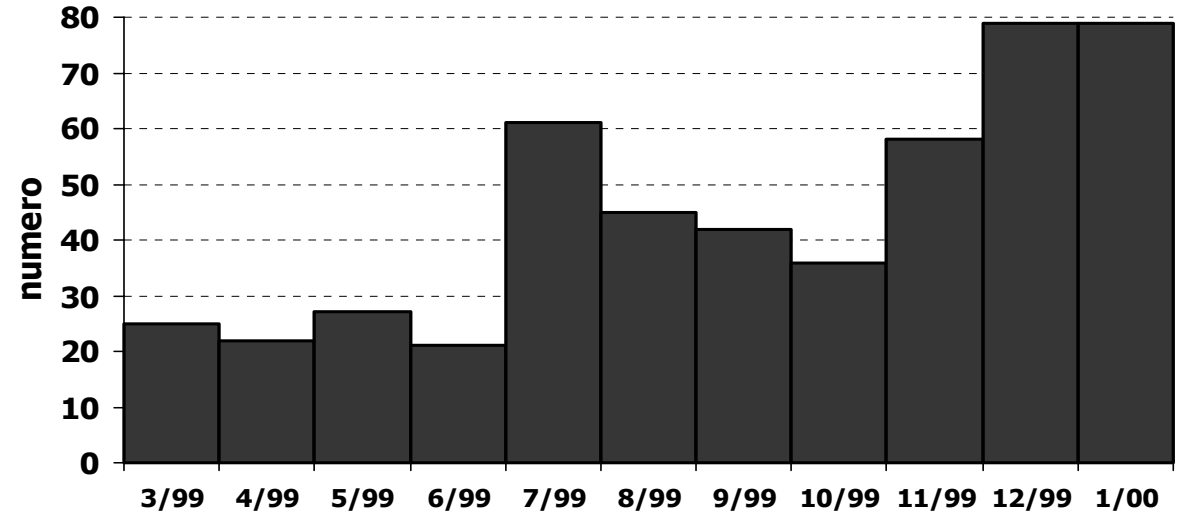
Servizi (1/2)

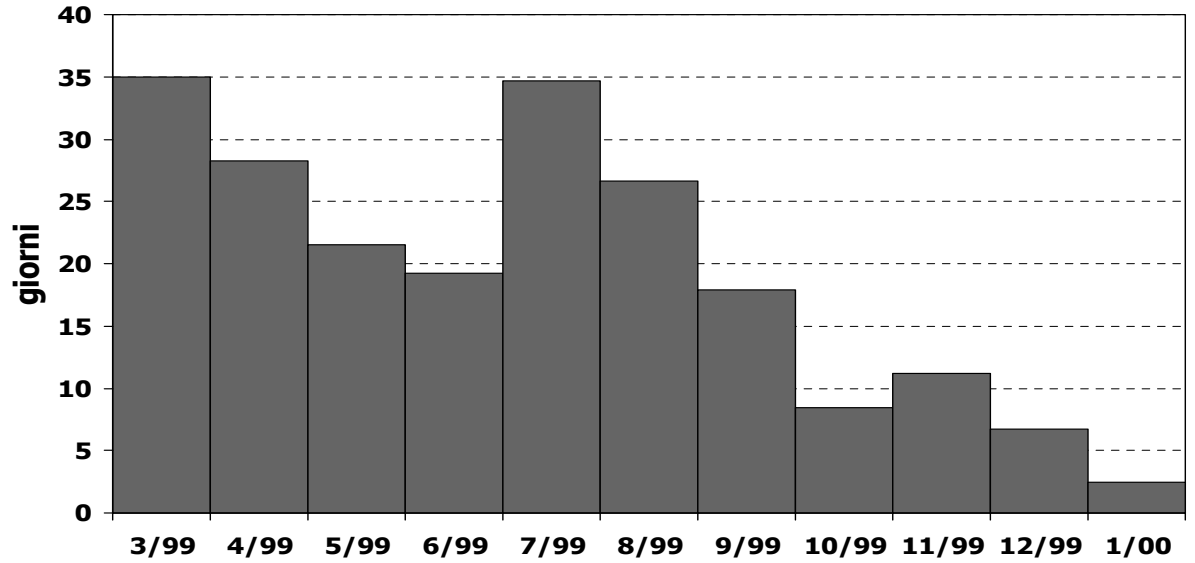
- Server web
  - **http://www.cert.garr.it/**
- Mailing list
  - **cert@garr.it**
    - gli iscritti sono i membri di GARR-CERT;
    - riceve anche i mail diretti ad **abuse@garr.it**;
    - chiunque può (e dovrebbe) usarlo per segnalare incidenti.
  - **sicurezza@garr.it**
    - segnalazione di allarmi di sicurezza
    - comunicazioni di interesse generale
    - iscrizione aperta a tutti

Servizi (2/2)

- Documenti (reperibili sul server web)
  - L. dell'Agnello, *Guida alla configurazione sicura del router*.
  - L. dell'Agnello, *Installazione e configurazione di Berkeley sendmail su piattaforma Unix*.
  - P. Amendola, *Virus diffusi via e-mail*.
  - P. Amendola, *SSH* (in preparazione).
- Security Alerts (P. Amendola)
  - più di 100 nello scorso anno;
  - tabelle riepilogative (A. Pinzani).
- Scansioni alla ricerca di problemi di sicurezza (F. Palmieri)
  - individuazione open mail relay (2)
  - individuazione reti amplificatrici broadcast (2)
    - l'ultima scansione ha prodotto 265 segnalazioni, i casi risolti sono il 55% (al 13/1)
- Controllo vulnerabiltà (su richiesta dell'APM).

Numero e durata degli incidenti





solo 13 giorni

Incidenti suddivisi per tipo