# Progetto “Sicurezza”

## Piano di attività

GRUPPO DI LAVORO SULLA SICUREZZA

Roberto Alfieri, Paolo Amendola, Cristina Bulfon, Roberto Cecchini,
Luca dell’Agnello, Enrico Fasanelli, Massimo Gravino, Michele Michelotto

17 Maggio 1999

# 1 Introduzione

La crescita esponenziale degli incidenti di sicurezza (si vedano, per esempio, le statistiche del CERT/CC o anche, più semplicemente, quello che è accaduto su alcune reti locali INFN nei mesi scorsi) è un fenomeno, purtroppo, incontrovertibile.

Senza entrare qui nel merito delle cause, è però ormai evidente la necessità di dotarsi di un servizio per la gestione e *prevenzione* di questo tipo di eventi.

Il fatto che l'analogo servizio per GARR-B sia stato dato in gestione proprio all'INFN ci permette di realizzare delle economie, evitando la duplicazione di alcune funzionalità. Bisogna anche notare, però, che le funzionalità dei due servizi non possono essere completamente sovrapponibili.

# 2 Obiettivi

Lo scopo del progetto è portare tutti i nodi INFN ad un "ragionevole" livello di sicurezza e riuscire a mantenerlo almeno costante per il futuro. Tutto cercando di automatizzare il più possibile le varie operazioni di controllo e aggiornamento che si rendano necessarie, in modo da non gravare eccessivamente sul carico di lavoro, già molto pesante, dei responsabili locali del calcolo.

# 3 Piano di lavoro

## 3.1 Scopo

Abbiamo ritenuto opportuno dividere l'attività del gruppo in tre parti:

1. attività istituzionali, e quindi senza scadenza precisa, che consentano il mantenimento dello *statu quo*;
2. attività di esecuzione relativamente rapida, che permettano un significativo incremento della sicurezza media (**FASE I**): vedi però i prerequisiti necessari.;
3. attività di più ampio respiro che permettano a tutti i nodi di raggiungere il livello di sicurezza ritenuto accettabile (**FASE II**).

## 3.2 Attività istituzionali

Visto che il servizio di CERT per GARR-B (**GARR-CERT**) è stato affidato proprio all'INFN, ci sembra inutile duplicare alcune funzioni, in particolare quelle di gestione incidenti, *help desk* e *security alert*[1].

[1] È previsto che la mailing list sec-manager@infn.it sia iscritta a security@garr.it (la lista *dei security alert* per la rete

Riteniamo invece che debbano essere mantenute le attività seguenti, perché interessano aspetti specifici dell'utenza INFN.

- Gestione del server web del gruppo.
- Attività di aggiornamento dell'utenza.
- Gestione della Certification Authority dell'INFN.
  Alla luce della pubblicazione sulla GU (n. 87 del 15/4/1999) delle regole tecniche per l'attuazione dell'Articolo 3 del DPR 10/11/1997 n. 513 che consente alle PA *di "istituire e gestire autonomamente servizi di certificazione per le firme digitali utilizzate nell'ambito dell'organizzazione interna degli uffici"* (Art. 62, Comma I), ci sembra importante continuare a mantenere questa attività.
  Tra l'altro, la Certification Authority può essere usata per garantire anche i certificati e le chiavi PGP dei membri di GARR-CERT.
- Mantenimento delle competenze del gruppo allo stato dell'arte del settore.
- Sviluppo di nuovi tools e prova di quelli esistenti.
- Servizio di *auditing*.

### 3.2.1 Fase I

Lo scopo di questa fase è principalmente quello di mettere al riparo il maggior numero possibile di LAN dagli attacchi degli *script kiddies* (cioè da persone tecnicamente non molto preparate, ma che hanno a disposizione tutta una serie di strumenti, anche molto sofisticati, già pronti e facilmente reperibili in rete) con il minor impiego possibile di risorse, sia dei membri del gruppo, sia dei responsabili locali del calcolo.

### 3.2.2 FASE II

Lo scopo di questa fase è di giungere ad una situazione "di regime" (per quello che riguarda la sicurezza). A questo fine deve essere nota, **e mantenibile tale**, la configurazione di tutto l'installato e deve essere controllabile l'accesso di **tutte** le LAN.

Per questo motivo riteniamo necessaria l'istituzione di una distribuzione di Linux "chiavi in mano", che non solo metta in grado chiunque di installare per conto proprio un sistema sicuro senza particolari competenze (a differenza di quanto succede con, ad esempio, Red Hat standard), ma permetta poi di *mantenere* il sistema aggiornato con le ultime versioni di software (ove non ci siano specifiche esigenze contrarie).

Sulla stessa linea va la proposta dell'istituzione di server dedicati, cioè senza utenti, per tutti i servizi essenziali (dns, mail, news, afs, ecc.). In questo modo, non solo si migliora la sicurezza dei sistemi, ma, raggiungendo una situazione standardizzata, si rende possibile l'automazione del servizio di aggiornamento del software (o, almeno, si facilita molto il compito dei responsabili locali).

È necessario inoltre, per ridurre i danni di eventuali intrusioni, l'eliminazione, o almeno la riduzione al minimo, della trasmissione di password in chiaro, visto che l'installazione di uno *sniffer* è una delle prime cose che viene fatta appena una macchina è stata compromessa.

Infine, visto la loro preponderanza, è indispensabile un'attenzione ai problemi della sicurezza delle piattaforme Windows (NT, perché non riteniamo le 9x difendibili), anche tenendo conto dei problemi legati alla nostra situazione: distribuzione su area geografica, configurazione remota (**NICE**), ecc..

## 3.3 Metodologia

Per un migliore controllo della realizzazione degli obiettivi proposti, sono stati specificati un considerevole numero di task e subtask relativamente elementari. Buona parte di questi hanno come

---

GARR), rimanendo sempre disponibile per le segnalazioni di interesse specifico INFN.

deliverables dei documenti, che saranno prontamente resi disponibili sul web server del gruppo (Task **P-1**).

## 3.4 Presupposti

Il primo, e fondamentale, presupposto è la collaborazione dei system manager locali, che dovranno accollarsi anche l'onere di rivestire la figura di security manager. Ci rendiamo conto che l'aggravio di lavoro sarà sicuramente pesante, siamo però ragionevolmente certi che, dopo una fase iniziale, dovrebbe ridursi a livelli accettabili.

Teniamo anche conto che gli incidenti di sicurezza si traducono sempre in un *enorme* aggravio di lavoro per i responsabili dei sistemi coinvolti.

Per quello che riguarda la **FASE I**, il presupposto fondamentale è che sia possibile filtrare tutti i pacchetti in ingresso alla LAN, e cioè il controllo del router. Dove questo non sia possibile, la messa in sicurezza richiederebbe la verifica delle configurazioni di *tutte* le macchine, cosa questa difficilmente realizzabile a breve scadenza.

# 4 Compiti dettagliati

Le cifre di manpower sono *globali*, quando però si è ritenuto opportuno abbiamo anche indicato tra parentesi il numero dei componenti del gruppo di lavoro.

Tra le attività istituzionali, poi, tutti i task, tranne **P-6.1**, sono da considerarsi *permanenti*, estesi cioè per tutta la durata del progetto: *le cifre sono quindi da intendersi per ogni anno*.

## 4.1 Attività istituzionali

- **Task P-1 (Server web) : 0.1 FTE**
  - Gestione del server web del gruppo
    **R. Cecchini**
- **Task P-2 (Aggiornamento utenza) : 0.2 FTE (2 persone)**
  - Attività di aggiornamento dell'utenza: corsi, documenti esplicativi, note d'uso, ecc..
- **Task P-3 (Gestione INFN CA) : 0.05 FTE**
  - Gestione della Certification Authority dell'INFN: rilascio di certificati X509 per utenti, server e software, firma di chiavi PGP.
    **R. Cecchini**
- **Task P-4 (Autoaggiornamento) : 0.05 FTE (per ogni membro del gruppo)**
  - Mantenimento delle competenze del gruppo allo stato dell'arte del settore.
- **Task P-5 (Tools) : 0.3 FTE**
  - Sviluppo di nuovi tools e prova di quelli esistenti: in particolare un campo da esplorare è quello dei sistemi di Network Intrusion Detection.
    **R. Cecchini: 0.1 FTE**
    **P. Amendola: 0.1 FTE**
    **M. Gravino: 0.05 FTE**
- **Task P-6 (Auditing) : 0.4 FTE**

  Istituzione di un servizio di *auditing* che consenta di tenere sotto controllo tutto il parco macchine,

in modo da essere in grado di poter intervenire rapidamente nel caso di scoperta di nuove vulnerabilità.
Le informazioni raccolte verranno inserite in un database consultabile anche, con opportuni meccanismi di sicurezza, dai responsabili locali.
La macchina dedicata a questo servizio, poi, potrà essere utilizzata anche dai responsabili locali per verificare *dall'esterno* le condizioni delle proprie LAN.
**R. Cecchini: 0.1 FTE**

- **SubTask P-6.1** : **0.3 FTE (2 persone)**
    - Studio di fattibilità, configurazione della macchina, preparazione dei programmi e del database
- **SubTask P-6.2** : **0.1 FTE (1 persona)**
    - Gestione: rilevazioni periodiche del parco software e hardware. La popolazione iniziale del database è compito del Task **2-2**.

## 4.2 FASE I

- **Task 1-1** (**Configurazione router**) : **0.1 FTE**
    - Revisione delle configurazioni software dei router di accesso alle LAN e loro adeguamento a standard comuni di sicurezza. In particolare:
        - revisione dell'attuale politica di accesso, con account, sia pure non privilegiati, senza password;
        - ACL che blocchino o limitino a certe macchine gli accessi alle porte specificate nella tabella di sopra e impediscano l'accesso dall'esterno di pacchetti con indirizzi interni e vice versa (per risolvere, sia pure parzialmente, il problema dell'*ip-spoofing*).

    **L. dell'Agnello**
- **Task 1-2** : (**Verifica macchine**) : **A CARICO DEI RESPONSABILI LOCALI**
    - Individuazione, sede per sede, delle macchine principali (quelle cioè i cui servizi non sono filtrati a livello di router) e verifica della loro configurazione in modo da renderle ragionevolmente `sicure'.

## 4.3 FASE II

- **Task 2-1** (**Controllo LAN**) : **0.25 FTE**

  Studio della soluzione migliore per il controllo degli accessi alle LAN in quei casi in cui il controllo dei router non è possibile.
    - **SubTask 2-1.1** : **0.05 FTE**
        - Censimento situazioni esistenti
    - **SubTask 2-1.2** : **0.2 FTE**
        - Studio soluzioni possibili: router, macchine con due interfacce di rete, ecc. e piano di applicazione
          R. Alfieri
- **Task 2-2** (**Censimento macchine**) : **0.2 FTE**
    - Rilevamento della situazione del parco installato.

Verrà utilizzato l'hardware e il software predisposti dal **SubTask P-6.1.**

- **Task 2-3** (**Server dedicati**) : **0.4 FTE**
  - Spostamento di tutti i servizi chiave su server dedicati: valutazione delle piattaforme hardware e software più adatte
    **E. Fasanelli (solo IMAP server): 0.15 FTE**
- **Task 2-4** (**Password**) : **0.4 FTE**
  - Riduzione al minimo della trasmissione di password in chiaro sulla rete.
    Valutazione delle soluzioni esistenti (**ssh**, **OPIE**, **srp**, ecc.) e piano di applicazione.
    **R. Alfieri: 0.1 FTE**
    **R. Cecchini: 0.05 FTE**
- **Task 2-5 (Distribuzione Linux) : COMPITO DI UN GRUPPO DI LAVORO SPECIFICO.**
  - Istituzione di una distribuzione di Linux 'chiavi in mano', installabile dall'utente finale senza necessariamente bisogno di personalizzazione da parte sua e che produca un sistema ragionevolmente sicuro.
- **Task 2-6** (**Sicurezza Windows**) : **0.4 FTE**
  - Sicurezza dei sistemi con Windows NT: studio del problema e individuazione soluzioni.
    Un problema particolarmente pressante è la sicurezza di **NICE** (tramite una VPN?).
    Andrà anche studiato il problema della migrazione da sistemi Windows 9x.
    **L. dell'Agnello: 0.1 FTE**
    **(coordinamento con gruppo NICE)**
- **Task 2-7** (**Sicurezza X11**) : **0.2 FTE**
  - Sicurezza X11: studio del problema e individuazione soluzioni.
    **M. Michelotto: 0.05 FTE**
    **M. Gravino: 0.05 FTE**

# 5 Deliverables

## 5.1 Attività istituzionali

I *deliverables* dei task **P-2** e **P-5** verranno anche pubblicati (eventualmente limitatamente al dominio **.infn.it**) sul server web del gruppo (task **P-1**).

- **Task P-2 (Aggiornamento utenza)**
  - Dispense, note d'uso, ecc..
- **Task P-5 (Tools)**
  - Manuali utente.
- **Task P-6 (Auditing)**
  - **SubTask P-6.1**
    - Documento con i risultati dello studio di fattibilità.
    - Macchina opportunamente configurata per la gestione del servizio e l'accesso sicuro degli utenti autorizzati
    - Database parco hardware e software (solo struttura).

- **SubTask P-6.2**
  - Database con i dati sul parco hardware e software.

## 5.2 FASE I

- **Task 1-1 (Configurazione router)**
  - Comandi di configurazione dei router

## 5.3 FASE II

- **Task 2-1 (Controllo LAN)**
  - **SubTask 2-1.1**
    - Documento con la descrizione delle situazioni esistenti nelle varie realtà locali.
  - **SubTask 2-1.2**
    - Documento con i risultati dello studio di fattibilità e proposte di attuazione.
- **Task 2-2 (Censimento macchine)**
  - Popolamento del database creato nel Task **P-6.1**
- **Task 2-3** (**Server dedicati**)
  - Documento con la descrizione delle configurazioni hardware e software consigliate, con particolare riguardo ai problemi di sicurezza dei servizi più critici (DNS, WWW, SMTP, ecc.).
- **Task 2-4 (Password)**
  - Documento con la valutazione dei pacchetti software provati e piano di applicazione
- **Task 2-6 (Sicurezza Windows)**
  - Documento con la descrizione dei problemi e i rimedi proposti.
- **Task 2-7** (**Sicurezza X11**)
  - Documento con la descrizione dei problemi e i rimedi proposti.

# 6 Risorse

## 6.1 Equipaggiamento

Per quello che riguarda l'hardware prevediamo la necessità di 3 macchine dedicate ai compiti sotto indicati:

1. Gestione della CA INFN (Task **P-1**).
2. Macchina di prova e sviluppo (Task **P-5**, **2-3** e **2-4**) **SOSPESO**
3. Macchina per l'auditing: su questa si intende anche permettere l'accesso ai security manager locali per consentire loro di provare la proprie LAN da una postazione remota (Task **P-6** e **2-2**).

Il costo di una macchina tipo è stato stimato intorno ai 5 ML.

## 6.2 Materiali

Per l'acquisto di software (nel caso in cui non si riesca ad ottenerlo in prova): 5 ML.

## 6.3 Viaggi

Per le missioni prevediamo, per ogni anno:

- 3 riunioni del gruppo di lavoro;
- partecipazione a due eventi internazionali.

| COMPITO | COSTO STIMATO (ML) |
|---|---|
| Lavoro extra INFN | - |
| Equipaggiamento | 10 |
| Materiali | 5 |
| Viaggi | 20 |

**Tabella 1**. Lavoro, Materiali e Spese di Viaggio richieste

## 6.4 Risorse umane

| TASK | DESCRIZIONE | FTE | ORE[2] | |
|---|---|---|---|---|
| **P-1** | Server web | 0.1 | 120 | Cecchini |
| **P-2** | Aggiornamento utenza | 0.2 | 240 | |
| **P-3** | Gestione INFN CA | 0.05 | 60 | Cecchini |
| **P-4** | Autoaggiornamento | 0.05[3] | 60[3] | |
| **P-5** | Tools | 0.3 | 360 | Amendola, Cecchini, Gravino |
| **P-6** | Auditing | | | Cecchini |
| **P-6.1** | istituzione | 0.3 | 360 | |
| **P-6.2** | gestione | 0.1 | 120 | |
| **1-1** | Configurazione router | 0.1 | 120 | dell'Agnello |
| **1-2** | Verifica macchine | | | |
| **2-1** | Controllo LAN | | | |
| **2-1.1** | censimento | 0.05 | 60 | |
| **2-1.2** | piano di applicazione | 0.2 | 240 | |

[2] Le stime sul numero di ore richiesto sono fatte sull'ipotesi di 20 giorni lavorativi di 6 ore per mese per 10 mesi l'anno.

[3] Per ogni membro del gruppo

| | | | | |
|---|---|---|---|---|
| **2-2** | Censimento macchine | 0.2 | 240 | |
| **2-3** | Server dedicati | 0.4 | 480 | Fasanelli |
| **2-4** | Password | 0.4 | 480 | Alfieri, Cecchini |
| **2-6** | Sicurezza Windows | 0.4 | 480 | dell'Agnello |
| **2-7** | Sicurezza X11 | 0.2 | 240 | Michelotto, Gravino |

**Tabella 2.** Sommario delle risorse per compito lavorativo.

# 7 Identificazione del rischio

In tutto quanto sopra indicato è fondamentale la completa collaborazione dei responsabili locali. Senza di essa tutto corre il rischio di rimanere lettera morta.

Un altro presupposto fondamentale è la possibilità del controllo completo degli accessi alla LAN (in un modo o nell'altro). Non è chiaro al momento se la cosa possa essere realizzata dappertutto e a che costi.

Un altro problema deriva dal fatto che tutte le persone coinvolte hanno molti altri incarichi da assolvere, quotidiani e spesso non dilazionabili, che possono provocare ritardi - difficilmente quantificabili - nell'assolvimento degli impegni presi.

# 8 Responsabilità organizzativa

| TASK | DESCRIZIONE | RESPONSABILE |
|---|---|---|
| **P-1** | Server web | Cecchini |
| **P-2** | Aggiornamento utenza | |
| **P-3** | Gestione INFN CA | Cecchini |
| **P-5** | Tools | |
| **P-6** | Auditing | |
| **1-1** | Configurazione router | dell'Agnello |
| **2-1** | Controllo LAN | Alfieri |
| **2-2** | Censimento macchine | |
| **2-3** | Server dedicati | Fasanelli |
| **2-4** | Password | Alfieri |
| **2-6** | Sicurezza Windows | dell'Agnello |
| **2-7** | Sicurezza X11 | Michelotto |

**Tabella 3.** Responsabili organizzativi

# Appendice

## Politica di accesso alla LAN

Nell'impossibilità, almeno nell'immediato, di controllare la configurazione di tutte le macchine esistenti sulla LAN per verificare l'esistenza di eventuali vulnerabilità, l'unica strada percorribile sembra essere al momento quella di bloccare (o filtrare) l'accesso dall'esterno a certi servizi ritenuti 'pericolosi'.

Naturalmente questo tipo di azione, in alcuni casi, può avere importanti conseguenze sul modo di lavorare degli utenti (basti pensare ad esempio all'uso dei comandi **r***, di cui si propone l'abolizione), e quindi la decisione non può essere solamente tecnica.

La tabella seguente elenca i servizi che dovrebbero venire bloccati o filtrati, limitati cioè ad alcune macchine 'ufficiali' (**B** o **F** in prima colonna, rispettivamente).

Per evitare un eccessivo appesantimento dei router, sono state elencate solo i servizi più utilizzati, ricavati da un'indagine su 7 reti locali, per un totale di 1300 nodi.

**smtp**
A nostro avviso dovrebbe esserci un solo mailer (più eventuali secondari) per LAN. Il che, tra l'altro risolverebbe automaticamente anche il problema del *mail spamming* e delle vulnerabilità delle vecchie versioni di **sendmail**.

**domain**
Il DNS usa connessioni TCP per gli *zone transfer* (che dovrebbero essere bloccati tranne che verso i server secondari, perchè molto utilizzati da alcuni script!) e UDP per le query client-server e server-server.
Quindi bloccare la porta TCP, tranne che verso gli eventuali server secondari esterni, dovrebbe avere solo conseguenze benefiche. Il blocco della porta UDP, invece, rende impossibile il funzionamento del name server.

**http**
I server **http** (e soprattutto i programmi CGI) sono una delle principali cause di intrusione. Il loro uso quindi dovrebbe essere limitato ai casi veramente necessari.

**sunrpc**
Bloccare questa porta inibisce i comandi **rpcinfo**, **showmount** e **mount** via **nfs**. Non blocca gli attacchi diretti a **mountd**. In Linux, *e solo per lui*, **mountd** ascolta sempre sulla porta 635, che vale quindi la pena di bloccare.

**netbios**
Il blocco sulle porte indicate in tabella (137-139 TCP e UDP) impedisce il funzionamento di **NICE**. Una soluzione temporanea sembra essere bloccare 137 e 138 (TCP) e 137 e 139 (UDP).
È importante bloccare dall'esterno i servizi offerti da **samba** su Linux, che è una delle più grosse fonti di vulnerabilità, sia per le configurazione errate, sia per errori nel programma.

**exec, login, shell**
Questi servizi sono intrinsicamente pericolosi e dovrebbero essere aboliti (anche all'interno della LAN, possibilmente). Dove sono veramente necessari dovrebbero essere sotituiti da **ssh**.

**nfs**
Riteniamo che questo sia un servizio intrinsecamente pericoloso e che il suo uso all'esterno della LAN vada eliminato. Per esempio è abbastanza frequente trovare volumi NFS, tra cui anche `/,` esportati al mondo!

| | SERVIZIO | PORTA | PROT | NOTE |
|---|---|---|---|---|
| **B** | **echo** | 7 | TCP/UDP | Insieme a **chargen** può servire per attacchi DoS |

| | SERVIZIO | PORTA | PROT | NOTE |
|---|---|---|---|---|
| **B** | **systat** | 11 | TCP | Insieme a **finger**, **netstat** e **who** fornisce informazioni utili a eventuali attaccanti |
| **B** | **daytime** | 13 | TCP/UDP | |
| **B** | **netstat** | 15 | TCP | Vedi la nota per **systat** |
| **B** | **chargen** | 19 | TCP/UDP | Vedi la nota per **echo** |
| **F** | **smtp** | 25 | TCP | |
| **B** | **time** | 37 | TCP/UDP | Sostituito da **ntp** |
| **F** | **domain** | 53 | TCP/UDP | |
| **B** | **bootp** | 6768 | UDP | |
| **B** | **tftp** | 69 | UDP | |
| **B** | **gopher** | 70 | TCP | |
| **B** | **finger** | 79 | TCP | Vedi la nota per **systat** |
| **F** | **http** | 80 | TCP | |
| **B** | **pop2** | 109 | TCP | |
| **F** | **pop3** | 110 | TCP | |
| **F** | **sunrpc** | 111<br>635 | TCP/UDP | |
| **F** | **nntp** | 119 | TCP | |
| **F** | **nbios-ns**<br>**nbios-dgm**<br>**nbios-ssn** | 137<br>138<br>139 | TCP/UDP | |
| **F** | **imap** | 143 | TCP | |
| **B** | **snmp**<br>**snmptrap** | 161<br>162 | TCP/UDP | |
| **F** | **xdmcp** | 177 | UDP | |
| **B** | **irc** | 194<br>6667 | TCP/UDP | |
| **B** | **exec**<br>**login**<br>**shell** | 512<br>513<br>514 | TCP | |
| **B** | **syslog** | 514 | UDP | |
| **B** | **printer** | 515 | TCP | |
| **B** | **uucp** | 540 | TCP | |
| **B** | **route** | 520 | UDP | |
| **B** | **openwin** | 2000 | TCP | |
| **F** | **NFS** | 2049 | TCP/UDP | |
| **F** | **X11** | 6000... | TCP | |