THE ITALIAN RESEARCH & EDUCATION NETWORK | Consortium GARR

La Security Policy della rete GARR

Claudio Allocchio

Roma 7 Aprile 2017

Il principio di base

GARR è una Community Network, realizzata per le sue specifiche Comunità di utenti per servirli in tutte le loro attività istituzionali e di supporto alle loro attività istituzionali che coinvolgono la rete ed i suoi contenuti

Che cosa significa “Security Policy”

- A **network security policy**, is a generic document that outlines rules for **computer network access**, determines how policies are enforced and lays out some of the basic architecture of the community security/network environment.

- **Information Security Policy** is a set or rules enacted by an organization to ensure that all users or networks of the IT structure within the organization's domain abide by the prescriptions regarding the **security** of data stored digitally within the boundaries the organization stretches its authority

- A **computer security policy** defines the goals and elements of an organization's **computer** systems. The definition can be highly formal or informal. **Security policies** are enforced by organizational **policies** or **security** mechanisms. A technical implementation defines whether a **computer** system is secure or insecure.

Come si crea una Security Policy

Ogni istituzione ha il proprio ambito di attività istituzionali:

- Fare ricerca nella fisica delle alte energie
- Educare i propri studenti
- Diffondere e dare accesso ai contenuti scientifici o culturali
- …

- E questo implica che ci sono differenze nell'approccio generale…

Come si crea una Security Policy

Nell'ambito di una Comunità come GARR, la creazione di una Security Policy richiede quindi un sovra-insieme di indicazioni che:

- Vengono sviluppate DENTRO la comunità
- Sono applicabili alla situazione specifica
- Vengono adottate da TUTTA la comunità
- Evolvono insieme alla comunità

Dove si applica?

All’interno dell’intera comunità !

- Sui servizi condivisi (rete, applicazioni, middleware)
- All’interno della propria organizzazione
- … sino al singolo elemento (PC, applicazione…)

Chi applica la Security Policy?

Il gestore della rete e dei servizi “in rete” (GARR)

e (AND)

La singola organizzazione al proprio interno, comprese la “virtual organizations”

→ problema di armonizzazione internazionale

Cosa c'è dentro una Security Policy

- Un quadro generale introduttivo
  - Definizione dei termini
    - Per esempio "qualità del dato"
  - Defiinizione dell'ambito di applicazione
    - Tutti coloro che appartengono alla "comunità", compreso ANCHE le organizzazioni virtuali internazionali
  - Definizione delle figure dei "responsabili"
    - Resp. Sicurezza, trattamento dati, …
  - Definizione del Campo di Applicazione
    - Non è strettamente solo e-security (anche carta e pratiche correnti!)

Cosa c'è dentro una Security Policy

- Un "Mission Statement"
  - Qual'è lo scopo della Security Policy
    - Renedere noti i valori e rischi
    - Prevedere misure di protezione e ricupero
    - Eliminare i "punti deboli del sistema" (globale)
  - Quali sono gli obiettivi da raggiungere
    - Avere procedure operative per la gestione dei problemi
    - Avere posizioni e responsabilità chiare nella gestione della sicurezza
    - Avere un controllo ed aggiornamento regolare della situazione

Cosa c'è dentro una Security Policy

- I principi generali
  - Avere una gestione consapevole ed adeguata dei rischi identificati
  - Avere una gestione a livelli comparabili all'interno della comunità
  - Adeguare le misure di sicurezza al rischio effettivo ed alle necessità delle organizzazioni
  - …

Cosa c'è dentro una Security Policy

- I riferimenti normativi
  - … "si si si… sembra facile" diceva una vecchia pubblicità
  - → allegato separato facilmente aggiornabile

Cosa c'è dentro una Security Policy

- La "governance" per attuale la Security Policy
  - Definire I ruoli all'interno delle organizzazioni
    - Il coordinatore della sicurezza (information Security Manager)
    - Il responsabile del monitoraggio e dell'applicazione (Information Security Officer)
  - Definire la documentazione
    - Lo stato dei rischi e classificazione
    - Le procedure di risposta ad un evento
    - Il "piano di continuità"
    - L'aggiornamento periodico dello stato
    - I codici di condotta
    - Le regole di gestione di credenziali (password certificati) e dei dati sensibili

Cosa c'è dentro una Security Policy

- La "governance" per attuale la Security Policy
  - Monitoraggio della situazione
    - Definizione dei parametri di controllo
    - Definizione delle azioni di "recovery" e protezione
  - Senzibilizzazione e Formazione
    - Le azioni minime di formazione verso tutti quelli che sono soggetti alla policy (praticamente tutti)

Cosa c'è dentro una Security Policy

- La struttura di gestione
  - È una politica comune!! Quindi:
    - Richiede continua discussione ed eleborazione
    - Gruppo di Gestione/aggiornamento
    - Gruppo operativo
    - …

Cosa c'è dentro una Security Policy

- Il riferimento alla gestione quotidiana di incidenti di sicurezza
  - Il GARR CERT e le sue procedure
  - Le interazioni pratiche sui servizi (filtraggi, misure di riduzione del problema, ecc.)

Discussione…