1 INTRODUZIONE

1.1 Scopo

La sicurezza del software di base ed applicativo richiede di stabilire un processo volto ad identificare rischi e contromisure di sicurezza ad ogni livello (fisico, logico e organizzativo) del contesto in cui tali software operano e sono utilizzati.

Pertanto, nel fornire delle linee guida per la configurazione sicura di tali software (nel seguito tale attività viene spesso indicata con il termine "hardening"), è necessario considerare vari elementi, quali le protezioni perimetrali (fisiche e logiche), le architetture di rete (DMZ, segmentazioni, etc.), le procedure organizzative (perché dietro alle tecnologie operano le persone), i programmi formativi di "security awareness", ecc.

Partendo da questo presupposto, il presente documento si pone l'obiettivo di fornire un insieme di indicazioni per affrontare e risolvere correttamente le problematiche legate alla sicurezza del software di base e di individuare le misure da adottare per difendere ogni componente da possibili minacce accidentali e/o intenzionali.

1.2 Struttura del Documento

I paragrafi a seguire entrano nel dettaglio delle singole componenti (software di base, middleware, office automation, ecc.) oggetto di approfondita analisi dal punto di vista delle best practice di sicurezza, e per ognuna forniscono un elenco delle misure di sicurezza da adottare a fronte delle principali minacce, in modo da diminuire l'esposizione ai rischi per la sicurezza delle informazioni e dei servizi erogati.

Più nel dettaglio il documento è strutturato come segue:

- Il Capitolo 4 fornisce:
  - un catalogo delle minacce alla sicurezza delle informazioni ritenute applicabili nel contesto del presente documento (par. 4.1).
  - un catalogo delle principali tipologie di attacco rispetto al software di base, al middleware e al software applicativo più comune (par. 4.2).
- Il Capitolo 5 fornisce un insieme di raccomandazioni generali 'trasversali' che realizzano la base comune per affrontare le problematiche di sicurezza delle specifiche componenti.
- Il Capitolo 6 fornisce:
  - in una prima tabella, l'elenco dei riferimenti alle istruzioni operative di hardening (o benchmarks) messe a disposizione da enti/istituzioni preposte ed affermate a livello internazionale, operanti con il pieno supporto dei rispettivi vendor;
  - in una seconda tabella, l'elenco delle baseline di configurazione e alcuni strumenti software per l'hardening, messi a disposizione direttamente dai vendor.

1.3 Ambito di Applicabilità

Il presente documento si applica alle principali tipologie di software di base, middleware e applicativo in uso presso le pubbliche amministrazioni, ed in particolare:

- Principali Sistemi Operativi UNIX,
- Sistemi operativi Microsoft Windows Server,
- Sistemi operativi Windows Client,
- Web Browser,
- Postazioni di Lavoro,

- Web Application Server,
- DBMS/Data base server,
- Mail Server,
- Enterprise Service Bus,
- Principali applicativi di Office Automation (Microsoft Office e OpenOffice).