

Linee Guida per la configurazione per adeguare la sicurezza del software di base

Sommario

1	INTRODUZIONE	6
1.1	SCOPO	6
1.2	STRUTTURA DEL DOCUMENTO	6
1.3	AMBITO DI APPLICABILITÀ	6
2	RIFERIMENTI	8
2.1	DOCUMENTI APPLICABILI	8
3	ACRONIMI	9
3.1	ACRONIMI	9
4	MINACCE E TIPOLOGIE DI ATTACCO	11
4.1	CATALOGO DELLE MINACCE	11
4.2	CATALOGO DELLE TIPOLOGIE DI ATTACCO	12
5	BEST PRACTICES PER ADEGUARE E MANTENERE LA SICUREZZA DEL SOFTWARE DI BASE	22
5.1	COMMON BEST PRACTICE	23
5.1.1	Utenze	23
	Utenze tecniche	24
	Terze parti	25
5.1.2	Autenticazione	25
5.1.3	Autorizzazione	28
5.1.4	Crittografia	30
5.1.5	Documentazione	32
5.1.6	Logging	32
5.1.7	Procedure	34
	Change management	34
	Maintenance	36
	Patching	38
	Secure testing	39
	Disposal	40
5.2	SICUREZZA DEI SISTEMI OPERATIVI	41
5.2.1	Architettura	41
5.2.2	Hardening	42
5.2.3	Utenze	47
5.2.4	Autenticazione	47
5.2.5	Autorizzazione	48
5.2.6	Crittografia	48
5.2.7	Documentazione	49
5.2.8	Logging	49
5.2.9	Antivirus	49
5.2.10	Procedure	49
5.2.11	Sicurezza di macOS	51
5.2.12	Sicurezza di Linux	60
5.2.13	Sicurezza di Windows	74
5.3	SICUREZZA DEL WEB BROWSER	85
5.3.1	Architettura	85
5.3.2	Hardening	85
5.3.3	Autorizzazione	91
5.3.4	Crittografia	91
5.3.5	Procedure	92

5.3.6	Informazioni aggiuntive.....	93
5.4	SICUREZZA DELLE POSTAZIONI DI LAVORO.....	93
5.4.1	Architettura.....	93
5.4.2	Hardening	94
5.4.3	Utenze.....	95
5.4.4	Autenticazione	95
5.4.5	Autorizzazione.....	95
5.4.6	Crittografia.....	95
5.4.7	Documentazione	95
5.4.8	Logging	95
5.4.9	Procedure.....	95
5.5	SICUREZZA DEI WEB APPLICATION SERVER	97
5.5.1	Architettura.....	97
5.5.2	Hardening	98
5.5.3	Utenze.....	102
5.5.4	Autenticazione	102
5.5.5	Autorizzazione.....	102
5.5.6	Crittografia.....	102
5.5.7	Documentazione	102
5.5.8	Logging	102
5.5.9	Sessioni.....	102
5.5.10	Procedure.....	103
5.5.11	Programmazione e Configurazione	105
5.6	SICUREZZA DEI DBMS/DATABASE SERVER	108
5.6.1	Architettura.....	108
5.6.2	Hardening	110
5.6.3	Utenze.....	112
5.6.4	Autenticazione	112
5.6.5	Autorizzazione.....	112
5.6.6	Crittografia.....	112
5.6.7	Documentazione	113
5.6.8	Logging	113
5.6.9	Sessioni.....	113
5.6.10	Procedure.....	113
5.6.11	Informazioni aggiuntive	113
5.7	SICUREZZA DEL MAIL SERVER.....	114
5.7.1	Architettura.....	114
5.7.2	Utenze.....	117
5.7.3	Autenticazione	117
5.7.4	Autorizzazione.....	117
5.7.5	Crittografia.....	118
5.7.6	Documentazione	118
5.7.7	Logging	118
5.7.8	Anti-Phishing	118
5.7.9	Anti-Spam	119
5.7.10	Procedure.....	119
5.8	SICUREZZA DEI ENTERPRISE SERVICE BUS (ESB)	121
5.8.1	Architettura.....	121
5.8.2	Hardening	121
5.8.3	Utenze.....	125
5.8.4	Autenticazione	125
5.8.5	Autorizzazione.....	126
5.8.6	Crittografia.....	126
5.8.7	Documentazione	126
5.8.8	Logging	126
5.8.9	Procedure.....	127
5.8.10	Informazioni aggiuntive	127

5.9	SICUREZZA DEL PACCHETTO MS OFFICE	127
5.9.1	<i>Hardening</i>	127
5.9.2	<i>Autorizzazione</i>	130
5.9.3	<i>Crittografia</i>	130
5.9.4	<i>Procedure</i>	131
5.9.5	<i>References and additional information</i>	131
5.10	SICUREZZA DEL PACCHETTO OPENOFFICE	131
5.10.1	<i>Hardening</i>	131
5.10.2	<i>Autorizzazione</i>	133
5.10.3	<i>Crittografia</i>	133
5.10.4	<i>Procedure</i>	133
6	RIFERIMENTI A ISTRUZIONI OPERATIVE E TOOLS DI HARDENING	136
6.1	ISTRUZIONI OPERATIVE (BENCHMARKS) DI TERZE PARTI	136
6.2	TOOLS DI HARDENING E BASELINE DI SICUREZZA FORNITE DAI VENDOR	139

LISTA DELLE TABELLE

Tabella 1 - Documenti Applicabili	8
Tabella 2 - Acronimi	10
Tabella 3 - Catalogo delle Minacce	11

LISTA DELLE FIGURE

Figura 1 - Scenario - Sicurezza ad ogni livello (fisico, logico e organizzativo)	22
--	----

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).