

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
--	----