

Sommario

Prefazione.....	XI
Introduzione	XIII
Capitolo 1 - Creare un programma di sicurezza	1
Gettare le fondamenta	2
Istituire i team	2
Informazioni di base per la sicurezza	3
Valutare le minacce e i rischi	3
Identificare	4
Valutare	4
Limitare	4
Monitorare	5
Stabilire le priorità	5
Definire gli obiettivi intermedi	6
Casi d'uso, tabletop ed esercitazioni	7
Ampliare il team e l'insieme di competenze	12
Conclusione	13
Capitolo 2 - Gestione delle risorse e documentazione.....	15
Classificazione delle informazioni	16
Fasi di attuazione della gestione delle risorse	16
Definire il ciclo di vita	17
Raccogliere le informazioni	18
Tenere traccia delle modifiche	19
Controlli e notifiche	20
Linee guida della gestione delle risorse	20
Automazione	20

Una fonte di verità	21
Organizzare un team per tutta l'azienda	21
Campioni dell'esecutivo	21
Licenze software	22
Definire le risorse	22
Documentazione	22
Attrezzatura di rete	22
Rete	23
Server	23
Desktop	24
Utenti	24
Applicazioni	24
Altro	24
Conclusione	25
Capitolo 3 - Normative	27
Linguaggio	28
Contenuto dei documenti	29
Argomenti	30
Archiviazione e comunicazione	31
Conclusione	32
Capitolo 4 - Standard e procedure	33
Standard	34
Linguaggio	34
Procedure	35
Linguaggio	35
Contenuto dei documenti	36
Conclusione	37
Capitolo 5 - Istruzione degli utenti	39
Processi interrotti	40
Colmare il divario	41
Costruire programmi personalizzati	41
Definire gli obiettivi	42
Definire i valori base	42
Esaminare e creare le regole e le linee guida del programma	42
Implementare e documentare l'infrastruttura del programma	42
Incoraggiamenti	43
Ludicizzazione	43
Definire i processi di risposta agli incidenti	43
Ottenere metriche significative	44
Misurazioni	44
Monitorare la percentuale di successo e i progressi	44
Metriche importanti	45
Conclusione	45

Capitolo 6 - Risposta agli incidenti	47
Processi	47
Processi pre incidente	47
Processi durante l'incidente	49
Processi post incidente	50
Strumenti e tecnologia	51
Analisi dei log	51
Analisi di file e dischi	52
Analisi della memoria	53
Analisi PCAP	53
Tutto in uno	54
Conclusione	54
Capitolo 7 - Ripristino in caso di disastro.....	55
Definire gli obiettivi	56
RPO (Recovery Point Objective)	56
RTO (Recovery Time Objective)	56
Strategie di ripristino	57
Backup	57
Standby di emergenza	57
Elevata disponibilità	58
Sistema alternativo	58
Trasferimento della funzione del sistema	59
Dipendenze	59
Scenari	59
Passaggio ai sistemi di emergenza e ritorno ai sistemi ripristinati	60
Test	61
Considerazioni sulla sicurezza	61
Conclusione	62
Capitolo 8 - Norme di conformità del settore e framework.....	63
Norme di conformità del settore	63
PCI DSS (Payment Card Industry Data Security Standard)	64
HIPAA (Health Insurance Portability & Accountability Act)	64
GLBA (Gramm-Leach Bliley Act)	65
FERPA (Family Educational Rights and Privacy Act)	66
SOX (Sarbanes-Oxley Act)	66
Framework	67
CCM (Cloud Control Matrix)	67
CIS (Center for Internet Security)	67
COBIT (Control Objectives for Information and Related Technologies)	67
COSO (Committee of Sponsoring Organizations of the Treadway Commission)	68
Serie ISO-27000	68
Framework di cyber sicurezza del NIST	68
Settori regolamentati	69
Finanza	69

Governo	69
Assistenza sanitaria	70
Conclusione	71
Capitolo 9 - Sicurezza fisica.....	73
Aspetti fisici	74
Limitare l'accesso	74
Videosorveglianza	74
Manutenzione dei sistemi di autenticazione	75
Proteggere i supporti di archiviazione	76
Data center	77
Aspetti operativi	77
Identificare i visitatori e gli appaltatori	78
Azioni dei visitatori	78
Azioni degli appaltatori	78
Badge	78
Corsi sulla sicurezza fisica	79
Conclusione	81
Capitolo 10 - Infrastruttura Microsoft Windows.....	83
Vittorie veloci	83
Aggiornamenti	84
Patch di terze parti	85
Condivisioni aperte	85
Servizi di dominio Active Directory	85
Foresta	86
Dominio	87
Controllori di dominio	87
Unità organizzative	88
Gruppi	89
Account	89
Oggetti criteri di gruppo	90
EMET	91
Configurazione di base	92
Configurazione personalizzata	95
Strategie di installazione aziendale	96
MS-SQL Server	98
Quando i fornitori di terze parti hanno accesso	99
Autenticazione MS SQL	99
Protezione dell'utente SA	100
Conclusione	101
Capitolo 11 - Server applicativi UNIX.....	103
Aggiornamenti	104
Aggiornamenti dei software di terze parti	104
Aggiornamenti del core del sistema operativo	106

Rinforzare un server applicativo UNIX	107
Disattivare i servizi	107
Autorizzazioni di accesso ai file	109
Firewall basati sugli host	110
Gestire l'integrità dei file	110
Partizioni del disco separate	111
chroot	112
Controlli di accesso obbligatori	113
Conclusione	113
Capitolo 12 - Endpoint	115
Aggiornamenti	116
Microsoft Windows	116
MacOS	116
Desktop Unix	117
Aggiornamenti di terze parti	117
Rinforzare gli endpoint	118
Disattivare i servizi	118
Desktop firewall	120
Crittografia completa del disco	121
Strumenti per proteggere gli endpoint	123
Gestione dei dispositivi portatili	124
Visibilità degli endpoint	124
Centralizzazione	125
Conclusione	126
Capitolo 13 - Gestione delle password e autenticazione a più fattori.....	127
Prassi fondamentali per le password	127
Software per la gestione delle password	129
Reimpostazione delle password	130
Violazione delle password	131
Crittografia, hash e salting	131
Crittografia	131
Hash	132
Salting	133
Dove e come archiviare le password	133
Oggetti protezione password	135
Impostare un FGPP	135
Autenticazione a più fattori	140
Perché 2FA?	140
Metodi 2FA	142
Come funziona	143
Minacce	143
Dove andrebbe implementata	144
Conclusione	144

Capitolo 14 - Infrastruttura della rete.....	147
Aggiornamento di firmware e software	147
Rafforzamento dei dispositivi	149
Servizi	150
SNMP	151
Protocolli cifrati	152
Rete di gestione	152
Router	153
Switch	154
Filtri in uscita	155
IPv6: una raccomandazione	155
TACACS+	156
Conclusione	157
Capitolo 15 - Segmentazione.....	159
Segmentazione della rete	159
Segmentazione fisica	159
Segmentazione logica	160
Esempio di rete fisica e rete logica	166
SDN (Software-Defined Networking)	168
Applicazione	168
Ruoli e responsabilità	169
Conclusione	171
Capitolo 16 - Gestione delle vulnerabilità	173
Come funziona la scansione delle vulnerabilità	174
Scansioni autenticate e scansioni non autenticate	174
Strumenti per la valutazione delle vulnerabilità	176
Programma di gestione delle vulnerabilità	178
Inizializzazione del programma	178
Ordinaria amministrazione	179
Priorità delle bonifiche	179
Accettazione del rischio	182
Conclusione	182
Capitolo 17 - Sviluppo	183
Scelta del linguaggio	183
OxAssembly	184
/* C e C++ */	184
GO func()	184
#!/Python/Ruby/Perl	185
<? PHP ?>	185
Linee guida per scrivere codice sicuro	186
Test	187
Test statici automatici	187
Test dinamici automatici	187

Revisione inter pares	188
Ciclo di vita dello sviluppo del sistema	188
Conclusione	190
Capitolo 18 - Il team viola.....	191
Fonti di informazioni di libero accesso	191
Tipi di informazioni e accesso	192
Strumenti OSINT	195
Team rosso	208
Conclusione	212
Capitolo 19 - IDS e IPS	213
Tipi IDS e IPS	213
NIDS (Network Based IDS)	214
HIDS (Host-Based IDS)	214
IPS (Intrusion Prevention System)	215
Eliminare il rumore	215
Scrivere le proprie firme	217
Dove collocare i NIDS e gli IPS	219
Protocolli crittografati	220
Conclusione	221
Capitolo 20 - Registrazione e monitoraggio.....	223
Che cosa registrare	224
Dove conservare i log	224
SIEM (Security Information and Event Management)	225
Progettare il SIEM	225
Analisi dei log	226
Esempi di log e allarmi	227
Sistemi di autenticazione	227
Log delle applicazioni	228
Log di proxy e firewall	228
Aggregazione dei log	229
Analisi dei casi d'uso	229
Conclusione	230
Capitolo 21 - Uno sforzo in più	231
Server di posta elettronica	231
Server DNS	233
Sicurezza attraverso segretezza	235
Risorse utili	236
Libri	236
Blog	236
Podcast	237
Strumenti	237
Siti web	237

Appendice A - Modelli per la formazione degli utenti.....	239
Diapositive formative sul phishing	239
Regole del programma sul phishing	242
Indice analitico	245