

# LINEE GUIDA PER LA MODELLAZIONE DELLE MINACCE ED INDIVIDUAZIONE DELLE AZIONI DI MITIGAZIONE CONFORMI AI PRINCIPI DEL SECURE/PRIVACY BY DESIGN



## SOMMARIO

<b>1</b>	<b>INTRODUZIONE .....</b>	<b>6</b>
1.1	SCOPO .....	6
1.2	STRUTTURA DEL DOCUMENTO .....	6
<b>2</b>	<b>RIFERIMENTI .....</b>	<b>7</b>
2.1	DOCUMENTI APPLICABILI .....	7
<b>3</b>	<b>DEFINIZIONI E ACRONIMI.....</b>	<b>8</b>
3.1	DEFINIZIONI.....	8
3.2	ACRONIMI .....	9
<b>4</b>	<b>ESIGENZE ED AMBITI DI APPLICAZIONE.....</b>	<b>11</b>
<b>5</b>	<b>PROGETTAZIONE DEL SOFTWARE SECURE/PRIVACY BY DESIGN .....</b>	<b>13</b>
5.1	PROCESSI DI SVILUPPO DEL SOFTWARE SICURO.....	13
5.1.1	<i>BSA Framework for Secure Software (BSA)</i> .....	13
5.1.2	<i>Open Software Assurance Maturity Model (SAMM)</i> .....	13
5.1.3	<i>Building Security in Maturity Model (BSIMM)</i> .....	14
5.1.4	<i>Comprehensive, Light-weight Application Security Process (CLASP)</i> .....	14
5.1.5	<i>Microsoft's Security Development Lifecycle (SDL)</i> .....	14
5.2	SECURE BY DESIGN.....	17
5.2.1	<i>Principi base del secure design</i> .....	17
5.2.2	<i>Pratiche di secure design</i> .....	21
5.2.2.1	Best practice di secure design per le applicazioni web .....	21
5.2.2.2	Best practice di secure design per il cloud .....	24
5.2.2.3	Best practice di secure design per le architetture serverless .....	26
5.2.2.3.1	Best practice di secure design per le architetture basate su registri distribuiti (DLT) .....	28
5.3	THREAT INTELLIGENCE E THREAT MODELING.....	31
5.4	THREAT MODELING E THREAT ASSESSMENT .....	31
5.5	MODELLAZIONE E INDIVIDUAZIONE DELLE MINACCE: THREAT MODELING .....	34
5.5.1	<i>Introduzione e concetti base</i> .....	35
5.5.2	<i>Motivazioni nell'uso del Threat Model</i> .....	36
5.5.2.1	Ricerca preventiva dei bug di sicurezza.....	36
5.5.2.2	Comprensione dei requisiti di sicurezza .....	36
5.5.2.3	Ingegnerizzazione e rilascio di prodotti più sicuri .....	36
5.5.3	<i>Processo di modellazione del sistema da proteggere</i> .....	36
5.5.3.1	Diagrammi DFD.....	37
5.5.4	<i>Tecniche di modellazione e individuazione delle minacce</i> .....	40
5.5.4.1	Microsoft SDL – STRIDE .....	40
5.5.4.2	Attack tree .....	61
5.5.4.3	TRIKE .....	63
5.5.4.4	P.A.S.T.A (Process for Attack Simulation and Threat Analysis) .....	64
5.5.4.5	Best practices di carattere generale.....	64
5.6	INDIRIZZAMENTO DELLE MINACCE .....	65
5.7	VALUTAZIONE DEL RISCHIO: TECNICHE DI RISK RANKING .....	66
5.7.1	<i>DREAD</i> .....	66
5.7.2	<i>Security Bulletin Severity Rating System (S.B.S.R.S)</i> .....	68
5.7.3	<i>Altri processi di valutazione del rischio</i> .....	69
5.8	PRIVACY BY DESIGN.....	69
5.8.1	<i>Introduzione e concetti base</i> .....	69
5.8.1.1	Proprietà.....	73
5.8.1.2	Principi .....	74
5.8.1.3	Riferimenti normativi .....	75
5.8.2	<i>Requisiti di sicurezza applicativi nel GDPR</i> .....	76
5.8.3	<i>Certificazioni</i> .....	77



5.8.3.1	Riferimenti normativi ed esempi di certificazione .....	79
5.8.4	<i>Best practices per il trattamento dei dati personali</i> .....	83
5.8.5	<i>Linee guida per lo sviluppo di applicazioni sicure conformi al GDPR</i> .....	84
5.8.6	<i>Tecniche di modellazione e individuazione delle minacce</i> .....	86
5.8.6.1	LINDDUN .....	86
5.8.6.2	PRoPAN .....	90
5.8.6.3	PriS .....	90
5.8.6.4	PFPSD .....	91
5.8.6.5	MPRA .....	91
5.8.6.6	Privacy in the Cloud .....	91
5.8.6.7	Adaptive privacy .....	92
5.8.6.8	STRAP .....	92
5.8.6.9	Microsoft privacy guidelines .....	92
5.8.6.10	PRET .....	93

## **6 LINEE GUIDA PER L'INDIVIDUAZIONE E LA RIVISITAZIONE DEI REQUISITI DI SICUREZZA E DI PRIVACY**

### **APPLICATIVI .....94**

6.1	LINEE GUIDA PER LA MODELLAZIONE DELLE MINACCE .....	94
6.1.1	<i>Identificazione degli obiettivi di sicurezza</i> .....	94
6.1.2	<i>Creazione di un disegno ad alto livello dell'applicazione</i> .....	94
6.1.2.1	Identificazione dei Ruoli .....	95
6.1.2.2	Identificare gli Scenari d'Uso Chiave .....	96
6.1.2.3	Identificare le Tecnologie .....	96
6.1.2.4	Identificare Meccanismi di Sicurezza Applicativa .....	96
6.1.3	<i>Scomposizione dell'applicazione</i> .....	96
6.1.3.1	Confini di fiducia (Trust boundaries) .....	97
6.1.3.2	Flussi di Dati .....	97
6.1.3.3	Punti d'Ingresso (Entry Points) .....	97
6.1.3.4	Punti di Uscita (Exit Points) .....	98
6.1.4	<i>Identificazione delle minacce</i> .....	98
6.1.4.1	Identificazione delle minacce e attacchi comuni .....	98
6.1.4.2	Identificazione delle potenziali minacce annidate nei casi d'uso .....	100
6.1.4.3	Identificazione delle potenziali minacce annidate nei flussi di dati .....	100
6.1.4.4	Esplorare ulteriori minacce utilizzando gli alberi delle minacce/attacchi .....	100
6.1.5	<i>Identificazione delle vulnerabilità</i> .....	100
6.2	IDENTIFICAZIONE DEL PROCESSO DI SVILUPPO DEL SOFTWARE SICURO .....	104
6.3	MODELLAZIONE E INDIVIDUAZIONE DELLE MINACCE CON STRIDE .....	107
6.4	VALUTAZIONE DEL RISCHIO DERIVANTE DALLE MINACCE INDIVIDUATE CON DREAD .....	107
6.5	MODELLAZIONE E INDIVIDUAZIONE DELLE MINACCE DI PRIVACY CON LINDUN .....	108

### **7 UN ESEMPIO APPLICATIVO: CASO D'USO "EASY WEB SITE" .....109**

7.1	DIAGRAMMA: USE CASE .....	109
7.2	INTERAZIONE: DA BROWSER CLIENT A WEB SERVER .....	110
7.2.1	<i>Assunzioni</i> .....	110
7.2.2	<i>Accesso a internet non valido</i> .....	110
7.2.3	<i>Mancanza di convalida dell'input da parte del "Web Server"</i> .....	110
7.2.4	<i>Cross Site Scripting</i> .....	111
7.2.5	<i>Ripudio di dati da parte del 'Browser Client'</i> .....	112
7.2.6	<i>Crash o fermo del processo 'Web Server'</i> .....	113
7.2.7	<i>Interruzione del flusso dati HTTPS (o inaccessibilità da parte del 'Web Server')</i> .....	114
7.2.8	<i>Elevazione di privilegi attraverso l'esecuzione remota di codice da parte del 'Web Server'</i> .....	115
7.2.9	<i>Elevazione dei privilegi attraverso il cambiamento del flusso di esecuzione nel codice del 'Web Server'</i> .....	115
7.2.10	<i>Cross Site Request Forgery</i> .....	116
7.3	INTERAZIONE: DA WEB SERVER A BROWSER CLIENT .....	117
7.3.1	<i>Assunzioni</i> .....	117
7.3.2	<i>Analisi delle minacce e mitigazioni</i> .....	117
7.4	INTERAZIONE: DA WEB SERVER A SQL DATABASE .....	117
7.4.1	<i>Assunzioni</i> .....	118



7.4.2	Vulnerabilità di SQL Injection nel 'SQL Database' .....	118
7.4.3	Possibile compromissione del 'SQL Database' .....	118
7.4.4	Consumo eccessivo di risorse da parte del 'Web Server' o del 'SQL Database' .....	119
7.5	INTERAZIONE: DA SQL DATABASE A WEB SERVER .....	120
7.5.1	Assunzioni .....	120
7.5.2	Persistent Cross Site Scripting .....	120
7.5.3	Controllo accesso debole per una risorsa .....	121
<b>8</b>	<b>BIBLIOGRAFIA .....</b>	<b>122</b>
<b>9</b>	<b>ANNEX A - ANALISI DELLA PANORAMICA DELLE CERTIFICAZIONI ESISTENTI .....</b>	<b>124</b>
9.1	A.1 - EPRIVACYSEAL .....	124
9.2	A.2 - EUROPRISE .....	124
9.3	A.3 - CNIL LABELS .....	126
9.4	A.4 - ICO PRIVACY SEAL .....	127
9.5	A.5 - CERTIFICAZIONE BASATA SU ISO/IEC 27001 .....	128
9.6	A.6 - CERTIFICAZIONE BASATA SU ISO/IEC 27018 .....	129
9.7	A.7 - SISTEMA PRIVACYMARK .....	130
9.8	A.8 - CERTIFICAZIONE PRIVACY BY DESIGN DELLA RYERSON UNIVERSITY & DELOITTE CANADA .....	131

## LISTA DELLE TABELLE

Tabella 1 - Documenti Applicabili .....	7
Tabella 2 - Definizioni .....	9
Tabella 3 - Acronimi .....	10
Tabella 4 - Vulnerabilità dovute a errori .....	11
Tabella 5 - Caratteristiche degli elementi DFD .....	39
Tabella 6 - STRIDE per elemento DFD .....	43
Tabella 7 - STRIDE proprietà violate .....	43
Tabella 8 - Tecniche di mitigazione .....	44
Tabella 9 - STRIDE: Indirizzamento dello Spoofing .....	47
Tabella 10 - Rischi di sicurezza OWASP relativi allo Spoofing .....	48
Tabella 11 - STRIDE: Indirizzamento del Tampering .....	49
Tabella 12 - Rischi di sicurezza OWASP relativi al Tampering .....	50
Tabella 13 - STRIDE: Indirizzamento della repudiation .....	51
Tabella 14 - Rischi di sicurezza OWASP relativi alla Repudiation .....	52
Tabella 15 - STRIDE: Indirizzamento dell'Information disclosure .....	53
Tabella 16 - Rischi di sicurezza OWASP relativi all'Information Disclosure .....	54
Tabella 17 - STRIDE: Indirizzamento del Denial of Service .....	56
Tabella 18 - Rischi di sicurezza OWASP relativi al Denial Of Service .....	57
Tabella 19 - STRIDE: Indirizzamento dell'Elevation of privilege .....	58
Tabella 20 - Rischi di sicurezza OWASP relativi all'Elevation Of Privilege .....	59
Tabella 21 - Modello DREAD .....	66
Tabella 22 - Sistema di classificazione del S.B.S.R.S. ....	68
Tabella 23 - Concetti alla base della Privacy .....	70
Tabella 24 - Minacce LINDDUN per elemento DFD .....	87
Tabella 25 - obiettivi di privacy basati sulle varie tipologie di minaccia previste in LINDDUN .....	88
Tabella 26 - LINDDUN Hard & Soft privacy .....	88
Tabella 27 - Mappatura tra obiettivi e tecniche di miglioramento della privacy .....	90

## LISTA DELLE FIGURE

Figura 1 - Processo del ciclo di sviluppo sicuro di Microsoft .....	15
Figura 2 - SDL: Passi nella modellazione delle minacce .....	16
Figura 3 - I quattro step del Framework .....	37
Figura 4 - Simbolismo nel Threat Modeling .....	38
Figura 5 - Diagramma del sistema .....	39
Figura 6 - Aggiunta dei "Trust boundaries" al diagramma .....	40

Figura 7 - Numerazione degli elementi del diagramma.....	40
Figura 8 - Esempio di disegno architetturale di una applicazione .....	95
Figura 9 - Diagramma dello use case .....	109
Figura 10 - Interazione tra Browser Client e Web Server .....	110
Figura 11 - Interazione tra Web Server e Browser Client .....	117
Figura 12 - Interazione tra Web Server e SQL Database.....	117
Figura 13 - Interazione tra SQL Database e Web Server .....	120