Intesys

Assessment per lo Sviluppo di Software Sicuro e GDPR Compliant

<<CLIENTE>>

<<NOME PROGETTO>>

Requisiti e misure di sicurezza identificati ed adottati

<<mese anno>>

LIVELLO DI RISERVATEZZA: <<da impostare a CONFIDENZIALE nella istanza consegnata al cliente>

SOMMARIO

1 Obiettivo

L'obiettivo di questo documento è rendicontare l'analisi del rischio come descritta e approfondita nei suoi elementi metodologici nel documento “Sviluppo di Software Sicuro e GDPR Compliant - Le nostre procedure e le nostre metodologie” (di seguito SSSGC) e, sulla base di questa analisi, descrivere le misure di sicurezza che Intesys propone di applicare per il progetto <<Nome Progetto>>.
Ulteriore obiettivo del documento è condividere con il cliente le valutazioni di rischio effettuate da Intesys e le misure di sicurezza da queste implicate secondo quanto descritto in SSSGC lasciando aperta la possibilità, qualora ritenuto opportuno dal cliente, di una ri-valutazione dei rischi effettuata congiuntamente con la possibilità di ampliare l'insieme delle misure di sicurezza da applicare.
In questa eventualità l'offerta economica, impostata sulla base del documento di progetto e di questo documento per le misure di sicurezza e che non prevede al livello di misure proposto nessun costo aggiuntivo, dovrà essere rivista per includere le ulteriori attività di sviluppo software implicate dalle ulteriori misure di sicurezza ritenute necessarie.

2 Il progetto

<<CLIENTE>> si è rivolta ad Intesys per <<breve descrizione dello scope del progetto, spesso ripreso tale e quale dalla introduzione del documento di progetto>>.

3 Analisi del rischio

Relativamente al progetto <<Nome Progetto>> e tenute in considerazione le specifiche funzionali che permettono di comprendere nel dettaglio i flussi informativi e il codice che li deve implementare, è stata redatta una analisi dei rischi relativamente alle 6 minacce della metodologica STRIDE (SPOOFING, TAMPERING, REPUDIATION, INFORMATION DISCLOSURE, DENIAL OF SERVICE, ELEVATION OF PRIVILEGE) approfonditamente descritte nel documento SSSGC.

Il risultato della analisi del rischio è riportato nella seguente tabella di calcolo del rischio:

MINACCE STRIDE	**PROBABILITA' [1-3|na]**					**IMPATTO S [1-3|na]**				**IMPATTO G**				**P*I**
	LCT	MOT	ORR	TAD	avgp	PRO	REP	MSL	CRP	QTD	TIP	QTI	avgi	
SPOOFING	1	1	1	1	B	1	1	1	1	1	1	1	B	**B**
TAMPERING	1	1	1	1	B	1	1	1	1				B	**B**
REPUDIATION	1	1	1	1	B	1	1	1	1				B	**B**
INFORMATION DISCLOSURE	1	1	1	1	B	1	1	1	1				B	**B**
DENIAL OF SERVICE	1	1	1	1	B	1	1	1	1				B	**B**
ELEVATION OF PRIVILEGE	1	1	1	1	B	1	1	1	1				B	**B**

La composizione Impatto S(icurezza dell’informazione) *Impatto G(dpr) per il calcolo del valore del rischio è ottenuta secondo la tabella seguente

Il valore di IMPATTO (complessivo) è calcolato secondo la seguente tabella ("N/A" viene valutato = 1).

IMPATTO (complessivo)	BASSO	MEDIO	ALTO
Somma valori	7-8-9-10	11-12-13-14-15-16-17	18-19-20-21-22

La composizione Probabilità * Impatto per il calcolo del valore del rischio è ottenuta secondo la tabella seguente

		PROBABILITA'		
		[B]ASSA (1)	[M]EDIA (2)	[A]LTA (3)
IMPATTO	[B]ASSO (1)	[B]ASSO (1)	[B]ASSO (1)	[M]EDIO (2)
	[M]EDIO (2)	[B]ASSO (1)	[M]EDIO (2)	[A]LTO (3)
	[A]LTO (3)	[M]EDIO (2)	[A]LTO (3)	[A]LTO (3)

3.1 Descrizione della tabella di calcolo

Come dettagliatamente descritto nel documento SSSGC per ogni minaccia sono stati valutati:

- i valori di 4 "Threat Agent Factors" (TAF) per il calcolo del valore medio di PROBABILITA':
  - Livello di competenza tecnica posseduto dal Gruppo di Threat Agents [LCT]
  - Motivazione [MOT]
  - Opportunità/Risorse richieste [ORR]
  - Dimensione del gruppo di threat agent [TAD]
- i valori di 4 "Key Impact Indicators" per il calcolo del valore medio di IMPATTO relativamente a "sicurezza delle informazioni":
  - Perdita di profitto [PRO]
  - Danno di reputazione [REP]
  - Multe/Spese legali [MSL]
  - Costo di ripristino [CRP]
- i valori di 3 "GDPR Impact Indicators" per il calcolo del valore medio di IMPATTO relativamente al GDPR:
  - Quantità di dati personali oggetto di trattamento [QTD]
  - Tipologia di dati personali oggetto di trattamento [TIP]
  - Quantità di interessati i cui dati personali sono oggetto di trattamento [QTI]

4 Definizione GTA e assegnazione singoli valori di PROBABILITA'

[NOTA SUL TEMPLATE DA TOGLIERE NELLA VERSIONE COMPILATA PER IL CLIENTE: sono state lasciate degli esempi di descrizioni puntuali per chiarire, semplificare e velocizzare la compilazione]

La valutazione della Probabilità è basata sulle caratteristiche dei singoli Threat Agent Factors – TAF, a loro volta strettamente dipendenti dal GTA relativo. E' necessario quindi identificare, minaccia per minaccia, il Gruppo di Threat Agents - GTA, cioè caratterizzare i gruppi di persone che possono avere interesse, capacità o semplice possibilità di minacciare l'applicazione.
Per SGL vanno considerati esclusivamente utenti "insiders" (escludendo utenti "outsiders") in quanto l'applicazione è utilizzata e utilizzabile solo dai dipendenti.
Di seguito è esplicitata la caratterizzazione del GTA e dei singoli TAF per ogni singola minaccia.

4.1.1 Spoofing

GTA: valutare se si è nel caso di utenti insiders – outsiders o entrambi, vengono considerate principalmente intenzioni malevole. Nel seguito si fa l'esempio di applicazione "business" utilizzata da utenti "insider", dipendenti o operatori legati alla azienda (es. intermediari, commerciali esterni, ...)

N.B. Si considera principalmente il caso di accesso con credenziali non proprie

LCT: il gruppo complessivo è quello dei dipendenti che possono avere accesso alla applicazione. Si considera un gruppo ristretto con numero ristretto di attori skillati (escludendo il personale IT interno), valore 1
MOT: la motivazione viene considerata bassa, valore 1
ORR: Si considera media la possibilità di conoscere credenziali di colleghi, risorse richieste medio-basse, valore 2
TAD: dimensione del gruppo ristretta, valore 1

4.1.2 Tampering

GTA:considerati solo insiders di tipo malevolo

LCT: possibilità di tampering limitata, ampiezza del gruppo di attori limitata, valore 1
MOT: motivazione considerata bassa, valore 1
ORR: Opportunità ridotte (superficie di attacco molto ristretta), risorse richieste alte, valore 1
TAD: dimensione del gruppo ristretta, valore 1

4.1.3 Repudiation

GTA:considerati solo insiders di tipo malevolo

LCT: il gruppo è ristretto a normali operatori insider, valore 1
MOT: motivazione considerata media (processi di valore elevato, può esserci motivazione a disconoscere passaggi operativi), valore 2
ORR: Opportunità ridotte (superficie di attacco molto ristretta), risorse richieste alte, valore 1
TAD: dimensione del gruppo ristretta, valore 1

4.1.4 Information Disclosure

GTA:considerati solo insiders di tipo malevolo

LCT: il gruppo è ristretto a normali operatori insider, valore 1
MOT: motivazione considerata media (informazioni di processo e commerciali rilevanti), valore 2
ORR: Quantità di dati a disposizione degli utilizzatori rilevante, dati accessibili, valore 3

TAD: dimensione del gruppo ristretta, valore 1

4.1.5 Denial of Service

GTA:considerati solo insiders di tipo malevolo

LCT: il gruppo è ristretto a normali operatori insider, competenza tecnica mediamente elevata, valore 2
MOT: per utenti malevoli può essere importante bloccare le operazioni per es. in periodo natalizio. Il denial of service è però un blocco temporaneo, valore 2.
ORR: opportunità 3 in quanto gli insider hanno accesso diretto alla applicazione, le risorse richieste sono relativamente complesse, valore 2.
TAD: dimensione ridotta (insiders), valore 1.

4.1.6 Elevation of Privilege

GTA:considerati solo insiders di tipo malevolo

LCT: la competenza richiesta non è semplice per gli insiders (escluso staff IT), valore 1
MOT: motivazione considerata media, con privilegi aumentati si possono creare artatamente disservizi, valore 2
ORR: opportunità 3 in quanto gli insider hanno accesso diretto alla applicazione, risorse richieste complesse, valore 2
TAD: dimensione ridotta (insiders), valore 1.

5 Key Impact Indicators

L'impatto viene calcolato rispetto a 4 dimensioni per ognuna delle 6 minacce.

5.1.1 Spoofing

Perdita di profitto [PRO]: abbiamo considerato esistano possibili perdite di profitto relativamente ad operazioni fraudolente con credenziali violate, valore 2
Danno di reputazione [REP]: considerato basso, valore 1
Multe/Spese Legali [MSL]: considerate basse, valore 1
Costo di ripristino [CRP][1]: intervento semplice, veloce e poco costoso, valore 1

5.1.2 Tampering

Perdita di profitto [PRO]: abbiamo considerato esistano possibili perdite di profitto relativamente a manomissione di dati (tenendo conto dell'utilizzo di backup), valore 2
Danno di reputazione [REP]: considerato medio visto il volume di ordini online, valore 2
Multe/Spese Legali [MSL]: considerate basse, valore 1
Costo di ripristino [CRP][1]: intervento potenzialmente complesso ma comunque veloce (restore dati) e poco costoso, valore 1

5.1.3 Repudiation

Perdita di profitto [PRO]: considerato basso, valore 1
Danno di reputazione [REP]: considerato basso, valore 1

Multe/Spese Legali [MSL]: considerate basse, valore 1
Costo di ripristino [CRP]: intervento semplice, veloce e poco costoso, valore 1

5.1.4 Information Disclosure

Perdita di profitto [PRO]: considerato basso, valore 1
Danno di reputazione [REP]: considerato medio visto il volume di transazioni online, valore 2
Multe/Spese Legali [MSL]: considerate basse, valore 1
Costo di ripristino [CRP]: intervento considerato semplice, veloce e poco costoso, valore 1

5.1.5 Denial of Service

Perdita di profitto [PRO]: non trascurabile, pur tenendo conto che il denial of service è per sua natura temporaneo, valore 2
Danno di reputazione [REP]: non trascurabile, valore 2
Multe/Spese Legali [MSL]: considerate trascurabili, vlore 1
Costo di ripristino [CRP]: intervento considerato semplice, veloce e poco costoso, valore 1

5.1.6 Elevation of Privilege

Perdita di profitto [PRO]: possibili perdite di profitto relativamente ad operazioni fraudolente con privilegi violati, valore 2
Danno di reputazione [REP]: considerato basso, valore 1
Multe/Spese Legali [MSL]: considerate basse, valore 1
Costo di ripristino [CRP][l]: intervento semplice, veloce e poco costoso, valore 1

6 GDPR Impact Indicators

L'impatto relativamente al GDPR non viene calcolato rispetto alle 6 minacce "STRIDE". In una prima fase viene effettuata una valutazione sulla tipologia di trattamento implicata dal progetto software in analisi per appurare se è necessario procedere ad una DPIA.
N.B. Questa valutazione viene effettuata indipendentemente dalla decisione in tal senso intrapresa dal Titolare del trattamento. Il relativo calcolo è esclusivamente al fine di valutare il livello di rischio.
Il risultato è che (in alternativa)

[
non si verifica NESSUNA delle fattispecie previste dal GDPR e riportate nel documento SSGC. Si è proceduto quindi ad una analisi dei 3 indicatori previsti dalla metodologia.

- Quantità di dati personali oggetto di trattamento [QTD]: valutare il numero di attributi in gioco e assegnare un punteggio da 1 a 3
- Tipologia di dati personali oggetto di trattamento [TIP]: se dati comuni, valore 1, valutare il valore se sono presenti dati più rilevanti/sensibili/particolari
- Quantità di interessati i cui dati personali sono oggetto di trattamento [QTI]: valutare il numero di record anagrafici in gioco e assegnare un punteggio da 1 a 3

]

[

Si verifica almeno una delle fattispecie previste dal GDPR, il livello di rischio per questa parte è settato ad ALTO con valore massimo uguale a 9. Questo valore si sommerà con i singoli valori di impatto per le singole minacce
]
---

7 Le misure da applicare

Il complesso lavoro di analisi del rischio è finalizzato a stabilire quali misure di sicurezza vanno adottate nella scrittura del codice e nella architettura della applicazione in modo da mitigare il livello di rischio calcolato. Come dettagliatamente descritto nel documento SSGC le misure di sicurezza da applicare sono quelle previste per ogni singolo livello di rischio relativamente ad ogni singola minaccia. Per ogni minaccia la colonna più a destra della tabella di calcolo del rischio indica il valore di rischio calcolato e, di conseguenza, definisce quale set di misure andrà applicato.
Il set di misure che saranno applicate (in questo caso “misure base” e “misure per livello di rischio basso”) vengono allegate al presente documento.

8 Piano dei test

E’ definito un processo di Software Quality Assurance (SQA) con l'obiettivo di assicurare che il processo di sviluppo software sia monitorato e sia compliant con lo standard ISO27001 e il GDPR. I dettagli delle procedure messe in atto sono specificati nel documento SSSGC.

9 Ruoli e responsabilità

I ruoli e le responsabilità relative all’applicazione delle misure di sicurezza identificate e al piano dei test programmato sono ripartiti secondo la seguente tabella:

RUOLI	RESPONSABILITÀ
Software Security Manager - SSM	Effettuazione dell'analisi dei rischi e relativa identificazione dei requisiti di sicurezza dei singoli progetti, approvazione del piano dei test di accettazione specificatamente dedicati alle funzioni di sicurezza (System Test e Application Test). Il ruolo di Software Security Manager è svolto dal Responsabile della Sicurezza.
Project Manager - PM	Definizione del piano dei test di sicurezza, controllo delle attività di sviluppo software nel rispetto dei requisiti.
Software Developer - SDE	In relazione ai compiti loro assegnati nel ciclo di sviluppo, realizzazione e controllo del software in ottemperanza agli adempimenti di sicurezza applicativa, conduzione del System Test e documentazione dei relativi risultati, conduzione dell’ Application Test e documentazione dei relativi risultati.

Il flusso operativo ripartito sui ruoli è il seguente:

Dopo che il PM ha completato e redatto i documenti di analisi funzionale / user interaction del progetto, il SSM procede ad effettuare l'analisi dei rischi identificando in diretta conseguenza i requisiti di sicurezza da rispettare.
Il PM procede alla definizione del piano dei test di sicurezza.
Il cliente, d'accordo con il PM, sentito il parere del SSM, può intervenire sulle misure di sicurezza da applicare concordandone di ulteriori o di diverse.
I SDE allocati al progetto realizzano il software nel rispetto dei requisiti di sicurezza stabiliti, sotto il controllo del PM.
Al termine dello sviluppo software o lungo stati di avanzamento SDE effettua i test di sicurezza previsti.