Privacy by design e by default

Un approccio concreto alla protezione dei dati
in particolare la necessità della validazione
della privacy and security by design degli applicativi software

INTRODUZIONE

Il concetto di ***protezione dei dati*** è percepito spesso in modo immediato come sinonimo di sicurezza, in realtà presenta dei connotati molti più estesi.

INTRODUZIONE

L’articolo 25 del GDPR, come noto, ha statuito che sia **al momento di determinare i mezzi del trattamento** (fase di design delle soluzioni) sia **all’atto del trattamento stesso**, il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate a garantire la conformità della soluzione disegnata ai principi e le tutele fondamentali previste dal GDPR.

Le misure citate, a titolo esemplificativo, dall'articolo 25 del GDPR sono da considerarsi senz'altro lo standard minimo di riferimento delle misure da adottare in fase di progettazione di una soluzione, quali la misura della "pseudonimizzazione" **valutata dal legislatore a priori "efficace"** al fine di implementare i principi di protezione dei dati personali e la misura della "minimizzazione" ritenuta anch'essa a priori adeguata ad integrare, nelle soluzioni in fase di progettazione, le necessarie garanzie di tutela dei diritti degli interessati.

Nel valutare l'adozione di misure di protezione dei dati e, quindi, nel valutarne anche la legittimità dell'esclusione (talvolta solo temporanea) di una misura, vanno considerati tutti gli elementi utili all'analisi del contesto, dei requisiti applicabili e dei rischi inerenti alla soluzione che si sta disegnando, tra cui in particolare andrebbero stimati:

- **lo stato dell'arte** e dei costi di attuazione di una misura.
- **la natura**, l'ambito di applicazione, il contesto e le finalità della soluzione in fase di progettazione che include il trattamento di dati personali.
- **tutti i rischi di violazione delle disposizioni del GDPR** o delle garanzie per i diritti delle persone interessate, incluse le diverse probabilità e gravità dei rischi.

Inoltre, sempre in fase di valutazione delle misure di protezione da adottare, il GDPR provvede che il tipico processo di “security by design” (ovvero il processo volto allo sviluppo sicuro di soluzioni dalla progettazione fino al testing) sia integrato dalla implementazione per **impostazione predefinita** di altre misure che, specificatamente, posso essere ritenute **adeguate a ridurre il campo dei dati personali o la portata dei trattamenti**.

I rischi inerenti la protezione dei dati personali dovrebbero essere considerati **in base a una valutazione oggettiva** mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato, tenendo a mente come **criterio di rischio target** tutti i possibili impatti negativi che potrebbero emergere per i diritti e le libertà di una persona interessata (ossia la persona a cui si riferiscono i dati personali oggetto di trattamento da parte della soluzione in progettazione), come ad esempio un consumatore, un cliente, un paziente, un utente web e via dicendo.

I rischi da analizzare e valutare in modo da individuare **le opzioni di trattamento opportune** devono essere considerati avendo riguardo delle operazioni di trattamento di dati personali insite nella soluzione in fase di progettazione suscettibili di cagionare un **danno fisico, materiale o immateriale alle persone interessate.**

Risk Assessment Table

		Severity of Harm (Impact)		
		Low (L)	Medium (M)	High (H)
Likelihood	High (H)	3	4	5
	Medium (M)	2	3	4
	Low (L)	1	2	3

Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità della soluzione progettata al GDPR spingono all'adozione di **politiche interne e misure volte a garantire di default:**

- la riduzione al minimo il trattamento dei dati personali.
- la pseudonimizzazione dei dati personali il più presto possibile.
- un alto livello di trasparenza per quanto riguarda le funzioni e il trattamento di dati personali per consentire all'interessato di controllare il trattamento dei dati.
- *continous improvement* da parte della azienda che progetta nuove soluzioni in modo da creare e migliorare continuamente, e non una tantum, le caratteristiche di sicurezza delle soluzioni disegnate.

LE BEST PRACTICE MESSE IN LUCE DALL'ENISA

Il documento di Enisa "*Recommendations on shaping technology according to GDPR provisions_Exploring the notion of data protection by default*" fa luce sulle scelte delle impostazioni predefinite che devono essere tenute in considerazione nell'ingegneria del software per garantire un adeguato livello di protezione dei dati personali, in conformità alle previsioni del GDPR.

L'obiettivo del documento, corredato da esempi pratici, è quello di rafforzare una della finalità del GDPR, ovvero di garantire una maggiore **equità nel trattamento dei dati personali**, bilanciando le scelte di business, di sicurezza e di protezione dei soggetti interessati (nella accezione di consumatori o utenti).

LE BEST PRACTICE MESSE IN LUCE DALL'ENISA

L'ENISA chiarisce, tuttavia, che le linee guida non vanno intese come uno standard di riferimento esaustivo ma un input all'analisi e ulteriore approfondimento sui diversi aspetti della protezione dei dati per impostazione predefinita, con particolare riferimento alle considerazioni che deriveranno dal **continuo bilanciamento** tra aspetti di protezione dei dati predefinite, requisiti di sicurezza e aspetti di usabilità delle soluzioni.

Mentre il GDPR **richiede** espressamente ai titolari del trattamento dei dati di operare trattamenti sulla base di un approccio "**privacy by design**", per i produttori di prodotti, servizi e applicazioni non è previsto obbligo diretto ai sensi del GDPR, tuttavia essi dovrebbero supportare i titolari del trattamento a raggiungere la piena compliance al GDPR, garantendo a loro volta una corretta progettazione e implementazione di misure pre-settings.

Il documento dell'ENISA pone molta attenzione in fase di progettazione di sistemi o serviti IT alle properties e funzionalità predefinite che **incideranno in maniera significativa sul primo impiego** dei sistemi o servizi, vale a dire i pre-settings che non comporteranno la richiesta di alcuna attività o scelta da parte dell'utente al primo utilizzo.

La cosiddetta "**Privacy Engineering**", riveste oggi un ruolo determinante perché in grado di determinare per tutti i servizi e applicativi utilizzati nella quotidianità ma anche a livello più sofisticato aziendale il tipo e l'efficacia dell'incorporazione dei requisiti di riservatezza nella progettazione, a monte, e nel funzionamento, a valle, dei sistemi di informazione.

In questo quadro, la stessa ENISA da atto che **la scelta dei valori predefiniti corretti e adeguati allo scopo** non è del tutto banale poiché richiede una valutazione della necessità per ogni scopo prefissato e un bilanciamento con altri requisiti che possono essere altrettanto importanti (si pensi all'usabilità).

Nel processo di progettazione di servizi e sistemi IT, gli sviluppatori devono decidere **i modi possibili per implementare la funzionalità desiderata.**

Per quanto riguarda le funzioni configurabili, quindi, gli sviluppatori devono determinare quali di essi devono essere pre-configurati, cioè impostati su **valori specifici** che vengono assegnati a un'impostazione configurabile del sistema o servizio, **fino a quando** tale impostazione sia cambiata mediante l'intervento dell'utente.

La domanda da porsi in fase di progettazione è:

QUESTI VALORI TENGONO CONTO

DEI PRINCIPI DATA PROTECTION?

I valori predefiniti di sicurezza determinano anche spesso **le proprietà di sicurezza di base** fornite da un servizio o un'applicazione.

Le impostazioni predefinite rilevanti per garantire la conformità al GDPR risultano, dunque, **tutte quelle che sono in grado di determinare il modo predefinito in cui un'applicazione o un dispositivo elabora i dati personali dell'utente**, ad esempio per quanto riguarda l'accesso ai dati di contatto, l'uso della videocamera o del microfono di un dispositivo, i dati di geo-localizzazione di un mobile app.

- quando sono settate le impostazioni predefinite essenziali per consentire il corretto funzionamento di sistemi e servizi senza **sottoporre agli utenti una moltitudine di domande e scelte da fare durante la loro esperienza di navigazione o utilizzo di un dispositivo o servizio**.
- quando sono settate le impostazioni predefinite essenziali per **ridurre la probabilità di** errori lato utente dovuti, ad esempio, a errate selezioni di valori al mancato knowledge dell'utente medio rispetto alle attività di configurazione.

Ciò premesso, l'ENISA sottolinea come in ogni caso la possibilità di modificare le impostazioni predefinite attinenti la protezione dei dati personali da parte dell'utente rappresenti **un requisito indispensabile** che dovrebbe essere previsto ogni qualvolta, al primo utilizzo, sono state implementate delle default settings nel servizio o sistema IT offerto, al pari di ciò che accade per la modifica dei valori predefiniti di sicurezza (si pensi ad esempio alla modifica della password predefinita al primo utilizzo).

In fase di progettazione di una soluzione, gli sviluppatori si trovano difronte alla valutazione di alcune decisioni da assumere circa le funzionalità o comportamenti specifici della soluzione che è in costruzione.

In sintesi, per ogni impostazione configurabile, deve essere deciso se è preimpostabile o meno e per ogni preimpostazione va verificato che siano soddisfatti tutti i requirements previsti nell'art. 25 del GDPR.

GDPR

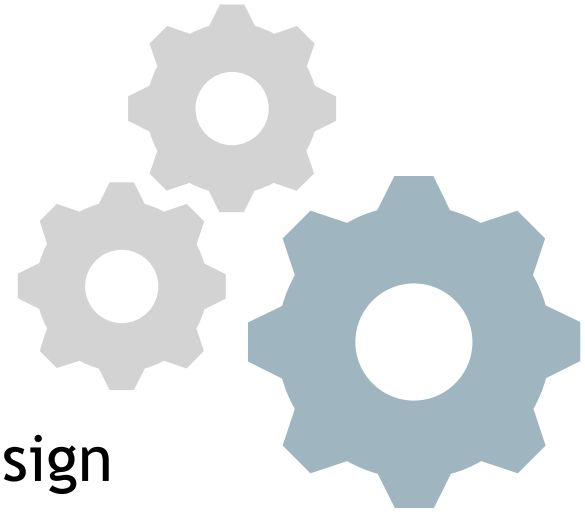
Companies must be able to provide a «reasonable» level of data protection and privacy to EU citizens. It's not completely clear what the GDPR governing body will consider reasonable

Il produttore della soluzione gioca naturalmente un ruolo determinante in questa fase, tuttavia l'ENISA sottolinea come anche il titolare del trattamento dei dati personali che utilizzerà quella soluzione, in virtù del **principio generale di accountability** (cioè il principio di responsabilizzazione nel dimostrare la sua conformità al GDPR) sarà tenuto, e quindi dovrà essere in grado, di **comprendere le impostazioni predefinite della soluzione in uso e tutte le possibili scelte di configurazione** che può percorrere al fine di modificare i valori predefiniti per accrescere il livello di protezione dei dati personali e la tutela dei diritti e delle libertà dei soggetti interessati.

Nel documento di linee guida dell'ENISA, l'Agenzia richiama alcune best practice di riferimento per l'impostazione dei valori predefiniti indicando alcuni esempi concreti per ciascuna delle 4 aree di misure citate dall'art. 25 del GDPR:

- quantità minima di dati personali.
- estensione minima del trattamento di dati personali.
- minimo periodo di conservazione dei dati personali.
- accessibilità minima dei dati personali.

Ridurre al minimo la quantità di dati personali da raccogliere e da utilizzare, in ogni step di un processo, è la **pratica alla base di tutto l'approccio PbD.** In altri termini, in ogni caso, a prescindere dal tipo di servizio o sistema da progettare, del contesto aziendale o degli utenti destinatari, il principio applicabile sempre è "meno dati personali, meglio è".



Privacy by design

Altra buona pratica suggerita dell'ENISA consiste nella **raccolta granulare di dati sulla base della necessità**, ovvero quando sussistono dei sotto-scopi che governano diverse fasi dell'elaborazione dei dati è una buona prassi che le impostazioni predefinite seguano questa granularità.

La minimizzazione, come anticipato, è una **misura concreta da valutare sia in termini quantitativi che qualitativi.**

Sotto il secondo profilo, "**l'entità minima**" dei dati può differire per lo stesso tipo di dati in base alle finalità delle funzionalità del sistema. L'ENISA riporta alcuni esempi concreti di grande utilità: nell'area delle app mobili, i dati sulla posizione sono necessari solo per alcuni scopi specifici (ad esempio l'uso del navigatore), dovrebbe essere quindi inibito per impostazione predefinita l'uso dei dati di posizione per altre finalità a meno che siano attività e configurate volontariamente dall'utente in seguito.

Infine, per determinare la minimizzazione dei dati personali, non è rilevante solo la dimensione in bit. L'obiettivo è **minimizzare il rischio** di trattamenti di dati appartenenti a categorie speciali (art. 9-10 GDPR) ovvero i cosiddetti dati sensibili o giudiziari senza che si sia verificata la condizione che ne legittima l'utilizzo o quando in ogni caso la medesima finalità potrebbe raggiungersi anche preferendo il dato personale comune a quello sensibile.

Il trattamento di dati personali, come noto, comprende vari tipi di operazioni di trattamento, così come elencate dall'art. 4 del GDPR (ad esempio cancellazione, modifica, trasmissione ecc.). L'ENISA fa luce sul fatto che **non è necessario ridurre il numero di operazioni di trattamento, ma ridurre al minimo il rischio** per i diritti e le libertà degli interessati connessi alle operazioni di trattamento.

Una buona pratica, pertanto, potrebbe essere considerata prevedere delle **dashboards** apposite, ossia dei cruscotti configurati per l'esercizio dei diritti in modalità semplificate (flag per selezioni opt-in o opt-out, button per la disattivazione di cookies ecc.).

CRITERIO DEL PERIODO DI CONSERVAZIONE NECESSARIA DEI DATI PERSONALI

Tale **principio di conservazione** limitata al **necessario**, si estende non solo ad esempio ai dati di un database aziendale ma **comprende anche tutte le copie o i log generati nel tempo**.

Trascorso il periodo di conservazione necessaria, i dati devo essere cancellati o anonimizzati.

CRITERIO DELLA ACCESSIBILITÀ CONTROLLATA

Buone politiche di *"access management"* adottate dall'azienda supportano certamente uno dei principi alla base della PbD, che è quello della **limitazione dell'accesso ai dati personali sulla base della necessità.**

Inoltre, la **limitazione degli accessi** richiama la necessità di controllare e limitare la condivisione dei dati posto che, come è ovvio, l'accessibilità ai dati aumenta se i dati personali vengono copiati o trasferiti da/ad altri destinatari o resi in altro modo disponibili (ad esempio mediante pubblicazione).

L'applicazione di un **approccio di PbD**, fondato sul dettame dell'art. 25 del GDPR nonché di linee guida come quelle emesse dall'ENISA o delle altre best practice di riferimento, rappresenta un vantaggio importante sotto diversi profili, sia in fase di sviluppo che nell'ambito dell'utilizzo di soluzioni in ambito aziendale.

Inoltre, un beneficio fondamentale per le aziende riguarda la possibilità di **non limitare lo sviluppo e la customizzazione delle soluzioni**, partendo dal presupposto che i parametri da rispettare (requisiti normativi del GDPR) non vanno intese come limitazioni ma come fattori abilitanti.

Non è sempre agevole e immediato individuare **il modo per tener traccia dei criteri adottati nelle scelte operate**, delle valutazioni condotte, delle opzioni di trattamento rischio adottate fin dalla fase di progettazione.

Inoltre, spesso si perde traccia documentale delle ragionevoli motivazioni che possono aver spinto l'azienda o il produttore di un sistema o servizio IT a preferire l'adozione di una misura invece che di un'altra (ad esempio tenendo in considerazione lo stato dell'arte, il contesto, i costi o altri elementi che il GDPR stesso prevede possano essere tenuti in considerazione in ottica di valutazione complessiva).

Nell'ambito di grandi progetti di disegno di architetture software o progetti di Cloud Migration (ad esempio di CRM aziendali) o ancora in progetti di sviluppo di servizi innovativi per le aziende, diventa cruciale tener traccia formale di tutte le scelte operate sin dall'avvio del progetto, in modo da garantire che l'azienda titolare del trattamento dei dati possa **comprovare l'adozione di una soluzione compliant al GDPR** (in linea al principio di accountability).

Sotto questo profilo un documento di estremo rilievo è rappresentato dai **Report di Solution Design** che generalmente descrivono, nell'ambito di grandi progetti, la metodologia di lavoro utilizzata (es. standard, hybrid agile ecc.), la prototipazione delle soluzioni e la messa in produzione finale o mediante rilasci graduali prima del go-live di una soluzione.

I REPORT DI SOLUTION DESIGN COME STRUMENTO DI ACCOUNTABILITY

Questo tipo di documento è sempre stato considerato di esclusivo appannaggio di "tecnici" ovvero di web designer, sviluppatori di software, progettisti ecc., essendo meno comune ogni apporto di contenuti e considerazioni legali o normative, anche basate su attività di **risk assessment** che descrivano le scelte operate nelle configurazioni di default settings in ottica privacy by design.

Risk Matrix

Hazard Severity	Likelihood of Occurrence: Very Unlikely (Little or no chance of occurrence)	Unlikely (A rare combination of factors would be required for an incident to result.)	Possible (Not certain to happen but an additional factor may result in an accident)	Probable (More likely to occur than not)
Minor (No or minor injury (first aid))	CARE	CARE	CARE	CAUTION
Moderate (Off-site medical treatment or DAFW*)	CARE	CARE	CAUTION	ALERT
Serious (More than one DAFW, long-term absence)	CARE	CAUTION	ALERT	STOP!
Major (Permanent disability or harm, fatality)	CAUTION	ALERT	STOP!	STOP!

*DAFW – Day Away From Work

CARE	Minor harm possible, serious harm very unlikely to occur; implement controls and ensure care is taken when performing activity.
CAUTION	Minor harm probable, major harm unlikely to occur; follow all control measures, increased level of competence required and ongoing self-assessment of risks identified.
ALERT	Moderate degree of harm probable but major harm unlikely; critically assess the risks and appropriate controls. Specific competence required and ongoing assessment of risks by individual and/or supervisor.
STOP!	Serious or major harm will probably occur; stop the activity and critically assess the risks, review safety aspects of activity and implement further, appropriate controls. Consider referencing HSE or other Best Practice, consider involving HSS.

Risulta, invece, a parere di chi scrive, di fondamentale importanza che tutta la documentazione descrittiva e attestante la prototipazione delle soluzioni sia supportata anche dai risultati di valutazioni normative, di legittimità e dei risultati delle valutazioni dei rischi e degli impatti per gli interessati (richiamando talvolta anche documenti specifici di DPIA) al fine di poter avere un maggior controllo delle scelte operate e **una traccia documentale atta a comprovare il livello di conformità a GDPR o altre previsioni normative applicabili della soluzione disegnata** (inclusi i provvedimenti o pareri delle Autorità Garanti).

La **metodologia di attuazione dell'approccio di privacy by design** dovrebbe essere descritta e tracciata in un documento al fine di tracciare gli steps e le modalità di valutazione del disegno della soluzione, ad esempio: riferimenti alle attività di risk assessment, alle valutazioni di impatto eseguite (**DPIA**), check di approfondimenti in ambito privacy dedicati a verificare la corretta implementazione delle misure di protezione prima dei singoli rilasci delle soluzioni, implementazione delle raccomandazioni del DPO (ove presente in azienda).

OpenSAAM è un framework supportato da OWASP (Open Web Application Security Project) che si basa su un insieme di procedure di sicurezza legate a quattro importanti funzioni di business critiche, coinvolte nello sviluppo del software, vale a dire Governance, Costruzione, Verifica e Distribuzione.

Ciascuna funzione di business adotta tre pratiche di sicurezza e ciascuna di esse è suddivisa in tre livelli di maturità. La valutazione delle minacce è la prima pratica di sicurezza adottata durante la funzione di business “Costruzione”. Questa utilizza il Threat modeling per identificare i potenziali rischi. OpenSAAM non si lega ad alcun approccio di modellazione delle minacce e raccomanda l'uso di STRIDE della Microsoft o TRIKE come possibili opzioni.

L'iniziativa di sicurezza **BSIMM** è stata progettata per aiutare i team di sviluppo software a comprendere e pianificare la sicurezza in un ciclo di vita di sviluppo delle applicazioni, studiando le pratiche di cinquantuno importanti iniziative di sicurezza software.

Aziende come Google, Adobe, Intel, Visa, Nokia, Sony e Microsoft hanno partecipato alla ricerca guidata da Gary McGraw (leader esperto di settore nella sicurezza del software, vicepresidente della Security Technology presso la Synopsys Inc. SNPS, autorità riconosciuta a livello mondiale per la sicurezza del software e autore di otto libri tra i più venduti su questa tematica). La metodologia risultante ha unito le migliori pratiche (parere del team BSIMM) in un'unica iniziativa.

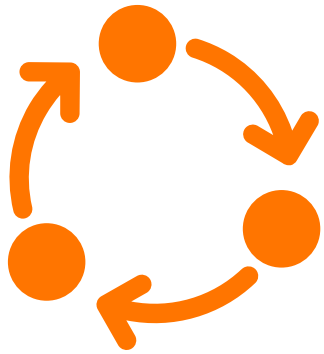
Il **CLASP** è un altro framework di sicurezza supportato dall'OWASP che contiene best practices formalizzate per attuare la sicurezza, in modo strutturato e ripetibile, nei cicli di vita di sviluppo di software in essere o in divenire.

Il framework esiste dal 2005, ma non sono stati registrati recenti aggiornamenti del progetto. È stato originariamente sviluppato dalla Secure Software Inc. e successivamente donato a OWASP che lo ha rilasciato come soluzione completa di sicurezza a favore delle organizzazioni. Insieme all'SDL di Microsoft, CLASP è stato riconosciuto come uno dei processi originali di alto profilo per lo sviluppo di software sicuro.

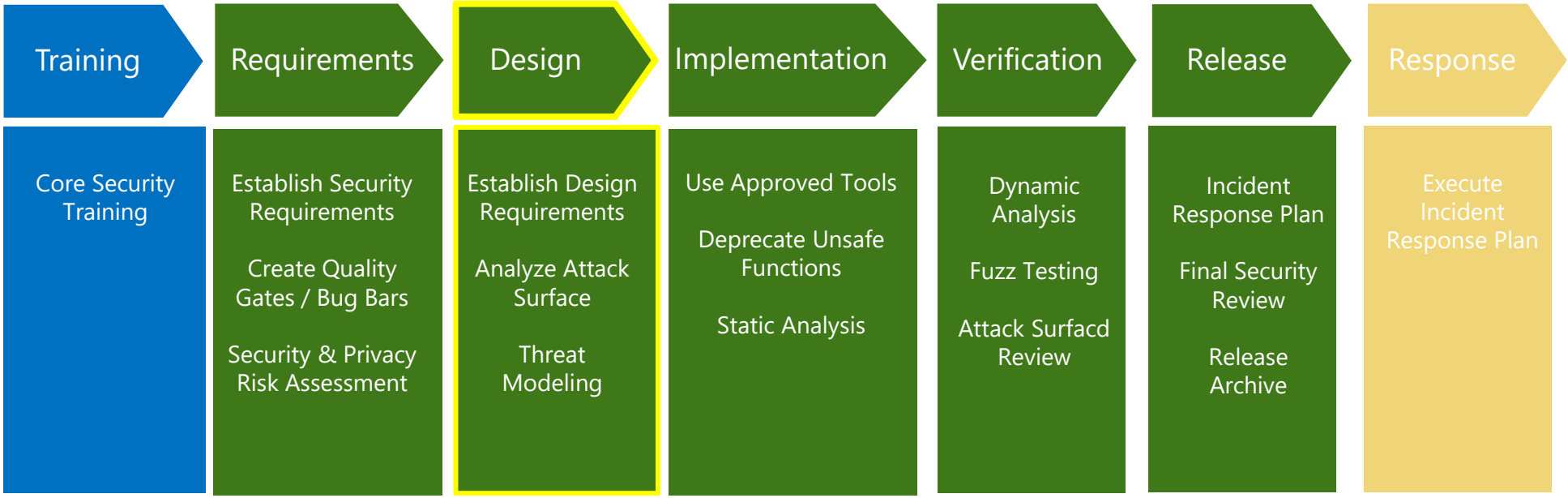
Il ciclo di vita di sviluppo sicuro (**SDL**) è una metodologia introdotta dall'iniziativa "**Trustworthy Computing**" di Microsoft. SDL mira a ridurre i costi di manutenzione del software e ad aumentare l'affidabilità implementando la sicurezza in ciascuna fase del ciclo di vita dello sviluppo.

Il processo consiste in pratiche di sicurezza, raggruppate in sette fasi distinte:

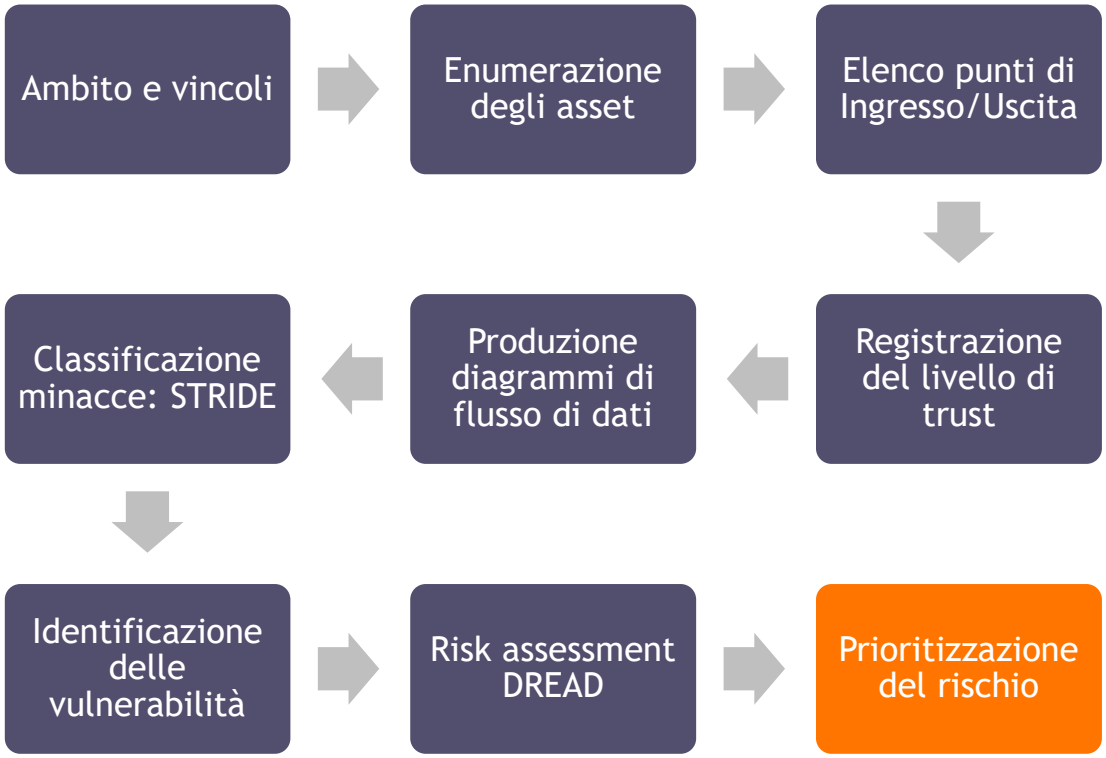
1. Formazione
2. Requisitazione
3. Progettazione
4. Implementazione
5. Verifica
6. Rilascio
7. Monitoraggio/manutenzione



Uno degli aspetti chiave dell'SDL è l'introduzione del **Threat Modeling** nella fase di progettazione, che promuove l'individuazione preventiva delle vulnerabilità presenti nelle applicazioni e alcune volte persino i potenziali difetti di progettazione.



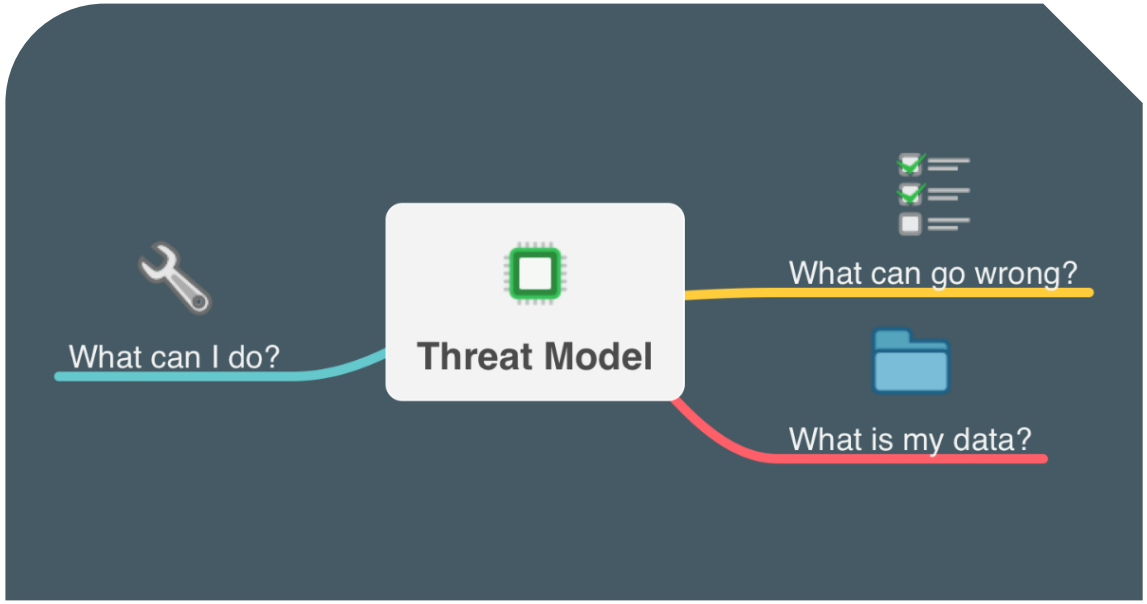
L'obiettivo che tutte le metodologie di modellazione delle minacce condividono è lo sviluppo di un processo a passi iterativi che un team di sviluppo può facilmente seguire durante la valutazione di un sistema software.



Quando ci si approccia con la modellizzazione delle minacce, è importante avere una corretta comprensione della terminologia di base:

• **Asset**, è qualcosa di valore su cui un avversario pone particolare interesse. I dati presenti in un database sono un esempio di Asset.
• **Minaccia** (threat), è un evento che può o non essere dannoso all'origine ma che può danneggiare o compromettere un'attività a seguito di un attacco.
• **Vulnerabilità**, è un difetto nella sicurezza di una o più parti di un sistema che rende possibile una minaccia.
• **Attacco**, è un tentativo da parte di un avversario di sfruttare una vulnerabilità.
• **Rischio**, è la probabilità di essere bersaglio di un attacco.
• **Contromisura**, è un'azione o uno strumento che contrasta una minaccia e mitiga il rischio.

La **modellazione delle minacce** è una parte importante del ciclo di vita del software che identifica le minacce che potrebbero non essere riconosciute nelle tradizionali sessioni di brainstorming sulla sicurezza.



Una volta raccolte le minacce individuate in una o più liste, il **passo successivo** nel processo di modellazione è quello di scorrere l'elenco o gli elenchi **indirizzando ciascuna minaccia**.

Ci sono quattro tipologie di azioni che si possono intraprendere per contrastare tali minacce:

- Mitigazione
- Eliminazione
- Spostamento
- Accettazione

Microsoft ha sviluppato la metodologia **DREAD** (tabella che segue) per valutare ciascun rischio individuato durante l'attività **STRIDE**. Ad ogni rischio viene assegnato un **punteggio DREAD** da parte del team di sicurezza/sviluppo i quali realizzano e applicano il modello delle minacce.

Danger level and colour	Avalanche probability and avalanche trigger	Recommended action in the backcountry
1 – LOW (green)	Natural slab avalanches highly unlikely. Human triggered avalanches **unlikely**.	Travel is generally safe. Normal caution advised
2 – MODERATE (yellow)	Natural slab avalanches unlikely. Human triggered avalanches **possible**.	Use caution in steeper terrain on certain aspects.
3 – CONSIDERABLE (orange)	Natural avalanches possible. Human triggered avalanches **probable**.	Be increasingly cautious in steeper terrain.
4 – HIGH (red)	Natural and human triggered avalanches **likely**.	Travel in avalanche terrain is not recommended.
5 – EXTREME (red, black border)	Widespread natural and human triggered avalanches **certain**.	Travel in avalanche terrain should be avoided and confined to low angle terrain, well away from avalanche path runouts.

In generale, in termini quantitativi, il rischio è definito come il prodotto tra la probabilità di accadimento dell'evento e l'impatto:

Rischio = Probabilità x Impatto

In effetti, se almeno uno dei due termini del prodotto tende a zero, percepiamo il rischio come basso. Viceversa percepiamo un rischio grave quando ambedue i termini sono elevati.

Nella metodologia **DREAD** il concetto di "**impatto**" viene declinato in termini di:
- danno (Damage)
- utenti interessati (Affected Users)

Mentre il concetto di "probabilità" viene declinato in termini di:
- riproducibilità (Reproducibility)
- sfruttabilità (Exploitability)
- rilevabilità (Discoverability)

DREAD è appunto l'acronimo che "**fattorizza**" il rischio rispetto a queste 5 distinte categorie che caratterizzano la minaccia

Damage potential

- Quanto sarebbe rilevante il danno in caso di concretizzazione della minaccia?

Reproducibility

- Quanto è facile che la minaccia possa ripetersi?

Exploitability

- Quanto tempo, sforzo e conoscenza è necessaria per concretizzare con successo la minaccia?

Affected Users

- Nel caso in cui la minaccia si concretizzi, quale percentuale di utenti sarebbe coinvolta?

Discoverability

- Quanto è facile per un attaccante scoprire la minaccia?

A ciascuna categoria viene attribuito un peso. Il “DREAD score” è la media dei 5 pesi, ossia:

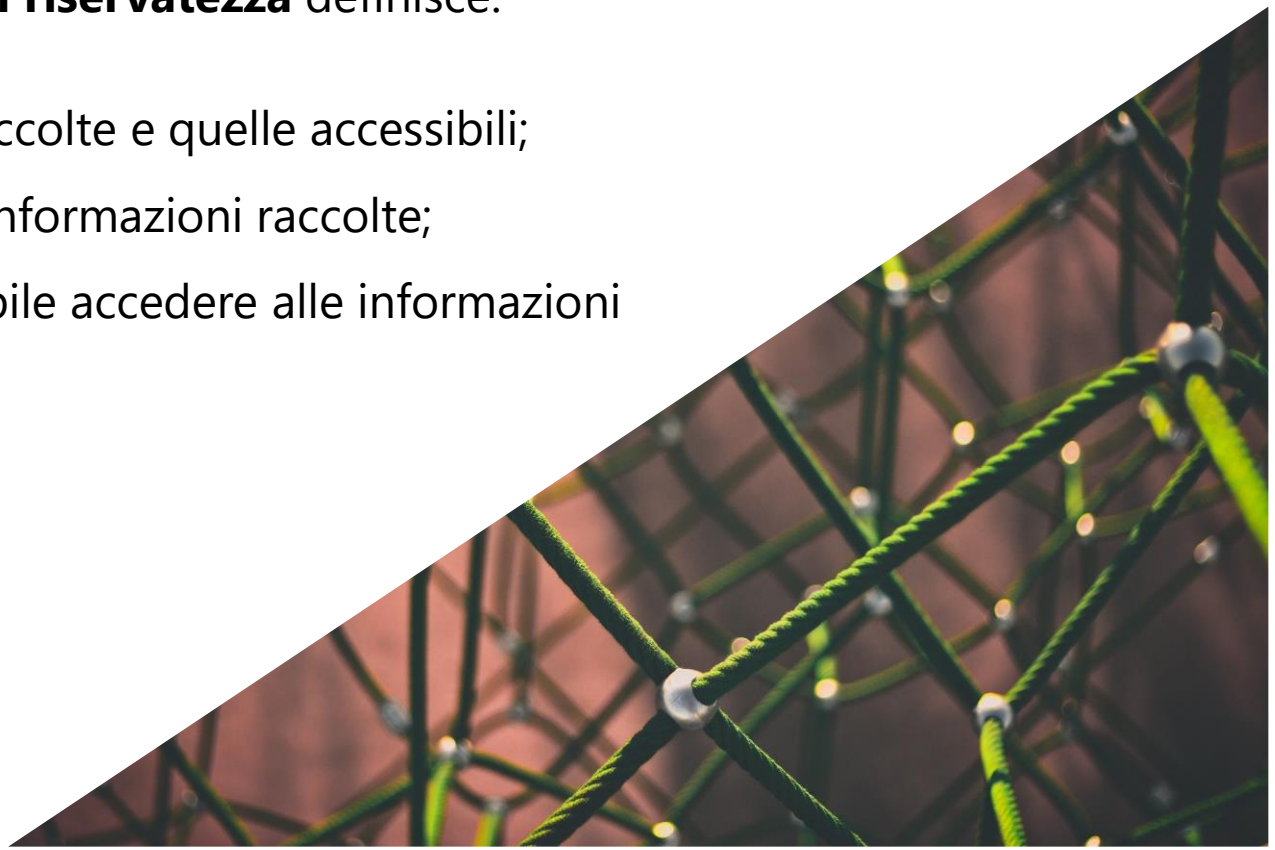
DREAD Score =
(Damage + Reproducibility + Exploitability + Affected Users + Discoverability) / 5

Occorre quindi valutare e dare un peso numerico alle cinque categorie della tabella sopra mostrata. A seconda del dominio considerato, ci si può riferire o a una scala (semplificata) di tre soli valori o a una scala (più granulare) a dieci valori.

I valori crescono rispettivamente al crescere del danno, della facilità di riproduzione, della facilità di sfruttamento, del numero di utenze coinvolte, della facilità di rilevamento.

Un'istruzione della **politica di riservatezza** definisce:

- I tipi di informazioni raccolte e quelle accessibili;
- Chi può accedere alle informazioni raccolte;
- Per quali scopi è possibile accedere alle informazioni

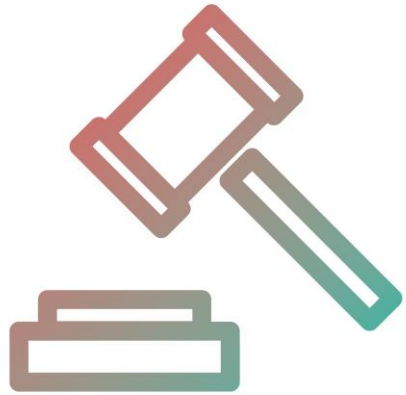


CONCETTI BASE PRIVACY BY DESIGN

Similmente alla miriade di normative sulla privacy disponibili, ci sono stati diversi tentativi di strutturare e classificare i concetti di privacy.

Di seguito si riportano alcuni esempi di tassonomie basate su due approcci distinti:

- Classificazione dei concetti di privacy da un punto di vista giuridico;
- Classificazione dei concetti di privacy da un punto di vista di ingegneria del software



La **Tassonomia di Solove** presenta una tassonomia delle violazioni della privacy da un punto di vista legale.

Anche se questa non tratta la privacy digitale, ma descrive la privacy in generale, fornisce comunque alcune informazioni utili in materia.

Solove opera una distinzione tra quattro gruppi di attività di base dannose:

- Raccolta dei dati
- Trattamento dei dati
- Diffusione dei dati
- Invasione

Linee guida FIPPs (Fair Information Practice Principles)

I principi si basano su **cinque** distinte **categorie:**

- **Avviso Consapevolezza**
- **Scelta/Consenso**
- **Accesso/Partecipazione**
- **Integrità/Sicurezza**
- **Enforcement/Redress**

European Data Protection Legislation

Riassumiamo la **Direttiva Europea sulla Protezione dei Dati** nei seguenti nove principi:

- Elaborazione corretta e lecita
- Consenso
- Finalità
- Minimalità
- Informazione minima
- Qualità dell'informazione
- Controllo dell'interessato
- Sensibilità
- Sicurezza delle informazioni

Poiché il DPD è stato creato in un momento in cui Internet era ancora agli inizi, nel 2012 è stata elaborata una proposta di riforma della legislazione attuale per rafforzare i diritti della privacy online.

Questa riforma indirizza:

• il "**diritto all'oblio**" ovvero, l'obbligo di fornire esplicitamente il consenso necessario al trattamento dei dati;
• il "**diritto di portabilità dei dati**" che consente un accesso più facile ai propri dati e una maggiore trasparenza sul modo in cui questi vengono gestiti.

Anche la responsabilità di coloro che trattano i dati personali è accresciuta dall'attuazione di principi quali "**Privacy by Design**".

CONCETTI BASE PRIVACY BY DESIGN

La privacy si basa prevalentemente su **due modelli di tutela**:

- ***hard privacy*** (la privacy quale libertà negativa)
- ***soft privacy*** (privacy quale libertà positiva)

Alla base del modello di privacy, ci sono alcune delle classiche proprietà di sicurezza quali:

- **confidenzialità,** garantisce che le informazioni siano accessibili solo da parte di persone autorizzate;
- **integrità,** garantisce l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione;
- **disponibilità** (o resistenza alla censura), garantisce che le informazioni siano accessibili agli utenti autorizzati;
- **non ripudio,** garantisce che non si sia in grado di negare ciò che si è fatto.

Le caratteristiche di queste proprietà si trovano nella norma ISO 17799.

A queste si aggiungono ulteriori proprietà quali:

- **Unlinkability**
- **Anonymity**
- **Pseudonymity**
- **Plausible deniability**
- **Undetectability and unobservability**
- **Confidentiality**
- **Content awareness**
- **Policy and consent compliance**

I PRINCIPI DELLA PRIVACY BY DESIGN

La **Privacy by Design** è un concetto sviluppato alla fine degli anni 90 da Ann Cavoukian commissario per l'informazione e la privacy dell'Ontario. Si tratta di un approccio ingegneristico che si concentra sull'intero processo a partire dai principi di privacy e protezione dei dati.

La privacy by Design può essere raggiunta applicando i sette principi su cui si basa:

- **Proattivo non reattivo, preventivo non correttivo**
- **Privacy come impostazione predefinita**
- **Privacy incorporata nella progettazione**
- **Piena funzionalità - somma positiva, non somma zero**
- **Sicurezza end-to-end - Tutela dell'intero ciclo di vita**
- **Visibilità e trasparenza**
- **Rispetto per la privacy degli utenti**

Il panorama tecnologico della privacy è stato classificato secondo tre paradigmi che tuttavia, non si escludono a vicenda:

- **Privacy come controllo**
- **Privacy come riservatezza**
- **Privacy come pratica**

Ridurre al minimo i dati personali utilizzati

Ridurre l'impatto dei rischi limitando la gestione di dati personali a ciò che è strettamente necessario per raggiungere lo scopo definito.

Gestire i periodi di conservazione dei dati personali

Ridurre l'impatto dei rischi assicurando che i dati personali non vengano mantenuti per più di quanto necessario.

Informare i soggetti e ottenere il consenso

Consentire ai soggetti interessati di effettuare una scelta libera, specifica e informata.

Partizionare i dati personali - Ridurre la possibilità che i dati personali possano essere correlati e che possa verificarsi una violazione di tutti i dati personali.

Cifrare i dati personali - Rendere incomprensibili i dati personali a chiunque senza autorizzazione di accesso.

Anonimizzare i dati personali - Eliminare le caratteristiche che identificano i dati personali.

LINDDUN è una metodologia speculare alla modellazione delle minacce STRIDE (STRIDE-per-element) e tratta le violazioni delle seguenti proprietà sulla privacy:

- **Collegabilità** (Linkability);
- **Identificabilità** (Identifiability);
- **Non ripudio** (Non Repudiation);
- **Rilevabilità** (Detectability);
- **Divulgazione di informazioni** (Disclosure of information);
- **Inconsapevolezza sul contenuto** (Content Unawareness);
- **Inaderenza alla politica sul conseno** (Policy and consent Non compliance).

La tabella seguente, mostra la correlazione tra le minacce di privacy previste da LINDDUN e le tipologie di elementi DFD sopra descritte:

Elemento DFD	L	I	N	D	D	U	N
Archivio dati	X	X	X	X	X		X
Flusso dati	X	X	X	X	X		X
Processo	X	X	X	X	X		X
Entità	X	X				X	

L'obiettivo di questa metodologia è quello di assistere gli ingegneri del software nella requisitazione al fine di ottenere le seguenti informazioni:

- Conoscenza del settore rilevante per la privacy
- Dati personali trattati
- Requisiti di riservatezza

La metodologia consiste in quattro fasi:

- Disegno del diagramma di contesto e dei diagrammi dei problemi
- Aggiunta dei requisiti di privacy al modello
- Generazione di grafici delle minacce alla privacy
- Analisi dei grafici delle minacce alla privacy

PriS è un metodo di ingegnerizzazione dei **requisiti di sicurezza**, che integra i requisiti di riservatezza già nelle fasi iniziali del processo di sviluppo del sistema.

PriS considera i **requisiti relativi alla privacy** come **obiettivi organizzativi** che devono essere soddisfatti e adotta l'uso di modelli di processi di privacy come un modo per:

1. Descrivere l'effetto dei requisiti relativi alla privacy sui processi aziendali
2. Facilitare l'identificazione dell'architettura di sistema che meglio supporta i processi aziendali in relazione agli aspetti di privacy

In questo modo, PriS fornisce un **approccio olistico** che va dagli obiettivi di alto livello ai sistemi informatici "**rispettosi della privacy**«. Il metodo si articola in **quattro fasi**:

1. **individuare** gli obiettivi di tutela della privacy
2. **analizzare** l' impatto degli obiettivi di tutela della privacy sui processi organizzativi
3. **modellare** i processi interessati utilizzando modelli di tutela della privacy
4. **identificare** le **tecniche** che meglio supportano o implementano i processi summenzionati

FPFSD è un **framework** per la **progettazione** di sistemi rispettosi della privacy (framework for privacy-friendly system design) in cui si attua una distinzione tra due diversi approcci alla privacy:

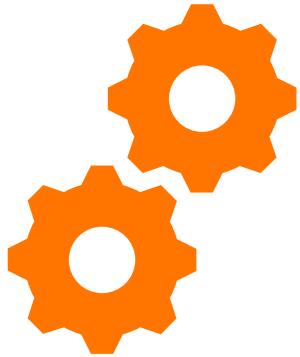
Privacy-by-policy, introduce l'approccio di notifica e consenso basato sui principi di Fair Information Practice Principles (FIPP) e implica che l'utente sia informato su quali informazioni vengono utilizzate e perché. Inoltre, l'utente può decidere di non fornire dati.

Privacy-by-architecture, incoraggia l'archiviazione dei dati presso il cliente invece di far archiviare le informazioni riservate dalle aziende stesse.

MPRA: una tecnica multilaterale per l'analisi dei requisiti in materia di tutela della privacy (multilateral privacy requirements analysis technique). Si articola in tre fasi principali: analisi degli stakeholder, analisi funzionale e analisi della privacy.

Privacy in the Cloud: In tempi recenti è stato realizzato uno dei primi framework in-the-cloud. Esso è composto da un linguaggio (basato su Secure Tropos) e da un processo (basato su PriS) a supporto dell'analisi della sicurezza e della privacy.

STRAP è un framework di analisi della privacy che è stato sviluppato sulla base dei risultati dell'analisi di sei framework esistenti.



Identificazione dei Ruoli

È importante identificare i **ruoli** all'interno dell'applicazione, ossia, **chi può fare cosa**. La fase di identificazione dei ruoli è utilizzata sia per determinare **ciò che dovrebbe accadere** (accesso alle risorse autorizzate come stabilito per lo specifico ruolo) che per determinare **ciò che non dovrebbe accadere** (accesso a risorse per le quali non si ha l'autorizzazione).

Identificare gli Scenari d'Uso Chiave

In questa fase occorre identificare le **principali funzionalità e modalità d'uso** e dettagliare gli aspetti legati alle attività di creazione, lettura, aggiornamento e cancellazione dei dati. Le caratteristiche chiave vengono spesso descritte nel contesto dei casi d'uso e permettono di far capire come l'applicazione è destinata ad essere utilizzata e come può essere utilizzata in modo improprio. I casi d'uso consentono di identificare i **flussi di dati** e di focalizzarsi sull'analisi di eventuali minacce nelle fasi successive di dettaglio della modellizzazione.

Identificare le Tecnologie

Occorre identificare tutte le tecnologie utilizzate e le loro caratteristiche: Sistemi operativi; Server Web; Server di Base Dati; tutte le tecnologie utilizzate per implementare la presentazione dei dati a livello utente, per gestire le regole di business, per l'accesso ai dati sottostanti e il linguaggio di sviluppo utilizzato.

Scomposizione dell'applicazione

La **scomposizione dell'applicazione** è utile per scoprire le minacce e le vulnerabilità del sistema. Nell'ottica di sicurezza, i componenti più importanti sono:

- confini di fiducia (trust boundaries);
- flussi di dati;
- punti di ingresso (entry points);
- punti di uscita (exit points).

Identificare Meccanismi di Sicurezza Applicativa

Un'altra fase importante è l'identificazione dei meccanismi di sicurezza applicativa, in particolare occorre analizzare i seguenti aspetti:

- Validazione input e dati
- Autenticazione
- Autorizzazione
- Gestione della configurazione
- Dati sensibili
- Gestione della sessione
- Crittografia
- Manipolazione dei parametri
- Gestione delle eccezioni
- Audit e gestione dei log

Confini di fiducia (Trust boundaries)

Identificare i confini di fiducia dell'applicazione aiuta a concentrare l'analisi sulle aree di maggiore interesse. I confini di fiducia evidenziano dove cambiano i livelli di fiducia. In quest'ambito, la fiducia è intesa in chiave di riservatezza e integrità.

Per identificare i confini di fiducia occorre:

- Iniziare individuando i confini del sistema esterno.
- Identificare i punti di controllo di accesso o i luoghi chiave in cui l'accesso richiede privilegi aggiuntivi o l'appartenenza ad un dato ruolo.
- Identificare i confini di fiducia da una prospettiva di flusso di dati

Flussi di Dati

È importante tracciare il **flusso dei dati** all'interno dell'applicazione dal punto di ingresso al punto d'uscita. Questa attività è necessaria per comprendere come interagisce l'applicazione con i sistemi esterni, i sistemi client e come **interagiscono** i componenti interni.

Punti d'Ingresso e Punti di Uscita

I **punti di ingresso** dell'applicazione servono anche come punti di ingresso per gli attacchi. Il front-end di una applicazione web che è in ascolto di richieste http è un esempio di punto di ingresso vulnerabile agli attacchi.

È importante identificare da dove l'applicazione **invia i dati all'utente o ai sistemi esterni**, dando priorità ai punti di uscita in cui l'applicazione scrive dati che includono l'input proveniente dall'utente o dati provenienti da fonti non attendibili, ad esempio basi dati condivise.

Identificazione delle minacce

In questa fase, è possibile individuare minacce e attacchi che potrebbero compromettere l'applicazione e gli obiettivi di sicurezza. Il processo di identificazione consiste in sessioni di brainstorming tra i team di sviluppo e test.

Durante questa attività di identificazione delle minacce si eseguono le seguenti attività:

- Identificazione delle minacce e degli attacchi comuni
- Identificazione delle minacce annidate nei casi d'uso
- Identificazione delle minacce annidate nei flussi di dati

Identificazione delle potenziali minacce annidate nei casi d'uso

Occorre esaminare i casi d'uso chiave, che sono stati individuati nella fasi precedenti, per capire il modo in cui un utente potrebbe influenzare malevolmente o involontariamente l'applicazione ad eseguire un'operazione non autorizzata o a divulgare dati riservati o privati. In questa fase ci si pongono domande immedesimandosi nella figura dell'aggressore.

Identificazione delle potenziali minacce annidate nei flussi di dati

Occorre rivedere i casi d'uso e gli scenari chiave e analizzare i flussi di dati, in particolare, i flussi di dati tra i singoli componenti dell'architettura. Il flusso di dati che attraversa i confini di fiducia è richiede particolare attenzione. Nella stesura del codice, si deve assumere che, tutti i dati esterni al confine di fiducia dell'applicativo siano dannosi.

Identificazione delle vulnerabilità

Così come è stato fatto nel processo di identificazione delle minacce, si fornisce di seguito una rassegna delle diverse categorie di vulnerabilità.

In questa fase, l'obiettivo è quello di analizzare le vulnerabilità (le minacce sono state già trattate nel paragrafo precedente) partendo dal principio che per poter analizzare correttamente un'applicazione è necessario valutare le sue vulnerabilità ad ogni livello.

Alcuni dei vantaggi apportati con l'integrazione degli aspetti di sicurezza nel ciclo di vita di sviluppo del sistema, sono:

- L'individuazione preventiva e la mitigazione delle vulnerabilità e dei problemi di sicurezza presenti nella configurazione dei sistemi, con conseguente riduzione dei costi per l'implementazione dei controlli di sicurezza e delle tecniche di mitigazione delle vulnerabilità;
- La consapevolezza delle potenziali sfide ingegneristiche dovute ai controlli di sicurezza obbligatori;
- L'identificazione dei servizi di sicurezza condivisi e riutilizzo delle strategie e degli strumenti di sicurezza che riducono i costi di sviluppo e migliorano la condizione di sicurezza complessiva del sistema, attraverso l'applicazione di metodi e tecniche collaudate;

- La facilitazione nell'attuazione delle decisioni prese da parte dei dirigenti, attraverso l'applicazione tempestiva di un processo completo di gestione del rischio;
- La documentazione di importanti decisioni di sicurezza prese durante il processo di sviluppo, per informare la direzione sulle considerazioni di sicurezza intraprese durante tutte le fasi dello sviluppo;
- Il miglioramento dell'organizzazione e della fiducia dei suoi utenti nel promuovere l'adozione e l'uso dei propri sistemi;
- Una migliore interoperabilità e integrazione dei sistemi che sarebbe difficile raggiungere se la sicurezza fosse considerata separatamente ai vari livelli.

La **modellazione delle minacce** è un approccio per analizzare la sicurezza di un'applicazione.

Si tratta di un approccio strutturato che consente di identificare, quantificare e affrontare i rischi di sicurezza associati a un'applicazione.

Il concetto di modellazione delle minacce non è nuovo, ma negli ultimi anni si è verificato un chiaro cambiamento di mentalità.

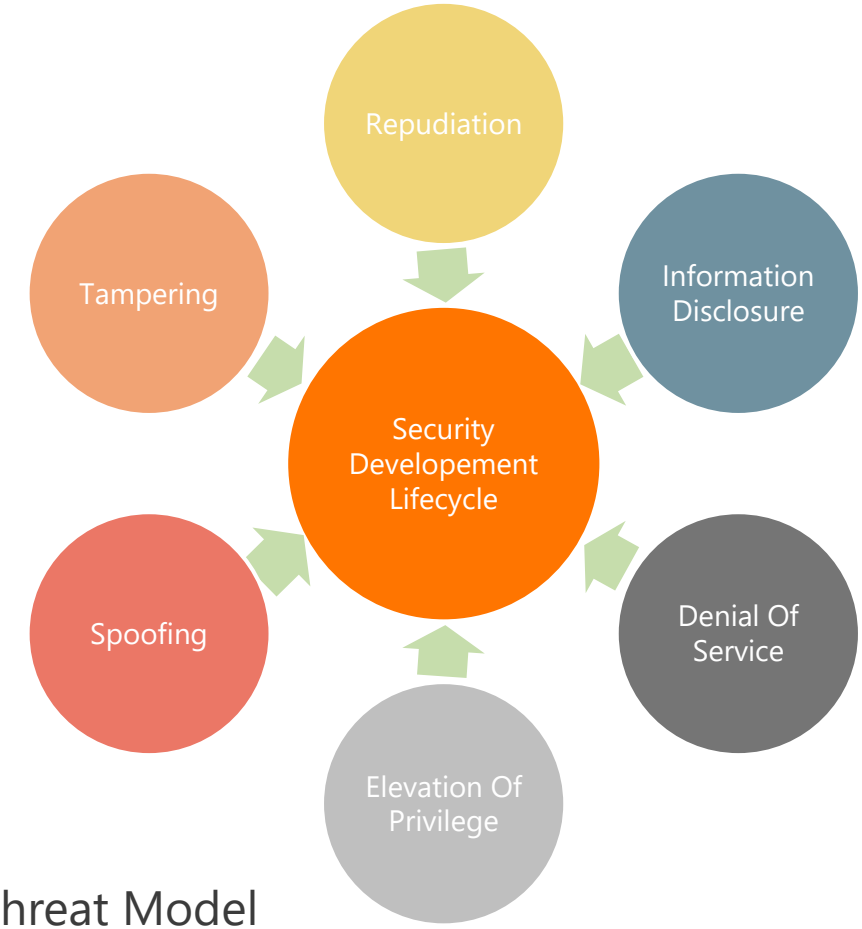
La modellazione delle minacce, oggi guarda ad un sistema dal punto di vista di un potenziale attaccante, piuttosto che dal punto di vista del difensore.

Microsoft è stata forte sostenitrice del processo negli ultimi anni.

Questi, i **vantaggi** introdotti dal processo di **modellazione delle minacce**:

- la conferma dell'idoneità degli elementi di sicurezza individuati da attuare;
- l'individuazione di eventuali lacune nelle caratteristiche di sicurezza da attuare;
- l'identificazione di eventuali altri elementi di sicurezza;
- l'identificazione dei requisiti di policy e di processo;
- l'identificazione dei requisiti da inserire nelle operazioni di sicurezza;
- l'identificazione dei requisiti in materia di tracciamento e monitoraggio;
- arrivare ai casi di abuso, se utilizzati, secondo la metodologia Agile;
- la comprensione dei requisiti di business continuity;
- la comprensione dei requisiti in materia di capacità e disponibilità.

La categorizzazione delle minacce di sicurezza può essere ottenuta mediante l'adozione di un modello denominato **STRIDE** che è l'acronimo che riunisce la gamma dei rischi a cui può essere soggetta l'applicazione e per i quali deve essere protetta.



STRIDE Threat Model

Le linee guida per la modellazione delle minacce ispirata a MS-SDL si suddivide nelle seguenti fasi:

- Identificazione degli asset
- Creazione di una panoramica dell'architettura
- Scomposizione del sistema in sotto-componenti fino al livello più basso possibile
- Identificazione delle minacce
- Documentazione delle minacce
- Valutazione delle minacce secondo il modello DREAD

CONCLUSIONE E RINGRAZIAMENTI

*“Il problema non è la tecnologia, ma **l'uso che se ne fa**.*
*Ogni cosa comporta dei rischi, l'importante è esserne **consapevoli** e valutare se il prezzo che paghiamo (meno privacy) è adeguato a quanto riceviamo in cambio.”*