UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unimc

Sviluppo software sicuro: un approccio pratico basato sulle linee guida AGID

Mariagrazia Forte

Venerdì 03 Ottobre 2025

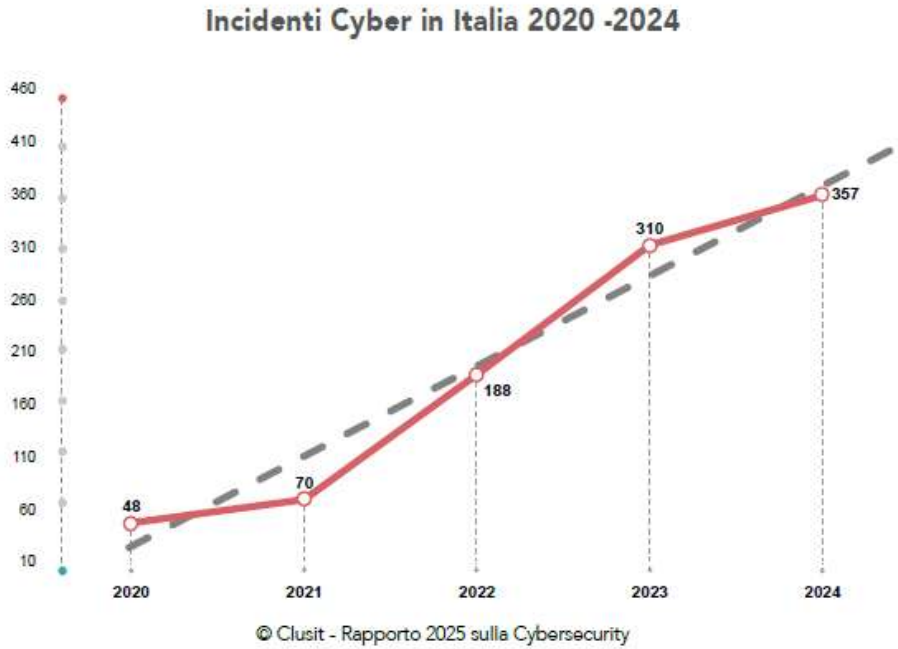
Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

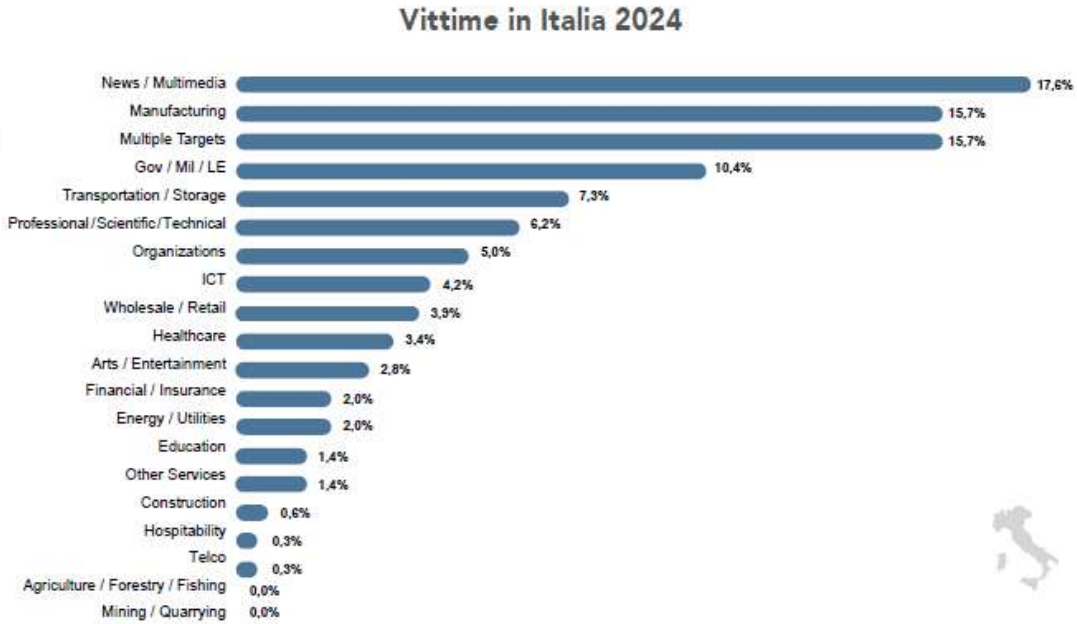
Introduzione

Il panorama delle vulnerabilità

I dati presenti nel «Rapporto Clusit sulla Cybersecurity in Italia e nel mondo 2025» confermano un trend ancora in crescita di attacchi (+39%) subiti in Italia rispetto al 2020.

La categoria merceologia per cui si rileva un maggior numero di attacchi è «News/Multimedia» mentre i settori che guidavano al classifica si trovano nelle posizioni immediatamente successive





Il caso News/Multimedia

Il posizionamento straordinario di *News / Multimedia* nella classifica delle vittime in Italia merita un approfondimento.

Tra gli incidenti pubblicamente noti c'è stato uno **specifico attacco** che ha colpito un ampio insieme di testate giornalistiche, ad opera dello stesso gruppo cybercriminale, che ha sfruttato una **vulnerabilità zero-Day** di un CMS diffusamente utilizzato.

Le fonti riferiscono di 77 vittime colpite (di cui 62 vittime note in Italia, 59 delle quali appartenenti appunto al settore *News / Multimedia*) e del furto dei dati personali di **5 milioni di utenti** (contenenti email, password, date di nascita e altre informazioni).

Sebbene si tratti di un avvenimento anomalo e probabilmente isolato, presenta delle ***lesson learnt*** utili per tutti gli ambiti in cui una tecnologia informatica è utilizzata in modo prevalente e presenta delle criticità di sicurezza. In tali casi può diventare un bersaglio interessante e appetibile per gli attaccanti perché i criminali hanno la certezza di generare con **una sola campagna di attacchi un numero ingente di danni**, fino a poter mettere in crisi un intero settore.

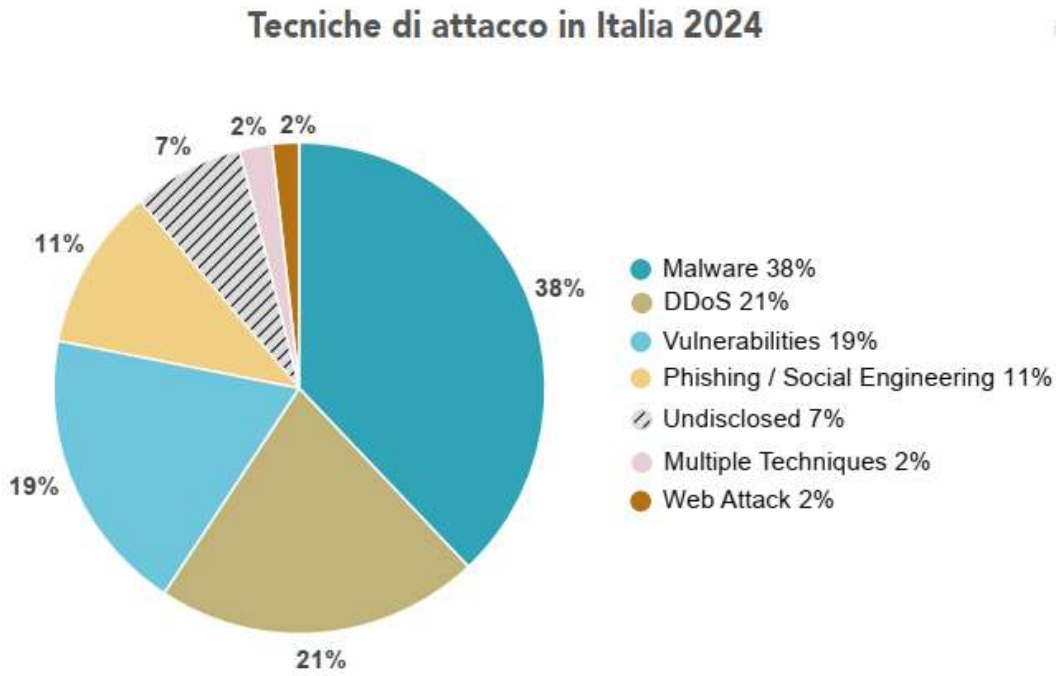
Un altro esempio sono i server Microsoft SharePoint on-premises sotto attacco a luglio a causa della vulnerabilità critica ToolShell (CVE-2025-53770 e CVE-2025-53771), sfruttata attivamente da hacker inclusi gruppi legati alla Cina.

Distribuzione delle tecniche di attacco

Tra le tecniche di attacco nel 2024 il *Malware* torna ad occupare la prima posizione, con il 38% degli incidenti.

I cyber incidenti causati da *DDos* si attestano al 21% , al terzo posto si trovano gli incidenti basati su *vulnerabilità* 19% quota storica per l'Italia.

Questo incremento è certamente giustificato dall'influenza degli incidenti che hanno colpito il settore *News/Multimedia.*



Strategia

Il rapporto Clusit permette di delineare come agire nei punti più critici e funzionali è cruciale per ottenere dei risultati.

Generalmente gli aspetti di sicurezza sono sottovalutati fin dalle prime fasi del ciclo di vita dello sviluppo software e di conseguenza sono molte le vulnerabilità introdotte e trasmesse negli stadi successivi.

È stato stimato, che un errore introdotto nella fase di specifica dei requisiti, può costare fino a 200 volte, se lo si corregge nelle successive fasi di sviluppo.

Anche l'appello della comunità OWASP sottolinea la necessità di accrescere la consapevolezza sulla sicurezza delle applicazioni, poiché il software non sicuro mette a repentaglio le infrastrutture anche più critiche (finanziarie, sanitarie e difensive)

Le Linee Guida AGID forniscono un approccio strutturato per ridurre tali rischi, ripensare la sicurezza è anche un obbligo di legge (Regolamento UE 679/2016).

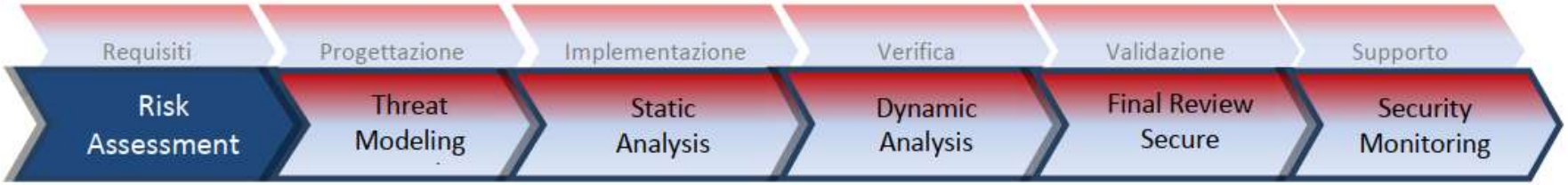
LA SICUREZZA NELLE FASI DEL CICLO DI SVILUPPO DEL SOFTWARE

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Ciclo di Vita dello Sviluppo del Software

SDLC (Software Development Life Cycle) è un processo strutturato per la creazione e la gestione di software, che suddivide il processo di sviluppo in fasi distinte come pianificazione, progettazione, sviluppo, test e distribuzione, con l'obiettivo di produrre software di alta qualità in modo efficiente e nel rispetto del budget e dei tempi.

SSDLC (**Secure Software Development Life Cycle)** è un processo strutturato che integra la sicurezza in ogni fase del ciclo di vita dello sviluppo del software (SDLC). L'obiettivo è sviluppare software più sicuro, identificando e mitigando le potenziali vulnerabilità fin dall'inizio, anziché occuparsene solo nelle fasi finali.



SSDLC

Requisiti: in questa fase sono effettuate analisi dei requisiti di sicurezza, dei rischi, delle probabilità di impatto delle minacce e dei casi di abuso.
Progettazione: in questa fase si esamina il sistema in divenire con l'ausilio di tecniche di analisi e modellazione delle minacce. Requisiti di sicurezza di maggior dettaglio si aggiungono a quelli prodotti nella precedente fase.

Implementazione: in questa fase si realizza il sistema attraverso la stesura di codice sicuro. Seguono esecuzione di test di sicurezza basati sull'analisi delle minacce e analisi statica del codice sorgente. Quest'ultima può produrre nuovi requisiti di sicurezza, che possono portare alla revisione del codice.

Verifica: in questa fase si analizzano gli aspetti di sicurezza del sistema in esecuzione in un ambiente controllato impiegando tecniche e strumenti di analisi dinamica;

Validazione: fase prima del rilascio nella quale è effettuata una final security review per la verifica del rispetto dei requisiti.

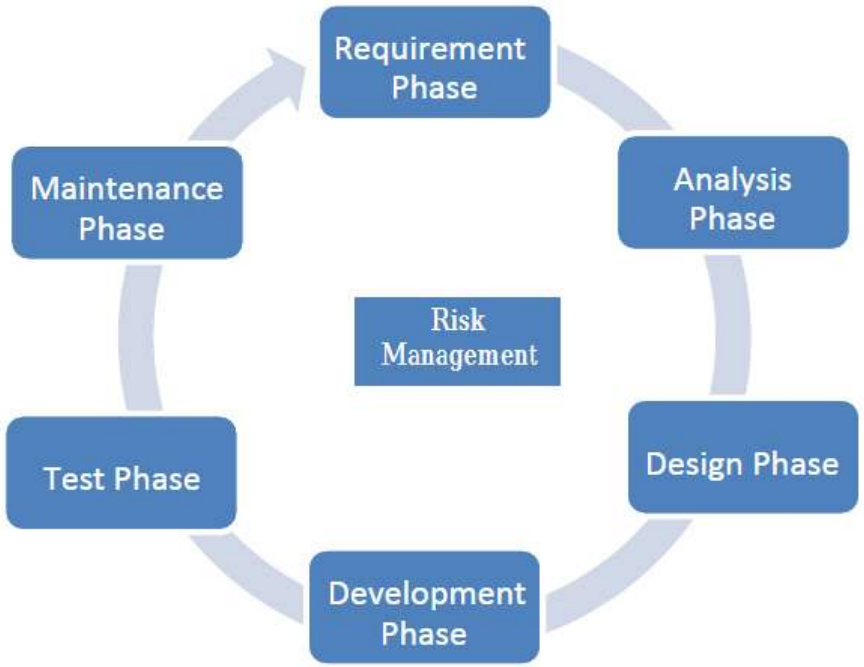
Supporto: in questa fase si esamina il sistema in essere con l'ausilio di tecniche di analisi e modellazione delle minacce e/o verifica statica/dinamica del codice applicativo, al fine di produrre nuovi requisiti di sicurezza di dettaglio per un'eventuale fase di reingegnerizzazione e/o patching del sistema.

Risk Assessment

L’obiettivo dell’analisi del rischio è identificare, valutare e misurare la probabilità e la gravità dei rischi (Risk Assessment) nei diversi processi, e decidere come comportarsi a fronte dei rischi identificati (Risk Management) al fine di minimizzarli o eliminarli.

Il Risk Assessment è uno strumento di analisi, semplice e accurato, che studia i rischi al fine d’individuare le soluzioni e le misure più adeguate

La gestione dei rischi per essere effettivamente efficace, deve essere totalmente integrata nell'SDLC



Requisiti

Attraverso l'analisi dei requisiti sono identificati e definiti gli obiettivi delle specifiche di sicurezza, i metodi necessari per implementarli e l'importanza che questi ricoprono.

I requisiti di sicurezza definiscono i requisiti funzionali e non funzionali che devono essere soddisfatti per ottenere le caratteristiche di sicurezza di un sistema IT.
Possono essere distinti in quattro diverse tipologie:

1. **Requisiti funzionali sicuri**: descrivono i criteri di sicurezza integrati in ciascun requisito funzionale. Tipicamente indicano anche ciò che non deve accadere
2. **Requisiti di sicurezza funzionale**: definiscono i servizi di sicurezza che devono essere implementati nel sistema sottoposto ad analisi. Alcuni esempi sono l'autenticazione, l'autorizzazione, il backup, il server-clustering, ecc.
3. **Requisiti di sicurezza non funzionali**: requisiti architetturali legati alla sicurezza, come "la robustezza" o "le prestazioni minime e la scalabilità". Questa tipologia è tipicamente derivata dai principi architetturali di secure-design.
4. **Requisiti di sviluppo sicuro**: descrivono le attività richieste durante lo sviluppo del sistema al fine di garantire che il sistema stesso nella sua versione finale sia esente da vulnerabilità. Alcuni esempi sono la "classificazione dei dati", le "linee guida di sviluppo sicuro" o la "metodologia di test". Tali requisiti sono derivati da framework metodologici basati su best-practices

Obiettivi di sicurezza

I principali obiettivi di sicurezza sono:

- **Riservatezza e Integrità** Riservatezza significa che le risorse possono essere utilizzate solo dalla parte legittima, integrità significa che devono essere modificabili solo dalle persone autorizzate.
- **Autenticità**
  Non-ripudio Garantisce che qualsiasi azione sul sistema non possa essere in seguito rinnegata.
- **Flusso Informativo** Il livello di sicurezza può avere regole diverse. Laddove componenti di sistema considerati di alto livello interagiscono con parti meno attendibili, si deve garantire che non vi sia alcuno scambio di dati dall'alto verso il basso
- **Controllo Accessi** Solo un utente fidato può avere accesso a un sistema sicuro.

  Il **Role-Based Access Control (RBAC)** i privilegi di accesso alle risorse dipendono dal ruolo che assumono nel tempo gli individui, l'assegnazione dei ruoli è centralizzata. **ABAC** (Attribute Based Access Control) fornisce i diritti di accesso in base agli attributi dell'utente. Gli attributi sono insiemi di etichette o proprietà che possono essere utilizzati per descrivere tutte le entità che devono essere considerate ai fini dell'autorizzazione.

Definizione dei requisiti di sicurezza

Le principali azioni di sicurezza da attuare:

- **Definizione degli elementi di sicurezza applicativa**, finalizzata alla valutazione dei requisiti:
  - Integrità,
  - Autenticità,
  - Riservatezza,
  - Disponibilità,
  - Non-ripudio,
  - Autorizzazione.
- **Definizione dei requisiti di privacy**, attraverso la raccolta strutturata delle informazioni:
  - Dati personali,
  - Servizi di terze parti,
  - Policy.
- **Risk assessment**, finalizzato alla valutazione del rischio.

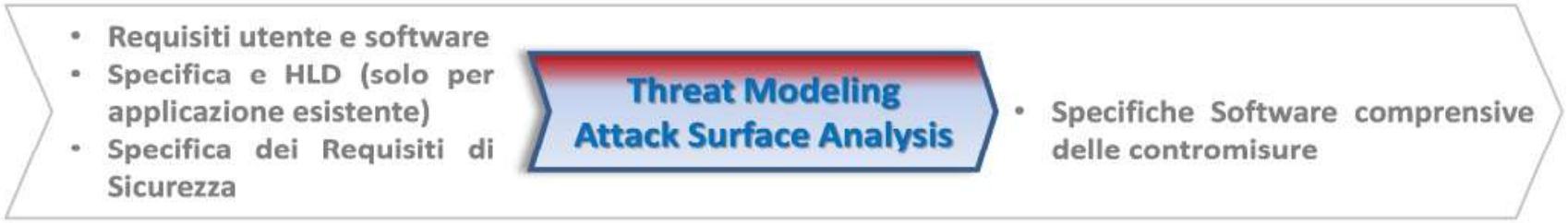
  Durante questo processo è utile classificare i vari rischi utilizzando diversi framework di sicurezza quali: OWASP Top 10, SANS CWE Top 25 o OWASP ASVS.

Progettazione

Le azioni di sicurezza di questa fase possono essere così sintetizzate:

- **Analisi e modellazione delle minacce**, attraverso l'identificazione dei componenti applicativi coinvolti, delle interfacce e degli agenti che potrebbero minacciare il sistema;
- **Analisi della superficie d'attacco e della finestra di opportunità**, individuazione delle parti del sistema che possono essere esposte ad attacchi rendendolo vulnerabile;
- **Piano di mitigation**, identificazione delle contromisure da adottare al fine di mitigare le potenziali minacce individuate
- **Secure Design Refactoring,** revisione progettuale che attua le contromisure individuate; produzione di un High Level Design conforme ai principi del Secure by Design;

Questa fase produce come output finale la Reportistica/documentazione completa che sintetizza i risultati per ogni punto precedente (Specifiche Software comprensive delle contromisure).



Implementazione

Le azioni di sicurezza che devono essere intraprese in questa fase sono:

- **Data Validation:** verificare la presenza di vulnerabilità che possono riguardare dati corrotti in ingresso che possono creare un comportamento anomalo dell'applicazione;
- **Control Flow**: verificare i rischi collegati all'assenza di specifiche sequenze di operazioni che, se non eseguite nel corretto ordine, possono portare a violazioni sulla memoria o sull'uso scorretto di determinati componenti;
- **Analisi Semantica**: rilevare eventuali problematiche legate all'uso pericoloso di determinate funzioni o API (es. funzioni deprecate);
- **Controllo Configurazioni**: verificare i parametri intrinseci di configurazione dell'applicazione;
- **Buffer Validation**: verificare la presenza di buffer overflow sfruttabile attraverso la scrittura o la lettura di un numero di dati superiore alla reale capacità del buffer stesso.

L'esame del codice sorgente deve generare:

- **Report delle Vulnerabilità riscontrate**: dettaglio delle vulnerabilità riscontrate nella fase di analisi statica del codice
- **Remediation Plan**: analisi dei falsi positivi per la risoluzione delle problematiche riscontrate nell'analisi stessa.

Verifica

Le azioni di sicurezza da intraprendere in questa fase:

- **Analisi dinamica**: Attuazione di test dinamici di sicurezza sull'applicazione in esecuzione in ambiente controllato;
- **Penetration Test**: esecuzione di scansioni ed analisi della superficie di attacco;
- **Test di autenticazione multilivello**: verifica delle modalità di gestione dell'accesso degli utenti;
- **Business Logic test**: esecuzione di test manuali sulle applicazioni in fase di esecuzione;
- **Analisi dei risultati**: individuazione e rimozione dei falsi positivi;
- **Remediation Plan**: definizione del piano di rientro e produzione di reportistica di sintesi e di dettaglio;

L'esame delle Applicazioni in esecuzione in ambiente di test deve produrre:

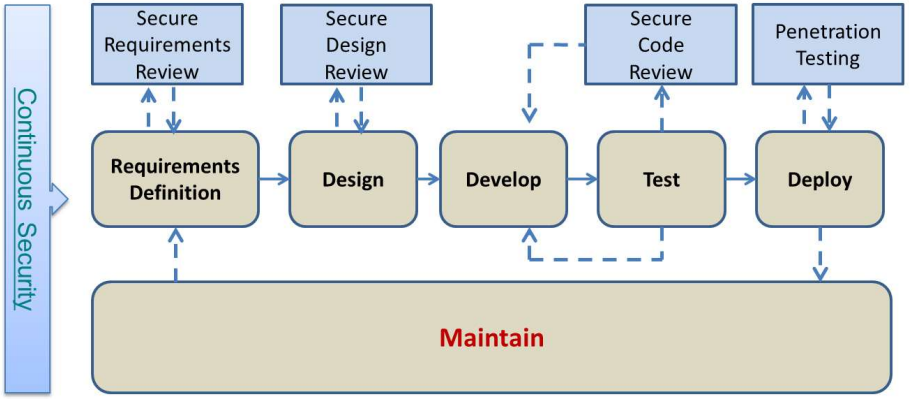
- **Vulnerability Assessment:** report di dettaglio delle vulnerabilità riscontrate nella fase di analisi dinamica;
- **Remediation Plan:** report che analizza i falsi positivi ed indirizza la risoluzione delle problematiche riscontrate.

Supporto per la manutenzione

L’obiettivo di questa fase è mantenere un prodotto sicuro, a partire dai nuovi trend sugli attacchi/minacce.

Il team deve analizzare le nuove minacce e individuare le contromisure necessarie rilasciando nuovi aggiornamenti/patch laddove necessario attraverso un processo di «Continuous Security».

Qualsiasi modifica a un sistema ha il potenziale per ridurre l'efficacia dei controlli esistenti o avere un impatto sulla riservatezza, sulla disponibilità o sull'integrità dello stesso.
La soluzione è garantire che nella valutazione delle modifiche del sistema sia inclusa una fase di valutazione del rischio.
Quando sono identificate nuove minacce, potrebbero essere necessari nuovi controlli per portare il rischio a un livello accettabile.
Le valutazioni periodiche del rischio sono importanti, anche quando un sistema cambia raramente.



La privacy nel SDLC

Principi della privacy

All'interno dalla ISO/IEC 29100:2011 sono descritti undici principi che indirizzano la progettazione, lo sviluppo e l'implementazione dei requisiti di protezione della privacy. Questi principi, sono anche un riferimento, il monitoraggio e la misurazione delle prestazioni del software e il controllo dei programmi di gestione della privacy in un'organizzazione.

Principi	Descrizione
Consenso e scelta	L'interessato deve poter scegliere se acconsentire o meno al trattamento dei propri dati personali
Scopo legittimo e specifico	Assicura che lo scopo sia conforme alla legge applicabile e si basi su una base giuridica ammissibile.
Limitazione della raccolta	Limita la raccolta dei dati personali a ciò che è strettamente necessario per gli scopi specificati
Minimizzazione Dati	Prevede la progettazione, l'implementazione e l'elaborazione dei dati, attraverso procedure o sistemi ICT, per ridurre al minimo i dati personali che vengono elaborati
Limitazione dell'utilizzo conservazione e divulgazione	Limita l'utilizzo, la conservazione e la divulgazione (incluso il trasferimento) dei dati personali a scopi specifici, espliciti e legittimi del trattamento.
Precisione e qualità	I dati personali elaborati devono essere accurati, completi, aggiornati, adeguati e pertinenti ai fini del trattamento.
Apertura, trasparenza e preavviso	Devono essere fornite informazioni chiare e accessibili sulle politiche stabilite dal titolare del trattamento e sulle procedure relative al trattamento dei dati personali
Partecipazione individuale e accesso	Gli interessati devono avere la possibilità di accedere e di rivedere i propri dati personali, a condizione che la loro identità sia autenticata con un livello adeguato di garanzia
Responsabilizzazione	Stabilisce che siano documentate e comunicate in modo appropriato tutte le politiche, le procedure e le pratiche relative alla privacy.
Sicurezza delle informazioni	Stabilisce la protezione dei dati personali con controlli appropriati a livello operativo, funzionale e strategico
Conformità alla privacy	Stabilisce di verificare e dimostrare che il trattamento rispetti la protezione dei dati e la tutela della privacy

Obblighi definiti GDPR

Principi	Descrizione
Limitazione nella raccolta	Il titolare del trattamento deve ottenere il consenso preventivo e inequivocabile da parte dell'interessato o informare l'interessato della raccolta di suoi dati personali e delle finalità di utilizzo. Il titolare del trattamento non deve acquisire dati personali con mezzi fraudolenti o altri mezzi illeciti. I titolari del trattamento dei dati dovrebbero raccogliere i dati senza il consenso, se autorizzati da un'ordinanza giudiziaria nazionale o da uno strumento giuridico equipollente. Il responsabile del trattamento dei dati dovrebbe adottare le opportune misure per evitare di raccogliere dati dai quali una persona potrebbe essere identificata facendo riferimento ad una banca dati. Il titolare del trattamento dei dati deve adottare misure adeguate per ottenere la conferma sul consenso da parte dell'interessato alla raccolta dei propri dati.
Qualità dei dati raccolti	Il titolare del trattamento dei dati personali deve adoperarsi nel mantenere i dati personali esatti e aggiornati entro i limiti necessari per il raggiungimento degli scopi dell'utilizzo.
Specifica dello scopo d'uso	Il titolare del trattamento deve specificare le finalità dell'utilizzo dei dati personali, non deve modificare le finalità d'uso al di fuori dell'ambito in cui le nuove finalità possono ragionevolmente essere considerate compatibili con quelle d'origine, la modifica delle finalità d'uso richiede il consenso preventivo.
Limitazione nell'uso dei dati	Un responsabile del trattamento dei dati personali non deve trattare i dati personali, senza ottenere il consenso preventivo da parte dell'interessato; non deve fornire dati personali a terzi senza ottenere il consenso preventivo da parte dell'interessato; le disposizioni delle due specifiche precedenti non si applicano nei casi in cui il trattamento dei dati personali si basa su leggi nazionali vigenti.
Misure di sicurezza	I dati personali devono essere protetti da adeguate misure di sicurezza contro rischi quali la perdita o l'accesso non autorizzato, la distruzione, l'uso, la modifica o la divulgazione dei dati
Apertura	Dovrebbe esistere una politica generale di apertura nei riguardi di sviluppi, pratiche e politiche in materia di dati personali. Dovrebbero essere prontamente disponibili mezzi per stabilire l'esistenza e la natura dei dati personali e le principali finalità del loro utilizzo, nonché l'identità e la residenza abituale della persona che raccoglie i dati.
Partecipazione individuale	Un individuo può avere il diritto a ottenere dal titolare del trattamento la conferma dell'esistenza o meno di dati che lo riguardano;
Responsabilizzazione	Il titolare del trattamento dei dati deve essere responsabile del rispetto delle misure che attuano i principi di cui sopra e di garantire che i responsabili del trattamento dei dati allo stesso modo si conformino.
Equivalenza di regime	Il titolare del trattamento dei dati non dovrebbe trasferire dati personali al di fuori delle proprie frontiere, a meno che la destinazione non abbia un regime di privacy equivalente a quello di origine

Obiettivi di protezione

Gli obiettivi di protezione mirano a fornire delle proprietà indipendenti dal contesto per i sistemi IT.

Nella sicurezza ICT la triade della riservatezza, dell'integrità e della disponibilità è stata ampiamente accettata, a completamento di questi obiettivi di protezione della sicurezza, sono stati proposti tre obiettivi di protezione specifici per la privacy.

Principi	Descrizione
Incollegabilità	Garantisce che i dati rilevanti per la privacy non possano essere collegati tra domini con scopo e contesto comuni. Ciò significa che i processi devono essere gestiti in modo tale che i dati rilevanti per la privacy non siano collegabili a qualsiasi altro insieme di dati rilevanti sulla privacy al di fuori del dominio.
Trasparenza	Garantisce che tutte le elaborazioni dei dati rilevanti per la privacy, comprese le impostazioni legali, tecniche e organizzative, possano essere comprese e ricostruite in qualsiasi momento. La trasparenza deve riguardare non solo l'elaborazione effettiva, ma anche l'elaborazione pianificata
Intervenibilità	Garantisce l'intervento in relazione a tutti i trattamenti di dati relativi alla privacy in corso o pianificati, in particolare da parte di coloro i cui dati vengono elaborati. L'obiettivo è l'applicazione di misure correttive e controbilanci ove necessario. L'intervenibilità è legata ai principi relativi ai diritti degli individui, ad es. i diritti di rettifica e cancellazione dei dati, il diritto di revocare il consenso o il diritto di presentare un reclamo o di sollevare una controversia per ottenere il rimedio.

Privacy by design

La Privacy by Design (PbD) può essere definita come “un approccio olistico concettuale che può essere applicato - end-to-end - all’interno di un’organizzazione, includendo le sue tecnologie informatiche, le sue pratiche commerciali, i suoi processi, la progettazione fisica e le infrastrutture di rete”.

L'utente dovrebbe essere considerato il centro di un sistema di protezione dei dati personali ("user centric").

Qualsiasi progetto - sia strutturale, sia concettuale - andrebbe realizzato considerando, sin dalla fase di progettazione, la riservatezza e la protezione dei dati personali.

La PbD comprende la seguente trilogia di applicazioni:

- Sistemi IT
- Pratiche di business
- Progettazione delle reti

In questo contesto si inserisce la necessità di prevedere l’ingegnerizzazione della privacy by design in ogni fase del ciclo di vita del software.

I sette principi della privacy by design

Proattivo non reattivo; Preventivo non correttivo	L'approccio di *Privacy by Design* (PbD) è caratterizzato da misure proattive piuttosto che reattive. Essa è diretta ad anticipare e previene gli eventi invasivi della privacy prima che accadano. PbD non attende che i rischi per la privacy si materializzino, né offre rimedi per la risoluzione delle infrazioni della privacy una volta che si sono verificati, in quanto è diretta ad impedire che si verifichino
Privacy come impostazione predefinita	La *Privacy by Design* è diretta a garantire il massimo grado di privacy prevedendo che i dati personali siano automaticamente protetti in qualsiasi sistema IT o di business. Nessuna azione è richiesta da parte dei singoli per proteggere la loro privacy, in quanto è integrata nei sistemi per impostazione predefinita.
Privacy incorporata nel design	La Privacy by Design è incorporato nel design e nell'architettura dei sistemi IT e di business. Non è attuata successivamente ad un evento. Il risultato è che la privacy diventa una componente essenziale delle funzionalità principali. La privacy è parte integrante del sistema, senza diminuirne la funzionalità.
Funzionalità completa; somma positiva, non somma zero	La *Privacy by Design* cerca di tutelare tutti i legittimi interessi e gli obiettivi in un'ottica *win-win*, senza prevedere delle soluzioni a somma zero che includano degli inutili trade-off
Sicurezza end-to-end - Protezione completa del ciclo di vita	La *Privacy by Design* che è stata incorporata in un sistema sin dal primo momento, si estende in modo sicuro durante l'intero ciclo di vita dei dati coinvolti: prevedendo robuste misure di sicurezza - essenziali per la privacy - dall'inizio alla fine di un ciclo di vita. Ciò garantisce che tutti i dati vengano conservati e distrutti – in modo sicuro e tempestivamente - alla fine del processo. Pertanto, la *Privacy by Design* garantisce una gestione delle informazioni sicura end-to-end.
Visibilità e trasparenza - Keep it Open	La *Privacy by Design* cerca di assicurare a tutti gli stakeholder che qualunque sia la pratica aziendale o la tecnologia coinvolta, essa opererà secondo le promesse e gli obiettivi dichiarati,
Rispetto per la privacy degli utenti - Mantenerlo incentrato sull'utente	La *Privacy by Design* richiede ai progettisti e agli operatori di garantire gli interessi dei singoli, offrendo robuste misure di privacy per impostazione predefinita.

Data protection Impact Assessment

La progettazione di qualsiasi software che coinvolga il trattamento dei dati personali deve essere preceduta da un'identificazione dei requisiti di protezione per la privacy, dal trattamento dei dati personali, analisi dei rischi.

I rischi per la privacy negli applicativi software dovrebbero essere trattati prima della loro implementazione sin dalla fase di progettazione (*Engineering Privacy by Design*).

In linea con il **GDPR**, qualora un trattamento dei dati personali possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, i titolari di quest'ultimo dovranno effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali o *Data Protection Impact Assessment*, «DPIA» quest'obbligo è applicabile anche al ciclo di vita del software.

Ciclo di vita dello sviluppo software nell'ambito del GDPR

Il GDPR ha un impatto profondo e significativo sul ciclo di vita dello sviluppo del software e sui relativi processi di sviluppo informatico per quelle organizzazioni che prevedono la realizzazione di progetti relativi a sistemi informativi all'interno dell'UE.

Può essere utilizzato uno dei molteplici e distinti tipi di SDLC, come Agile, DevOps, Waterfall, Iterative, ecc, ma tutti coprono l'intero ciclo di vita di un sistema informativo.

Nella maggior parte delle tecnologie impiegate, si trovano in comune i seguenti moduli:

- livelli di trasporto dati e sicurezza;
- livelli di database e architettura dei dati;
- livelli applicativi e logici;
- livelli di presentazione e portale.

Il GDPR ha impatto nel SDLC per le imprese che installano sistemi nell'UE e aumenta la complessità dei progetti funzionali e tecnici associati ai vari livelli tecnici indicati, le influenze da parte del GDPR devono essere affrontate nella fase di pianificazione dell'SDLC, per evitare sovraccosti significativi e rielaborazioni successive nel processo informatico.

L'impatto del GDPR sullo sviluppo del software inizia dall'architettura dei dati e dai livelli di trasporto di questi, per arrivare fino ai livelli di portale e di presentazione. La chiave di base per il successo dello sviluppo IT è la pianificazione di tali requisiti durante le fasi iniziali; sebbene possano aggiungere una certa complessità alle fasi iniziali i costi di sviluppo complessivi saranno notevolmente ridotti al minimo se considerati il più precocemente possibile nel processo di costruzione dei sistemi IT.

Privacy Implementation Strategy

Gli elementi definiti all'interno della Privacy Implementation Strategy, i requisiti di protezione della privacy e le strategie di design per la privacy, dovranno essere inquadrati all'interno di ciascuna fase della Engineering privacy by design e rimappati per ciascuna fase del ciclo di vita dei software.

Le attività da svolgere secondo il *Privacy Engineering Framework* del MITRE sono:

Definizione dei requisiti privacy

Input: Requisiti di privacy di base e test; Normative, best practice e procedure applicabili sulla privacy; requisiti funzionali; Profili di rischio per la privacy.

Attività: Data Protection Impact Assessment sugli obiettivi di protezione individuati; Selezionare e perfezionare i requisiti di protezione per la privacy di base e effettuare dei test; Sviluppare dei requisiti di protezione della privacy personalizzati e testarli sulla base dei risultati della DPIA.

Output: Requisiti di protezione per la privacy specifici per il software.

Design e sviluppo privacy

Input: Requisiti Architetturali e funzionali specifici per la privacy

Attività: Identificare strategie e modelli di design della privacy; Identificare controlli di privacy, criteri tecnici e policy; Sviluppare dati e modelli di processo che riflettano i controlli di privacy identificati; Allineare, integrare e implementare i controlli di privacy con gli elementi funzionali; Analizzare il rischio del design di privacy

Output: Componenti del software implementati; Mitigazione dei rischi accettabili per la privacy residua

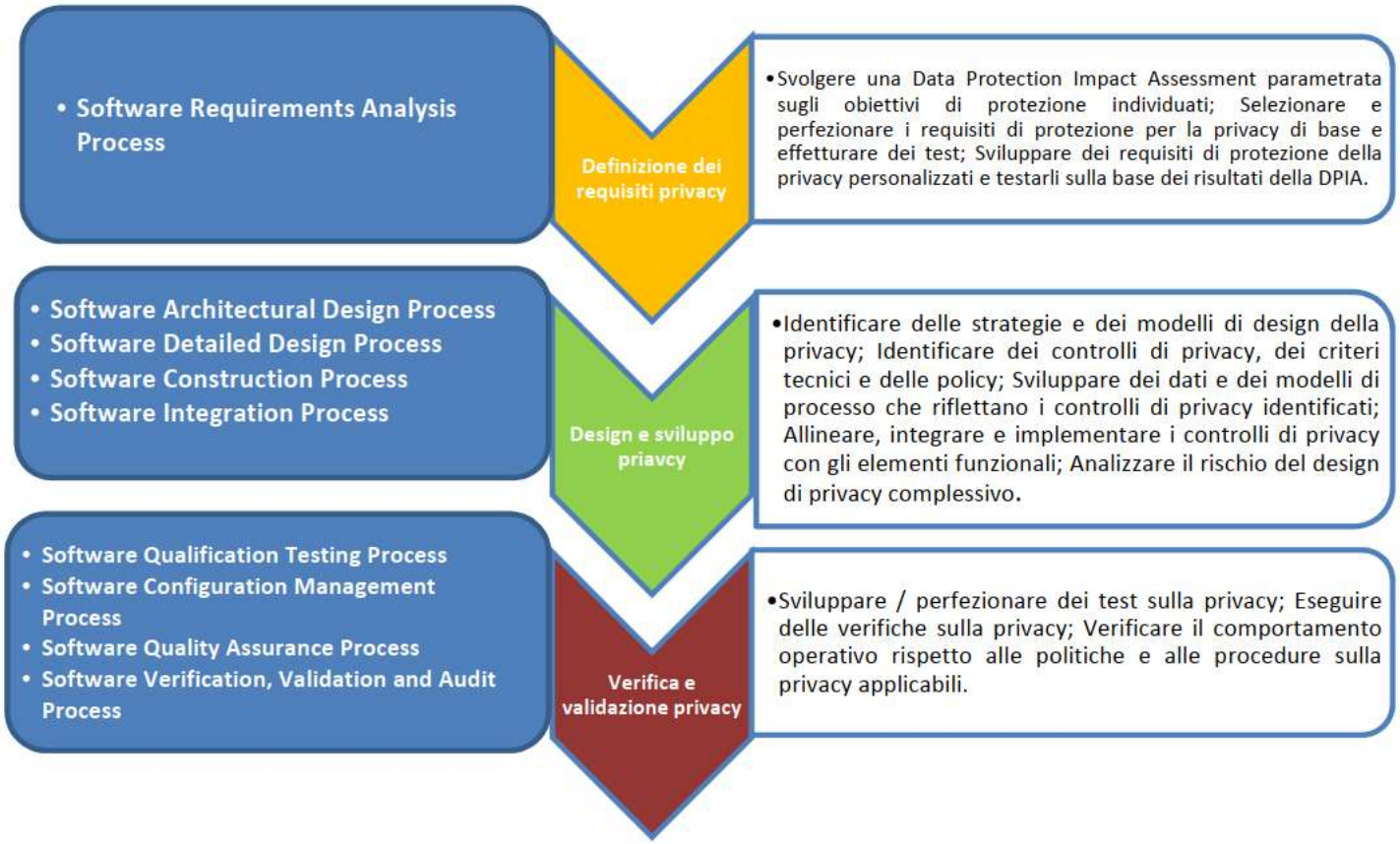
Verifica e validazione privacy

Input: Componenti del software implementati; Requisiti di privacy specifici del sistema e test; Politiche e procedure di privacy applicabili.

Attività: Sviluppare/perfezionare i test sulla privacy; Eseguire delle verifiche sulla privacy; Verificare il comportamento operativo rispetto alle politiche e alle procedure sulla privacy applicabili.

Output: Risultati dei test di privacy; Documentazione delle Incoerenze sulla privacy documentate; Descrizione del piano di trattamento della privacy.

Integrazione della Engineering Privacy by Design nel Software Life Cycle Process



Conclusioni

L'adozione di un approccio olistico alla privacy e alla sicurezza non è più un'opzione, ma una necessità critica. L'integrazione di un Ciclo di Sviluppo del Software Sicuro (SSDLC) garantisce che la sicurezza sia incorporata fin dalla progettazione, non aggiunta come un ripensamento. Questo approccio proattivo è fondamentale per proteggere i dati e costruire la fiducia degli utenti.

Il Privacy Engineering Framework e il principio di Privacy by Default sono i pilastri che supportano questa visione. Implementando questi principi, i team di sviluppo possono creare prodotti e servizi che rispettano la privacy degli utenti in modo intrinseco, riducendo i rischi e garantendo la conformità normativa.

In un'era in cui i dati sono la risorsa più preziosa, rendere la privacy una priorità etica e tecnica non solo protegge gli utenti, ma rafforza anche la reputazione e il valore a lungo termine di un'organizzazione.

Grazie per il vostro tempo