Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

LINEE GUIDA DI SICUREZZA NELLO SVILUPPO DELLE APPLICAZIONI

Redatto da	Pietro Marchionni
Rivisto da	Giovanni Caporale
Autorizzato da	Francesco Tortorelli
Versione	1.0

Dati di controllo del documento

Data di emissione	21 Novembre 2017
N. pagine	
Sommario delle versioni	*Versione* / *Data*: 1.0 / 21/11/2017
Modifiche rispetto alla versione precedente	N/A
Lista(e) di distribuzione	Pubblico

Sommario

1 INTRODUZIONE

1.1 COMPENDIO

Il documento contiene le linee guida per lo sviluppo del software sicuro nella pubblica amministrazione.

Le linee guida sono suddivise nelle seguenti tematiche:

1. Linee Guida per l'adozione di un ciclo di sviluppo di software sicuro;
2. Linee Guida per lo sviluppo sicuro di codice;
3. Linee Guida per la configurazione per adeguare la sicurezza del software di base;
4. Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design;

1.2 SCOPO

La sicurezza ha un'importanza fondamentale in quanto è necessaria per garantire la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica amministrazione. Essa è inoltre direttamente collegata ai principi di privacy previsti dall'ordinamento giuridico.

Le linee guida per la sicurezza ICT delle Pubbliche amministrazioni hanno lo scopo di fornire indicazioni sulle misure da adottare in ciascuna componente della Mappa del Modello strategico.

In particolare l'obiettivo è di definire un'architettura della sicurezza per servizi sia critici che non critici che definisca i principi e le linee guida del modello architetturale di gestione dei servizi e contestualizzazione rispetto al cluster dei dati gestiti.

Nel dettaglio, per ciascuna tematica:

1. Scopo delle linee guida per l'adozione di un ciclo di sviluppo di software sicuro è fornire le best practices per intraprendere un processo di sviluppo del software "sicuro", applicabile attraverso l'identificazione e l'implementazione di opportune azioni di sicurezza nel corso di tutte le fasi del ciclo di sviluppo software.
2. La sicurezza del software di base ed applicativo richiede di stabilire un processo volto ad identificare rischi e contromisure di sicurezza ad ogni livello (fisico, logico e organizzativo) del contesto in cui tali software operano e sono utilizzati. Pertanto, nel fornire delle linee guida per la configurazione sicura di tali software (nel seguito tale attività viene spesso indicata con il termine "hardening"), è necessario considerare vari elementi, quali le protezioni perimetrali (fisiche e logiche), le architetture di rete (DMZ, segmentazioni, etc.), le procedure organizzative (perché dietro alle tecnologie operano le persone), i programmi formativi di "security awareness", ecc. Partendo da questo presupposto, le linee guida per la configurazione per adeguare la sicurezza del software di base si pongono l'obiettivo

di fornire un insieme di indicazioni per affrontare e risolvere correttamente le problematiche legate alla sicurezza del software di base e di individuare le misure da adottare per difendere ogni componente da possibili minacce accidentali e/o intenzionali.

3. Scopo delle linee guida per lo sviluppo sicuro di codice è supportare lo sviluppo di applicazioni informatiche sicure. Queste linee guida, costituiscono un insieme di best practices da seguire al fine prevenire eventuali problematiche di sicurezza nel codice e forniscono nel contempo uno strumento utile nell'individuazione di possibili vulnerabilità presenti nel codice sorgente e le relative contromisure da applicare
4. Gli obiettivi degli attacchi sono spesso vulnerabilità che si celano all'interno delle applicazioni software. La comunità OWASP (www.owasp.org) sottolinea la necessità di accrescere la consapevolezza sulla sicurezza delle applicazioni in quanto il software non sicuro mette a repentaglio le infrastrutture finanziarie, sanitarie, difensive, etc. Le linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design vogliono analizzare il contesto (processi, metodi e modelli) della Progettazione di Applicazioni Sicure con l'obiettivo di fornire best practices per la modellazione delle minacce e conseguente individuazione di azioni di mitigazione, in conformità con i principi "Secure/privacy by Design". Ciò costituisce una fase importante nel processo di individuazione preventiva dei requisiti di sicurezza e privacy.

1.3 AREA DI APPLICAZIONE

Il presente documento si applica alla Pubblica Amministrazione.

Queste best practice si inseriscono nell'ambito delle attività previste nel Piano Triennale per l'Informatica nella PA.

1.4 ACRONIMI, ABBREVIAZIONI E GLOSSARIO

Per questa sezione si faccia riferimento alle analoghe sezioni dei documenti delle linee guida indicate nel paragrafo 1.1.

2 RIFERIMENTI NORMATIVI, GRUPPO DI LAVORO, ED ELENCO DEGLI ALLEGATI

2.1 PREMESSE GENERALI

Il Piano Triennale per l'Informatica nella PA riporta il "Modello strategico di evoluzione del sistema informatico nella PA".

Il Piano triennale è costruito sulla base di un Modello strategico di evoluzione del sistema informativo della Pubblica amministrazione e indirizza il piano delle gare, il piano dei finanziamenti e i piani triennali delle singole PA.

Il Piano propone un modello sistemico, diffuso e condiviso, di gestione e di utilizzo delle tecnologie digitali più innovative, improntato a uno stile di management agile ed evolutivo, e basato su una chiara governance dei diversi livelli della Pubblica amministrazione.

La sinergia e l'equilibrio tra le tre direttrici (tecnologie innovative, stile di management agile e modello di governance chiaro ed efficace) garantiscono al sistema Paese un più efficace sfruttamento dei benefici delle nuove tecnologie e assicurano ai cittadini un vantaggio in termini di semplicità di accesso e miglioramento dei servizi digitali esistenti.

2.2 RIFERIMENTI NORMATIVI

- Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico – Presidenza del Consiglio dei Ministri – Dicembre 2013
- PIANO NAZIONALE PER LA PROTEZIONE CIBERNETICA E LA SICUREZZA INFORMATICA Presidenza del Consiglio dei Ministri – Marzo 2017
- Direttiva 1° agosto 2015 – Presidente del Consiglio dei ministri – Agosto 2015

2.3 ALLEGATI

1. Linee guida per l'adozione di un ciclo di sviluppo di software sicuro
2. Linee Guida per lo sviluppo sicuro di codice
3. Linee Guida per la configurazione per adeguare la sicurezza del software di base
4. Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design

3 CONTENUTI TECNICI

3.1 AMBITO

L'evoluzione degli attacchi informatici sta comportando lo spostamento degli obiettivi verso attacchi diretti alle applicazioni.

I fattori chiave di questa evoluzione sono i progressi fatti dagli attaccanti, il rilascio di nuove tecnologie, l'uso di sistemi sempre più complessi.

Gli obiettivi degli attacchi sono le vulnerabilità che si celano all'interno delle applicazioni software che forniscono un facile percorso d'ingresso per compromettere i sistemi o lanciare ulteriori attacchi e malware. Tra le cause c'è anche il fatto che fino ad ora si è seguito un approccio concentrato soprattutto sulla correzione delle difettosità funzionali e sulle performance delle logiche applicative, trascurando l'attuazione di pratiche di progettazione e programmazione che garantiscono la sicurezza del codice.

Da qui anche l'appello della comunità OWASP che sottolinea la necessità di accrescere la consapevolezza sulla sicurezza delle applicazioni in quanto il SW non sicuro mette a repentaglio le infrastrutture anche più critiche (finanziarie, sanitarie e difensive).

Per rispondere in modo efficace alle sfide di sicurezza delle applicazioni, è necessario dotarsi di soluzioni adeguate per:

- Migliorare la gestione del programma di sicurezza delle applicazioni. Le componenti chiave di un programma di sicurezza devono includere:
  - Risk Management Integration;
  - Architect & Developer Guidance;
  - Process Improvement (SDLC);
  - Secure Development Activities;
  - Vulnerability Management Integration;
- Valutare il codice software e le applicazioni al fine di identificare le vulnerabilità;
- Automatizzare la correlazione dei risultati della verifica della sicurezza per applicazioni interattive, statiche e dinamiche.

A tale scopo sono quindi state individuate aree chiave su cui concentrare gli sforzi difensivi, tra cui l'area dello sviluppo di software sicuro, che viene dettagliata nelle best practice allegate a questo documento.

3.2 IMPATTI TECNICI E ORGANIZZATIVI PER L'APPLICAZIONE DELLE LG

Le linee guida danno indicazioni alle PAC e PAL su come strutturare lo sviluppo di applicazioni e su come organizzare gli ambienti operativi che le ospitano.

Gli impatti sono quindi di carattere:

1. Organizzativo: le PA devono avere al loro interno una struttura tecnica che possa guidare e monitorare gli sviluppi dei servizi erogati secondo le linee guida proposte. Tale struttura dovrà inoltre garantire il continuo aggiornamento dei servizi in base all'evoluzione degli attacchi informatici.
2. Operativo: le PA devono avere internamente od esternamente infrastrutture tecniche che possano gestire operativamente i servizi garantendone l'integrità e la sicurezza
3. Funzionale: la PA deve avere una struttura funzionale che possa gestire le aree operative e di sviluppo concertandone le attività e garantendo la loro piena operatività.

3.3 SPECIFICHE TECNICHE

Le specifiche tecniche sono dettagliate all'interno degli allegati indicati nella sezione 2.3

3.4 STRATEGIA DI APPLICAZIONE

Le best practice in oggetto possono essere utilmente impiegate come riferimenti per la produzione di profili di protezione che permettano, in fase di acquisizione di applicazioni, di indicare le caratteristiche funzionali ritenute necessarie - in relazione al contesto applicativo o al contesto di utilizzo - o per indicare, in caso di affidamento di attività di gestione software esternalizzate, i requisiti tecnici ed i controlli da prevedere in funzione dei livelli di sicurezza richiesti propedeutici alla messa in esercizio del software.

L'Amministrazione, infatti, fornirà regole precise per l'accettazione dei sistemi e delle applicazioni rilasciate dai fornitori o sviluppate internamente. Nello specifico dovranno essere evidenziati gli obblighi relativi alle fasi di design, coding e maintanance del Software (Development Life Cycle) e la tipologia di controlli/attività effettuati dall'Amministrazione durante l'intera fase di progetto.
Il Fornitore di software – o il team interno di sviluppo sarà quindi tenuto ad indirizzare in maniera adeguata la sicurezza del software prodotto secondo i principali standard di settore (dettagliati negli allegati) per lo sviluppo sicuro, adottando le best practice, risolvendo eventuali vulnerabilità ed aderendo ai termini contenuti nei contratti stipulati, garantendo il rispetto degli stessi per il personale coinvolto ed eventuali sub-contractors. Il Fornitore di Software dovrà inoltre garantire l'adeguata protezione delle informazioni relative

alle problematiche di sicurezza note ed alla loro relativa documentazione, assicurando che durante tutto il processo di sviluppo dell'applicazione, il codice sorgente sarà oggetto di continue revisioni di sicurezza volte ad eliminare le vulnerabilità presenti, indicando gli standard, le policy, e le best pratice adottate.
Le figure interne all'Amministrazione interessate alle presenti best practice sono le seguenti:

- **Responsabile della transizione al digitale**. La transizione al digitale consisterà anche nella digitalizzazione dei procedimenti interni associata all'introduzione di best practice nello sviluppo di procedure software.
- **Responsabile dei Sistemi Informativi**
- **Responsabile del Procedimento dei bandi di gara** o in generale delle procedure di affidamento aventi come oggetto la fornitura di software applicativo. All'interno delle possibili procedure di gara, il RUP deve esigere dal fornitore della singola applicazione software l'adozione di standard specifici per rilasciare "software sicuro".

4. MONITORAGGIO DELL'APPLICAZIONE DELLE LG

3.5 MONITORAGGIO DELL'APPLICAZIONE DELLE LG

AgID monitorerà l'applicazione delle linee guida con un questionario annuale dove verranno richieste informazioni sugli strumenti adottati e sui risultati conseguiti.

5. RESPONSABILITA'

La responsabilità all'interno della struttura organizzativa di AgID è dell'area CERT-PA.

ALLEGATI TECNICI – APPENDICI

ALLEGATO A. Linee guida per l'adozione di un ciclo di sviluppo di software sicuro

ALLEGATO B. Linee Guida per lo sviluppo sicuro di codice

ALLEGATO C. Linee Guida per la configurazione per adeguare la sicurezza del software di base

ALLEGATO D. Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design