REGOLAMENTO DEL PROCESSO DI Vulnerability Management

Emesso il 27/09/2022

Owner del Regolamento: IT Operation Security & Governance

Indice

1 PREMESSA

Flowe S.p.A Società Benefit (di seguito anche Flowe o la Società) utilizza vari assets informativi come applicazioni, sistemi ed infrastrutture per esercitare le proprie funzioni aziendali. Tali assets sono collegati a reti affidabili e non affidabili per elaborare, scambiare e archiviare informazioni. Pertanto, essi dovranno essere protetti contro il possibile sfruttamento esterno ed interno delle relative vulnerabilità e nell'ambito della protezione di tali risorse sarà necessario effettuare una valutazione continua delle vulnerabilità di tali risorse.

Una vulnerabilità è una debolezza di un asset che potrebbe essere sfruttata da vari vettori di minaccia. Il panorama delle vulnerabilità cambia ogni giorno a causa dei progressi tecnologici, delle falle non identificate negli asset, delle configurazioni errate e degli errori umani. I criminali informatici sono sempre in prima linea per sfruttare queste vulnerabilità per ottenere un accesso non autorizzato alla rete aziendale ed esporre informazioni sensibili per vari motivi negativi.

Al fine di identificare, analizzare e rimediare le vulnerabilità, la Società effettua delle attività di Vulnerability Assessment. Una delle tecniche più complete di Vulnerability Assessment è il Penetration Test (PT) che prevede un attacco vero e proprio, condotto da esperti autorizzati, che si comportano come fossero veri e propri criminali. Ai fini del presente documento, verrà utilizzata la nomenclatura Vulnerability Assessment senza distinzione delle varie tecniche che è possibile adottare.

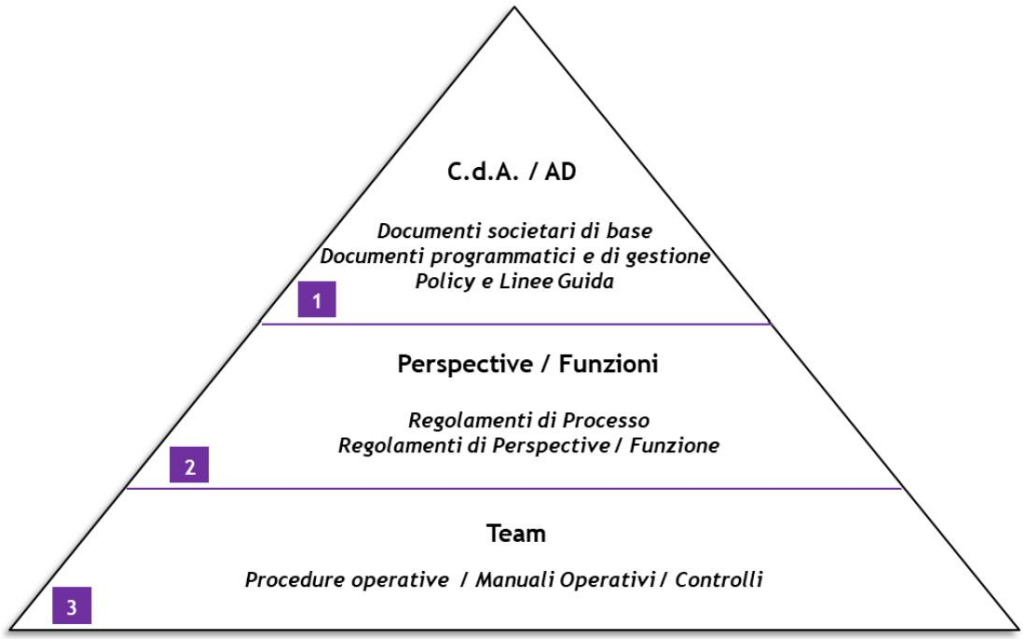
1.1 OBIETTIVO DEL DOCUMENTO

Obiettivo del presente documento è quello di fornire indicazioni operative per la gestione e la mitigazione delle vulnerabilità identificate a livello applicativo ed infrastrutturale che potrebbero essere sfruttate ai danni di Flowe e pregiudicare il corretto funzionamento dei suoi processi operativi e di business, e più in dettaglio:

- descrivere il flusso procedurale e le attività operative con cui vengono rilevate, gestite, mitigate e monitorate le vulnerabilità;
- indicare e fornire istruzioni sugli strumenti a supporto del processo;
- descrivere le responsabilità delle unità organizzative di Flowe coinvolte nel processo.

Con riferimento alla “Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna”, il presente documento si colloca al secondo livello della piramide documentale richiamata nello schema seguente.

Modello della normativa interna di riferimento



2 AMBITO DI APPLICAZIONE

Il presente Regolamento si applica a Flowe S.p.A. Società Benefit.

3 AGGIORNAMENTO DEL DOCUMENTO

L'aggiornamento del documento è a cura della *Perspective Augmented Intelligence* che dovrà provvedere a revisionarlo con cadenza almeno annuale o qualora si verifichi un cambiamento sostanziale, che possa influire in modo diretto o indiretto sul processo qui descritto.

4 STRUMENTI A SUPPORTO DEL PROCESSO

Gli strumenti a supporto del processo di identificazione delle vulnerabilità includono:

- **Tool "Registro delle vulnerabilità":** repository in cui vengono registrate tutte le vulnerabilità identificate ed i relativi dettagli;
- **Report:** documento, definito a seguito dell'attività di Vulnerability Assessment effettuata dal Fornitore Terzo a livello applicativo ed infrastrutturale, in cui vengono forniti i dettagli sull'attività condotta e sulle vulnerabilità identificate nel corso della stessa.

5 ATTORI, RUOLI E RESPONSABILITA'

Il modello organizzativo adottato dalla Società per la gestione delle vulnerabilità prevede il coinvolgimento di IT Operation Security & Governance appartenente alla *Perspective Augmented*

Intelligence, del Key Business User (come definito nel "Regolamento del processo di identificazione e classificazione degli asset") e di Fornitori esterni con i quali è stipulato un contratto, che si impegnano, per quanto di competenza, ad applicare rigorosamente i principi contenuti nel presente Regolamento.

Vengono indicati di seguito i ruoli e le responsabilità dei principali attori coinvolti per la gestione delle vulnerabilità in Flowe.

5.1 IT OPERATION SECURITY & GOVERNANCE

IT Operation Security & Governance ha la responsabilità di:

- Identificare, a seconda dell'asset di riferimento, il Fornitore più opportuno per procedere ai Vunerability Assessment necessari a identificare le vulnerabilità;
- Registrare le vulnerabilità emerse dalle attività di Vulnerability Assessement (tool Registro delle vulnerabilità);
- Valutare, supportato dal Key Business User, le vulnerabilità identificate all'interno del Report;
- Definire e pianificare le azioni di rimedio;
- Verificare l'effettivo rimedio alle vulnerabilità disponendo un'ulteriore scansione automatica o manuale;
- Registrare la chiusura delle vulnerabilità all'interno del registro (tool Registro delle vulnerabilità).

5.2 KEY BUSINESS USER

Il Key Business User ha la responsabilità di:

- Supportare *IT Operation Security & Governance* nell'analisi degli impatti di business delle vulnerabilità identificate tramite Vulnerability Assessment.

5.3 FORNITORI ESTERNI

I Fornitori esterni con i quali è stato stipulato un contratto si occupano dell'attività di valutazione automatica e/o manuale delle vulnerabilità a livello applicativo ed a livello infrastrutturale tramite esecuzione di Vulnerability Assessment e condividono con *IT Operation Security & Governance* un documento di dettaglio contenente tutte le vulnerabilità con relativa identificazione del livello di criticità.

Qualora necessario, collaborano con la Società, per condividere tutte le informazioni necessarie a definire le azioni di rimedio più adeguate a sanare le vulnerabilità identificate o ridurre il rischio a livello più accettabili.

6 FASI DEL PROCESSO DI VULNERABILITY MANAGEMENT

Il processo di Vulnerability Management si compone delle fasi illustrate qui di seguito:

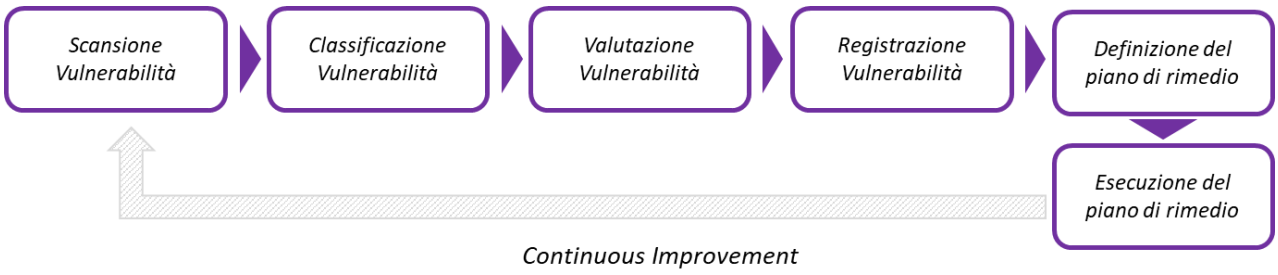


Figure 1 – Processo di Vulnerability Management

6.1 SCANSIONE DELLE VULNERABILITÀ

Questa fase fa riferimento all'identificazione delle vulnerabilità all'interno dell'asset, che può essere eseguita:

- **A livello infrastrutturale**
- **A livello applicativo (App Flowe)**

IT Operation Security & Governance, a seconda dell'asset di riferimento, identifica il Fornitore più opportuno per effettuare l'attività di Vulnerability Assessment volta all'identificazione delle vulnerabilità.

Scansione delle vulnerabilità a livello infrastrutturale

L'infrastruttura, ospitata in ambienti cloud di terze parti, dovrà essere sottoposta a scansione periodica per individuare le vulnerabilità.

La scansione a livello infrastrutturale dovrà essere effettuata almeno annualmente tramite il supporto di Fornitori esterni.

Scansione delle vulnerabilità a livello applicativo

La Società effettua la scansione delle vulnerabilità a livello applicativo indicativamente bisettimanalmente (sulla base delle funzioni rilasciate nelle versioni iOS e Android dell'applicativo) avvalendosi del supporto di Fornitori Terzi.

6.2 CLASSIFICAZIONE E ATTRIBUZIONE DEL LIVELLO DI CRITICITÀ

A seguito dell'identificazione delle vulnerabilità, quest'ultime devono essere classificate e prioritizzate.

La classificazione è il processo di categorizzazione delle vulnerabilità identificate dai Fornitori Esterni che hanno effettuato l'attività di Vulnerability Assessment. Questi forniscono ad *IT Operation Security & Governance* due fattori utili all'attribuzione del livello di criticità della vulnerabilità:

- Punteggio CVSS: valore ottenuto dallo standard CVSS (Common Vulnerability Scoring

System) che determina la gravità di una vulnerabilità

Classificazione CVSS	Punteggio CVSS
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

- Fattore di exploitability (sfruttabilità): valore che tiene conto della facilità con la quale un attaccante riesce a sfruttare una vulnerabilità. I valori sono compresi fra 1 (vulnerabilità facilmente sfruttabile) e 4 (vulnerabilità difficilmente sfruttabile).

Sulla base della classificazione ottenuta, *IT Operation Security & Governance* attribuirà ad ogni vulnerabilità un livello di criticità tra i seguenti:

- Basso
- Medio
- Alto
- Critico

6.3 VALUTAZIONE DELLA VULNERABILITÀ

IT Operation Security & Governance procede con la valutazione delle vulnerabilità identificate, dando precedenza alle vulnerabilità che hanno ottenuto un punteggio con livello di criticità pari a "Critico".

Nel processo di valutazione, *IT Operation Security & Governance*, eventualmente supportata dal Key Business User, identificherà le azioni di rimedio da attuare per risolvere la vulnerabilità tenendo conto della fattibilità delle stesse in termini di timing, effort e costi.

La valutazione effettuata condurrà alla definizione del Piano di Rimedio.

6.4 DEFINIZIONE DEL PIANO DI RIMEDIO E MITIGAZIONE DELLE VULNERABILITÀ

Tenendo conto dei dettagli forniti rispetto alle vulnerabilità identificate, *IT Operation Security & Governance* definisce le azioni di rimedio e procede alla pianificazione delle stesse.

Le tempistiche previste per la risoluzione delle vulnerabilità sono le seguenti:

- **Vulnerabilità critiche:** risoluzione immediata entro massimo 15 giorni;
- **Vulnerabilità alte:** risoluzione entro 30 giorni;
- **Vulnerabilità medie e basse:** le tempistiche delle remediation verranno valutate caso per caso.

La pianificazione delle azioni di rimedio verrà formalizzata in occasione di un meeting ricorrente in cui è prevista la partecipazione anche del Key Business User.

Nella definizione del piano di rimedio *IT Operation Security & Governance* potrà valersi del supporto dei Fornitori esterni, che si sono occupati del Vulnerability Assessment, al fine di identificare le soluzioni da realizzare per sanare le scoperture e quindi mitigare le vulnerabilità.

6.5 DOCUMENTAZIONE DELLA VULNERABILITÀ

IT Operation Security & Governance , una volta attribuito il livello di criticità alle vulnerabilità identificate, dovrà procedere alla registrazione dei risultati all'interno di un repository centrale (tool Registro delle Vulnerabilità).

All'interno del repository devono essere compilati almeno i seguenti campi:

- Asset di riferimento
- Asset Owner
- Tipologia della vulnerabilità
- Descrizione della vulnerabilità
- Livello di criticità
- Data di identificazione della criticità

6.6 ESECUZIONE DEL PIANO DI RIMEDIO E RICONVALIDA

Una volta finalizzato il piano di rimedio, quest'ultimo dovrà essere eseguito secondo le scadenze pianificate.

Dopo aver posto rimedio alla vulnerabilità, *IT Operation Security & Governance* dovrà convalidare l'azione intrapresa, effettuando nuovamente la scansione delle vulnerabilità e verificando che l'azione di rimedio realizzata sia risultata adeguata ad eliminare la vulnerabilità o, quantomeno, a mitigarla riducendo il rischio ad un livello accettabile.

Una volta conclusi tutti questi processi, i risultati e le azioni dovranno essere registrati all'interno del Registro indicando lo stato della vulnerabilità come "chiuso".

7 NORMATIVA

Nel presente capitolo si richiama il contesto normativo di riferimento per le attività in esame. L'elenco fornito non si ritiene esaustivo e viene riportato principalmente allo scopo di richiamare l'attenzione sui principali riferimenti, della normativa generale ed interna aziendale, sui quali si fonda il presente Regolamento.

Normativa interna:

- Policy di Sicurezza di Flowe;
- Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna;

- Regolamento del processo di identificazione e classificazione degli asset.

Normativa esterna:

- Circolare n. 285 del 17 dicembre 2013 – *Disposizioni di vigilanza per le Banche;*
- EBA/GL/2017/05 "Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP) e successivi aggiornamenti";
- Banca d'Italia Circolare n. 285 del 17 dicembre 2013 – Disposizioni di vigilanza per le Banche e successivi aggiornamenti;
- EBA/GL/2019/02 - Orientamenti in materia di esternalizzazione e successivi aggiornamenti;
- Provvedimento Della Banca d'Italia de 23 luglio 2019, Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica e successivi aggiornamenti;
- Direttiva (UE) 2015/2366 PSD2 – (Payment Services Directive 2) e successivi aggiornamenti.