Organizzazione	
Documenti di riferimento:	• **PIC_FW_ortm_Piano valutazione sicurezza RunAs_1_0.doc** • **PIC_UO_tstp_Report valutazione sicurezza RunAs_1_0.doc** • **PIC_IA_8_sirk_AnalisiDelRischio_260109_1_2.doc** • **PIC_IA8_vapt_ProgettazioneTestVAPT_090123_1_1.doc** • **Risultati VAPT – Allegato 1 – VA.doc;** • **Risultati VAPT – Allegato 2 – PT.doc;** • **PIC_IA8_vapt_ProgettazioneTestVAPT_090123_1_1.doc;** • **PIC_IA8_sirk_AnalisiDelRischio_260109_1_3.doc**

ESITO DELL'ASSESSMENT

CARENZE

1. Il documento finale non riporta le eccezioni e le modifiche apportate in corso d'opera rispetto a quanto pianificato, ad esempio: i test pianificati il giorno 28/1/09 sono stati ridotti, cioè il numero di porte scansite è stato ridotto dal 100% del controllo fisico previsto ad un insieme logico significativo in termini di sicurezza, ciò a causa delle stime effettuate che evidenziavano una fine lavori oltre i tempi stimati per l'esecuzione del test. Tale situazione denota inoltre una inesatta pianificazione delle attività.
2. Non vi è evidenza del collegamento tra i risultati prodotti e le specifiche TUV Italia concordate in fase di progettazione del test.
3. La simbologia adottata per gli esiti (simboli e colori) non è supportata da una spiegazione dei criteri adottati per l'assegnazione di ciascuna valutazione.
4. Non risultano esiti per quanto concerne la vulnerabilità V06 sebbene questa sia stata considerata tra quelle da ridurre nella fase di valutazione dei rischi (tale anomalia era già stata rilevata dall'analisi Documentale precedentemente effettuata da TUV Italia).
5. Rilievi inerenti il documento **PIC_FW_ortm_Piano valutazione sicurezza RunAs_1_0.doc**

   Non esiste riscontro diretto rispetto all'attività oggetto del presente documento e del documento collegato di esito di valutazione codice PIC_UO_tstp_Report valutazione sicurezza RunAs_1_0.doc.

   Tale attività non risultava mappata nell'analisi dei rischi al paragrafo finale di definizione della stessa all'atto dell'audit in loco (documento codice PIC_IA_8_sirk_AnalisiDelRischio_260109_1_2.doc), in cui, al capitolo 6, lettera j), si fa riferimento ad un elemento di VA proposto (testualmente "consigliato") di reverse engineering sul modulo RunAs, mentre nel documento oggetto di valutazione si fa riferimento ad altra metodologia.
   Risulta invece mappata nella revisione 3 del suddetto documento (documento PIC_IA_8_sirk_AnalisiDelRischio_260109_1_2.doc) al paragrafo 5.9.2 step S1, nel quale si rimanda, con indicazione al Capitolo 6, ad indicazione specifica prevista e richiamata in [4] nel paragrafo 1.5.
   L'ultima revisione del documento di progettazione esecutiva (documento PIC_IA8_vapt_ProgettazioneTestVAPT_090123_1_1.doc) di fatto non richiama la valutazione del modulo RunAs e non ne pianifica alcuna attività presso TSF, pertanto appare come slegato dal resto delle attività di VA/PT.

Osservazione Paragrafo 1.5
Non vi sono riferimenti alle Linee Guida TUV. Qualunque attività di VA/PT eseguita sul modulo RunAs non è conforme alle linee diffuse.

Paragrafo 2.2.2
Non è evidente se le indicazioni di dettaglio nella definizione dello "scope" di applicabilità della ISO/IEC14598 fanno genericamente riferimento a potenziali ambiti di "scope" (come sembrerebbe riportato nel paragrafo "Possibili prodotti da valutare" o se tale indicazione fa riferimento alle possibilità di valutazione nell'ambito di quelle selezionate per il modulo RunAs, oggetto della valutazione di sicurezza.

Paragrafo 2.2.2.8
Il paragrafo 2.2.2.8 non ha riscontro effettivo nella realtà della valutazione di sicurezza del modulo RunAs poiché non ha applicazione nel documento di raccolta evidenze dei risultati di valutazione codice PIC_UO_tstp_Report valutazione sicurezza RunAs_1_0.doc cui si rimanda. In tale documento, infatti, la rappresentazione dell'esito della valutazione segue uno schema completamente diverso da quello proposto.

Paragrafo 3.1
La finalità della valutazione non è chiaramente esposta.

Paragrafo 3.2
Non si ha alcuna evidenza del contenuto della documentazione di specifica elencata. Non è possibile stabilire evidenze oggettive del lavoro svolto senza riscontri con la documentazione indicata.

Paragrafo 3.3
Alla luce di quanto esposto al punto precedente, non esistono specifiche oggettive sulle caratteristiche indagate.

Paragrafo 3.3
L'indicazione di verifiche puntuali non appare esaustiva. Quanto citato al paragrafo 2.2, come da osservazioni precedenti, appare come un insieme di specifiche di norma, di scelte dell'azienda a procedere, di esempi da tracciare e di attività reali. Non è riscontrabile il reale carico di attività svolto nell'arco del tempo/uomo indicato.

Paragrafo 3.6
Non si ha riscontro delle verifiche puntuali citate né dei casi di test da applicare.

Paragrafo 3.7
Il paragrafo cita, per la prima volta, riscontri di documentazione (sarebbe stao opportuno quindi citare tutti i riferimenti prima delle altre indicazioni nei paragrafi precedenti). Tuttavia la citazione ad un ipotetico documento [3] non trova riscontro poiché nella definizione dei documenti di riferimento abbiamo solamente un documento [1] e [2], come di evince al paragrafo 1.5. Non vi è peraltro alcun riscontro obiettivo delle indicazioni della documentazione di riferimento Microsoft, cui si rimanda per un generico link di esempio, quindi chiaramente non esaustiva. Non sono descritte con sufficiente chiarezza le attività operative dei singoli casi di prova. Non sono descritte le specifiche che differenziano RunAsLauncher, RunAsService, Cachemanager, CreateProcessWithLogon nell'ambito del c.d. modulo RunAs.

6. Rilievi inerenti il documento **PIC_UO_tstp_Report valutazione sicurezza RunAs_1_0.doc**

Si veda quanto esposto precedentemente per il documento PIC_FW_ortm_Piano valutazione sicurezza RunAs_1_0.doc.

Paragrafo 2.2
Permangono le difficoltà di interpretare oggettivamente il valore della valutazione svolta poiché mancano tutti i riferimenti di dettaglio del modulo RunAs, delle sue componenti, delle modalità con le quali sono svolte le azioni di test, come sono raccolte le evidenze oggettive di test ed in base a quali criteri. La già citata norma ISO/IEC 9126 e la selezione della caratteristica da misurare (Qualità interna > Funzionalità > Sicurezza) definisce il criterio ma non la regola di applicazione né tantomeno la modalità di misurazione.

7. Rilievi inerenti il documenti [a] PIC_IA8_vapt_RisultatiTestVAPT090206_1_0.doc; [a1] Risultati VAPT – Allegato 1 – VA.doc; [a2] Risultati VAPT – Allegato 2 – PT.doc; [b] PIC_IA8_vapt_ProgettazioneTestVAPT_090123_1_1.doc; [c] PIC_IA8_sirk_AnalisiDelRischio_260109_1_3.doc

L'analisi documentale conclusiva viene eseguita partendo dai risultati dell'attività di VA/PT e risalendo, per ciascuno di essi, alla specifica di progettazione esecutiva che ne ha definito le modalità di esecuzione, e l'analisi dei rischi, che ne ha definito la necessità, l'ambito ed il risultato atteso ai fini della determinazione del rischio. Il documento di risultati del test viene analizzato tenendo conto dei due allegati citati.

La prima osservazione generale è che il rilascio della documentazione appare parzialmente conforme alle linee guida TUV, per quanto queste siano richiamate nei documenti [a], [b] come riferimenti solo per la scelta delle attività di test. Infatti non sono chiaramente evidenziate sempre le metodologie adottate ma solo enumerati gli strumenti (tool), senza peraltro specificare con quale script o opzione viene usato il tool medesimo.

La seconda osservazione generale è che non disponiamo dei documenti di dettaglio operativo e di riscontro di HackingTeam, società incaricata delle attività di VA/PT. Non vi è modo pertanto di avere riscontri diretti con gli esiti delle loro attività, per quanto riportato in [a], [a1] e [a2].

La terza osservazione generale è che nella parte di executive summary, per le valutazioni di sicurezza mappate al paragrafo 3.3, sono indicate descrizioni di impatto e contromisure con tre livelli di sicurezza rilevata, per le quali, in alcune di queste, non si riscontra come il livello associato sia effettivamente conseguente con le probabilità di impatto, le eventuali contromisure e l'analisi del rischio a monte.

Questa riflessione può essere edotta da una serie di potenziali difficoltà interpretative.

Si prenda a solo titolo di esempio quando riportato in [a] al paragrafo 4.2, che ha dettaglio operativo in [a2]. Si consideri il fatto che il test riportato in [a] paragrafo 4.2 viene richiamato nell'executive summary di [a] paragrafo 3.3 test 1.a come OK, ESITO POSITIVO, LIVELLO DI SICUREZZA APPROPRIATO; ALCUNI ACCORGIMENTI DA APPORTARE.
L'esame di dettaglio in [a2] riferito al paragrafo 1.4.2 con risultati espressi in 1.4.3 evidenzia la possibilità di compiere operazioni su volumi di rete condivisi, creazione cartelle, modifiche file anche di siti web istituzionali, lettura di parametri di connessione a database ecc. Questi rilievi vengono considerati in [a] paragrafo 3.3 punto 1.a "Ipotesi di scenario" come strumenti che possono consentire operazioni: tali ipotesi di scenario come rendono il controllo eseguito di livello OK anziché di ESITO NEGATIVO. In base a quale considerazione di rischio posso assegnare un livello tale per cui le ipotesi di scenario evidenziate sono da considerarsi residuali e pertanto è corretto assegnare tale livello di attestazione?

Queste considerazioni, estendibili a tutte le valutazione di VA/PT, sposano l'ultima notazione: salendo a ritroso il percorso documentale da [a] verso [b] verso [c], permangono dubbi su come l'attività di VA/PT possa confermare o meno l'attestazione del rischio residuo definita in [c]. Non si determina, in modo oggettivo, come ad ogni rilievo eseguito ed elencato in [a] possano esserci scelte indebitamente corrette nel giudicare che i risultati elencati rientrino in un range di esame di rischio che si possa considerare effettivamente residuo rispetto all'analisi generale eseguita in [c].

COMMENTI

1. La definizione "a regola d'arte" può essere riferita solo all'ambito elettrotecnico essendo prevista nello standard IEC 61508 (sicurezza in campo elettrico), pertanto risulta impropria nel contesto analizzato.

CONCLUSIONI

Sulla base delle evidenze raccolte nel corso dell'assessment e a fronte delle carenze individuate si conclude che il VS/PT eseguito:

1. non soddisfa i requisiti di progettazione e pianificazione;
2. non dimostra il valore di rischio residuo atteso a seguito della valutazione dei rischi;
3. sebbene tutte le attività siano state svolte con metodo sembra che il lavoro svolto abbia affrontato solo aspetti iniziali, sembra cioè aver solo scalfito la superficie di un tema assai più vasto ed articolato; per questo se ne raccomanda una ripetizione a breve che, completando quanto evidenziato dalle carenze, estenda le analisi e le valutazioni in modo da approfondire quanto più possibile quanto evidenziato in particolare dai rilievi 5, 6 e 7.