LOMBARDIA INFORMATICA

Classificazione: ~~da definire~~ RISERVATO

Verbale di Riunione

Data e luogo:

04 Giugno 2014

Redattore:

Responsabile:

Oggetto dell'incontro:

Presentazione dei risultati relativi alle attività di Audit condotte sul contratto 270/12 del 14 Maggio 2012

Lista dei partecipanti:

Cognome, nome	Azienda di appartenenza
	Lombardia Informatica
	Lombardia Informatica
	Lombardia Informatica
	Lombardia Informatica
	Lombardia Informatica
	Lombardia Informatica
	Lombardia Informatica
	Lombardia Informatica
	Maglan
	Maglan
	Santer Reply
	Santer Reply
	Santer Reply

Tematiche affrontate:

Coerentemente a quanto disposto dall'articolo 11 comma 1 del contratto 270/12 sottoscritto in data 14 maggio 2012, Lombardia Informatica ha incaricato la società Deloitte Consulting S.p.A., che si è avvalsa delle competenze della società Maglan Europe S.r.l., di effettuare un'attività di Audit., al fine di verificare la compliance delle attività eseguite dal fornitore nell'esecuzionre dei contrattoo rispetto a quanto disposto da tutta la documentazione di gara e per gli aspetti migliorativi da quanto offerta da Santer Reply nell'offerta tecnica.

L'esito delle attività di Audit è descritto nell'allegato tecnico che si allega al presente verbale e che ne costituisce parte integrante.

Nell'allegato tecnico per ciascuna delle non conformità emersa nel corso dell'Audit viene indicata la soluzione che il fornitore dovrà adottare per poter superare quanto evidenziato. Inoltre ciascuna delle non conformità rilevate viene identificata con un livello priorità di soluzione secondo quanto di seguito riportato:

Legenda:

- ✓ A: immediato;
- ✓ B: breve termine;
- ✓ C: medio termine;
- ✓ D: medio-lungo termine.

Azioni Definite:

Lombardia Informatica richiede al fornitore di predisporre un piano, che partendo dall'esito delle attività di Audit, e dalle loro criticità, descriva le attività che si intendono mettere in atto al fine di risolvere le non conformità evidenziate.

Santer Reply si rende disponibile a predisporre un piano di remediation, che tenga conto delle priorità evidenziate, ed a sottoporlo all'approvazionre di Lombardi Informatica entro il 13 GIU 2014

Lombardia Informatica si riserva di verificare le azioni messe in atto dal piano concordato e rende disponibile, per la consultazione presso la propria sede, la documentazione tecnica risultante dalle attività di audit effettuate.

Letto firmato e sottoscritto

Lombardia Informatica

Santer Reply

ALLEGATO TECNICO

Adeguamento Organizzativo

RISULTANZE AUDIT ORGANIZZATIVO	REMEDIATION	PRIORITA'
PROCESSO DI GESTIONE CHIAVI CRITTOGRAFICHE		
✓ Non sono state identificate chiare responsabilità in merito alla gestione della sicurezza;	Identificare funzione interna con chiari compiti di controllo verso le tematica di information security (CISO).	A
RESPONSABILITA' GESTIONE CHIAVI		
✓ Non sono state identificate chiare responsabilità interne e di controllo verso i fornitori	Identificare chiari punti di controllo e responsabilità con cui assoggettare la sicurezza dei fornitori (es. processo / funzione di audit periodico).	B

Sviluppo Codice

RISULTANZE AUDIT ORGANIZZATIVO	REMEDIATION	PRIORITA'
DEFINIZIONE E GESTIONE DEI SECURITY REQUIREMENTS DI PROGETTO		
✓ Nella fase di sviluppo del software non sono formalizzate e quindi considerate indicazioni di sicurezza di dettaglio (Security Requirement) relativi alle specifica piattaforma / linguaggio di programmazione utilizzati.	▪ Acquisire le indicazioni del Pen Test, tradurle in requisiti di sicurezza di dettaglio con il supporto di personale skillato in tecniche di secure coding; ▪ Attuare recoding per eliminare le criticità riscontrate; ▪ Formalizzare requisiti di sicurezza per ogni futuro cambiamento e/o modifica significativa;	A
PROCESSO DI PROCESSO DI SVILUPPO DEL CODICE		
✓ Non è stato rilevato un processo strutturato di sviluppo del software (SDLC) che prevede tutte le fasi volte a garantire la sicurezza (security requirement, test, accettazione ..); ✓ Ad oggi nelle fasi di sviluppo non sono prese in considerazioni le indicazioni di sicurezza relative alla specifica piattaforma o framework di sviluppo	▪ Strutturare e formalizzare il processo di sviluppo; ▪ Adeguare processo di sviluppo considerando ed implementando le best practice di sviluppo sicuro; ▪ Dotarsi di strumenti / processi di verifica del codice che prevedano fasi di test	B

(requisiti di sviluppo sicuro nella fase di programmazione) utilizzato; ✓ Non vengono definite procedure e controlli per verificare la presenza di codice potenzialmente dannoso o vulnerabile nelle applicazioni.	specifici; ▪ Pianificare attività di controllo periodiche;	
PRINCIPALI VULNERABILITA' APPLICATIVE RISCONTRATE Data la fragilità strutturale non è stato eseguito un test con tool automatici per verificare la presenza di vulnerabilità note nel codice sviluppato (API, moduli, macro) al fine di evitare possibili ripercussioni sulla continuità operativa del servizio erogato.		
✓ Il software non prevede in alcuni punti i controlli di input/output ed in particolare permette di processare dei comandi (memorizzare, eseguire, inoltrare, etc.) come parte del vettore in ingresso. ✓ Il log applicativo non traccia adeguati e sufficienti eventi di sicurezza; ✓ Non vengono bonificate e cancellate le aree di memoria in cui risiedono file temporanei ✓ L'analisi ha evidenziato la possibilità di accedere alle chiavi private di cifratura ✓ L'analisi ha evidenziato una forte interdipendenze tra i sistemi da approfondire in termini di sicurezza	▪ Acquisire le indicazioni del Pen Test, tradurle in requisiti di sicurezza di dettaglio con il supporto di personale skillato in tecniche di secure coding; ▪ Attuare recoding per eliminare le criticità riscontrate; ▪ Approfondire il livello di tracciatura dei log applicativi (vedi sezione log); ▪ Adeguare modalità di gestione / cancellazione sicura dei file temporanei; ▪ Adeguare modalità di gestione degli script delle chiavi crittografiche; ▪ Verificare interdipendenze tra i sistemi e flussi e relativa protezione;	C

Change Management

RISULTANZE AUDIT ORGANIZZATIVO	REMEDIATION	PRIORITA'
PROCESSO DI CHANGE MANAGEMENT		
✓ A fronte di nuovi sviluppi o modifiche (vedi indicazioni processo di Change Management- CM) non vengono eseguiti controlli specifici per verificare debolezze intrinseche o presenza di codice potenzialmente dannoso o vulnerabile;	▪ Eseguire i controlli di sicurezza a fronte di nuovi sviluppi o change e documentarli opportunamente con e i relativi esiti; ▪ verificare i parametri di sicurezza dell'applicativo Subversion che supporta il processo di CM	B
AMBIENTI E TIPOLOGIA DI DATI UTILIZZATI		
✓ Non è stata rilevata la segregazione tra ambiente di sviluppo e produzione ✓ I dati utilizzati dal software nell'ambiente	▪ Creare la separazione degli ambienti tra sviluppo/collaudo e produzione ▪ I dati utilizzati dal software nei vari	D

di sviluppo e test sono una copia dei dati di produzione e contengono dati personali reali.	ambienti, ad eccezione della Produzione, non devono essere reali e comunque non devono contenere dati personali reali ▪ Implementare sistemi per la protezione del codice sorgente in ambiente di sviluppo e test;	
VERIFICHE PRIMA DELLA MESSA IN PRODUZIONE		
✓ Al momento del rilascio del software non sono effettuati opportuni controlli per verificare la sicurezza del software. In particolare, devono essere eseguite almeno attività di vulnerability assessment dal punto di vista infrastrutturale e applicativo.	▪ Al momento del rilascio del software devono essere effettuati opportuni controlli per verificare la sicurezza del software. In particolare, devono essere eseguite almeno attività di vulnerability assessment dal punto di vista infrastrutturale e applicativo ▪ Il rilascio del software in Produzione deve avvenire solo dopo aver superato tutti i controlli stabiliti (formali, funzionali e di sicurezza) e solo dopo essere stato installato ed opportunamente verificato in ambiente di Collaudo.	**D**
SEGREGAZIONE COMPITI SVILUPPO TEST E PRODUZIONE		
✓ Rilevata assenza di separazione di responsabilità tra chi opera in produzione e in ambiente di sviluppo test	▪ Garantire la separazione dei compiti tra sviluppo e messa in produzione; ▪ Il rilascio del software in Produzione deve avvenire solo a seguito di esplicita autorizzazione	**C**

Cifratura – Gestione Chiavi

RISULTANZE AUDIT ORGANIZZATIVO	REMEDIATION	PRIORITA'
PROCESSO DI GESTIONE CHIAVI CRITTOGRAFICHE		
✓ Non è attuato e/o formalizzato nessun processo per la gestione delle chiavi crittografiche, in particolare per la chiave crittografica RSA 1024 gestita per conto di Lombardia Informatica.	Definire il processo e valutare l'eventualeimplementazione delle chiavi a 2048 bit	**A**
RESPONSABILITA' GESTIONE CHIAVI		
✓ Le responsabilità gestionali vengono gestite in maniera informale con il coinvolgimento del personale sistemistico	Definire chiare responsabilità gestionali, operative e di controllo periodico	**B**

che opera all'interno dell'ambito tecnologico		
PROTEZIONE DELLE CHIAVI CRITTOGRAFICHE		
✓ L'audit tecnologico ha evidenziato le necessità di proteggere le chiavi crittografiche in maniera consistente (In particolare rilevata la possibilità di accedere anche a dati sensibili)	Adeguare secondo le specifiche emerse dal Pen Test (vedi Decryption private Keys Exposed) dopo avere effettuato un analisi esaustiva	A

Hardening dei Sistemi

RISULTANZE AUDIT ORGANIZZATIVO	REMEDIATION	PRIORITA'
CONFIGURAZIONE SISTEMI – S.O.		
✓ Non sono state rilevate attività di sicurizzazione / hardening dei sistemi a livello di sistema operativo;	Dotarsi di informazioni aggiornate circa i protocolli di hardening da utilizzare sulle diverse piattaforme ed implementarle;	A
CONFIGURAZIONE SISTEMI – Applicazioni - D.B.		
✓ Sono state rilevate componenti software e applicative non aggiornate;	Le componenti software degli applicativi e dei DBMS non più supportate o inutili ai fini operativi devono essere aggiornate o rimosse.	A
CONFIGURAZIONE LISTENER		
✓ Sono state rilevate vulnerabilità nei listener file	I file di configurazione contenenti informazioni sulle connessioni al database (listener file) devono essere configurati in modo da garantire la riservatezza delle credenziali di accesso ai database e delle connessioni, l'integrità della configurazione del listener stesso e la disponibilità delle connessioni verso i database.	B
PROCESSO DI PATCHING		
✓ Sono state rilevate componenti software e applicative non aggiornate;	I software applicativi (web server) devono essere aggiornati con le patch di sicurezza rilasciate dai relativi fornitori e di cui è stata accertata la compatibilità con l'operatività dei sistemi stessi. L'installazione delle patch di sicurezza deve avvenire ad ogni successivo rilascio da parte dei fornitori. Qualora non sia possibile installare gli aggiornamenti deve essere tenuto traccia delle	B

	patch non installate e della motivazione per la quale non si è proceduto all'installazione.	
ANALISI DELLE MINACCE DEI SISTEMI		
✓ Non si ha evidenza dell'esecuzione di un'analisi dei rischi che prenda in considerazioni le reali vulnerabilità dei sistemi analizzati;	Redigere e mantenere aggiornato un elenco delle vulnerabilità che affliggono i sistemi, con informazioni sulla loro criticità, sui possibili impatti sull'operatività e sulle contromisure applicabili per la mitigazione del rischio associato alla vulnerabilità;	D
TRACCIATURA MODIFICHE		
✓ Non sono implementati audit Trial che garantiscano una verifica puntuale e storica delle modifiche occorse	Implementare meccanismi per la gestione delle configurazioni dei sistemi in grado di tenere traccia dei cambiamenti apportati ai sistemi stessi.	B
GESTIONE FILE TEMPORANEI		
✓ Sono stati rilevati diversi file temporanei potenzialmente rischiosi per la riservatezza delle informazioni;	I file temporanei generati dai sistemi e dalle applicazioni devono essere cancellati quando non più utilizzati e non necessari ad attività di monitoraggio o di tracciamento.	A

Identity Management

RISULTANZE AUDIT ORGANIZZATIVO	REMEDIATION	PRIORITA'
GESTIONE UTENZE DEI SISTEMI, DB E AMMINISTRAZIONE APPLICAZIONE		
Non sono stati rilevati i seguenti aspetti: • utilizzo utenze personali • elementi enforcement password (8 caratteri, complessità, history, cambio password, ecc.) • gestione dei profili correlati alle mansioni • revisione efficace dei profili di accesso	Adeguare i processi di gestione utenze dei sistemi, DB, amministrazione applicazione	A
SICUREZZA CREDENZIALI DI ACCESSO AI DB		
✓ Le utenze con relative password per l'accesso ai DB sono risultate vulnerabili a semplici attacchi dizionario (sono state decifrate e rese leggibili in	Le credenziali di accesso ai database devono essere meno banali e memorizzate con algoritmi di cifratura più robusti rispetto all'attuale.	A