MISURE MINIME DI SICUREZZA - REGEL

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	*Regel dispone della gestione di ruoli e permessi per ogni utenza e funzionalità, con la possibilità di indicare la tipologia di accesso.*
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	*Regel registra gli accessi automaticamente tracciando le operazioni del singolo utente e mettendole a disposizione dell'utente amministratore.*
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	*Regel consente di profilare ciascun utente tramite un sistema di permessi e profili, al fine di gestire i privilegi per ogni funzionalità.*
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	*Regel registra ogni singola attività svolta sui dati dell'applicativo. La gestione dei LOG permette la registrazione sequenziale e cronologica delle operazioni che progressivamente vengono eseguite sul sistema, effettuate da qualsiasi utente.*
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	*Con Regel è possibile gestire in qualsiasi momento la profilazione di qualsiasi utente verificandone lo stato di attivazione, i ruoli e permessi di profilazione assegnati.*
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	*Ogni singola operazione sull'utenza amministrativa (CRUD) viene tracciata nei log di sistema.*
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	

5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	*Gli utenti che accedono a Regel devono impostare una password alfanumerica di almeno 8 caratteri.* *I parametri per la gestione delle autenticazioni e delle password sono:* - *Lunghezza minima del codice di accesso (8 caratteri)* - *Numero minimo dei caratteri minuscoli* - *Numero minimo dei caratteri maiuscoli* - *Numero minimo dei caratteri numerici* - *Numero minimo dei caratteri speciali*
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	*Le caratteristiche del punto 571M limitano l'utilizzo di credenziali deboli.*
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	*Tale funzione sarà implementata nel sistema.*
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	*Tale funzione sarà implementata nel sistema.*
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	

5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	*In Regel i privilegi sono distinti tra i vari utenti, ogni utente ha distinte credenziali.*
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	*In Regel ogni utente corrisponde ad una anagrafica.*
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	*In Regel le credenziali sono conservate in forma criptata (funzione di hashing "bcrypt") all'interno della database e sono accessibili solo tramite il software.*
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	*In Regel vengono mantenuti tutti i backup di qualsiasi momento temporale. Ogni giorno il backup viene fatto 4 volte:* - *Ore 01.00* - *Ore 11.00* - *Ore 14.00* - *Ore 19.00* *Nell'infrastruttura locale è mantenuto per 5 giorni.* *Ogni giorno alle 19.00 viene eseguito il backup in una ulteriore infrastruttura e mantenuto per 5 anni.*
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	*In Regel vengono fatti test di ripristino di tutti i dati di un precedente backup ogni 7 giorni.*
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	*In Regel i backup vengono effettuati con strumenti diversi e l'integrità dei dati nel backup viene verificato con software automatici.*
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	*In Regel vengono fatti test di ripristino di tutti i dati di un precedente backup ogni 7 giorni.*
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	*In Regel i backup sono accessibili solo al fornitore del software. La comunicazione tra la produzione del backup e lo storage avviene con il protocollo HTTPS.*
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	*In Regel i backup vengono gestiti in storage diversi da quelli dell'infrastruttura dell'azienda fornitrice.* *Le copie sono su droplet differenti all'interno dell'infrastruttura datacenter della prima azienda fornitrice e copiati sull'infrastruttura di una seconda azienda fornitrice.*

Firmato da:
MANCINI PAOLA
Motivo:

Data: 29/12/2017 13:33:59