Misure Minime di Sicurezza
Prodotti Unidos S.r.l.
Piattaforme CLOUD
Amministratore di Sistema: Italo Rosario Amorosa

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.	Tutti i prodotti Unidos S.r.l. consentono una gestione personalizzata dei profili dell'utente. Ogni utente può ricoprire un ruolo e utilizzare funzioni secondo una scala gerarchica.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Tutti i prodotti Unidos S.r.l. sono dotati di LOG mediante il quale si effettua una registrazione puntuale e minuziosa.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Tutti i prodotti Unidos S.r.l. consentono una gestione personalizzata dei profili dell'utente. Ogni utente può ricoprire un ruolo e utilizzare funzioni secondo una scala gerarchica.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Tutti i prodotti Unidos S.r.l. sono dotati di LOG mediante il quale si effettua una registrazione puntuale e minuziosa. I LOG sono archiviati per 6 mesi e non sono modificabili neanche dagli operatori tecnici. Solo l'Amministratore di Sistema può accedere ai LOG e/o aprire l'accesso agli sviluppatori.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Sulle utenze viene effettuata una eliminazione di tipo logica, in questo modo è sempre possibile risalire alle informazioni di quell'utente anche nel tempo. Il tutto è trasparente all'utente finale.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Non esiste un sistema automatico ma eventuali anomalie sono immediatamente segnalate all'Amministratore di Sistema che controlla la correttezza delle informazioni registrate.
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.	n.d.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Ogni informazione è tracciata sui LOG; L'eliminazione è di tipo logico.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza	n.g.

				amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	L'Amministratore di Sistema riceve informazioni dai sistemi quando un Admin modifica le impostazioni di un altro Admin.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Tutti i LOG dei prodotti Unidos S.r.l. tracciano ogni movimento ivi compresi i tentativi falliti di accesso.
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.	L'accesso alle piattaforme è demandato al controllo del Token di Google. Attraverso Google è possibile attivare tutti i livelli di sicurezza ivi compresi i sistemi di autenticazione a più fattori.
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).	Le configurazioni evitano che gli utenti possano utilizzare password deboli
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Le configurazioni evitano che gli utenti possano utilizzare password deboli
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le configurazioni impongono ai clienti la modifica della password ogni 3 mesi.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Le configurazioni impongono il divieto di riuso della password nei 6 mesi successivi.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Le configurazioni impongono un elevato livello di sicurezza ivi compresi i controlli sul tempo anti robot.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Le configurazioni impongono che le credenziali non possano essere utilizzate prima di 6 mesi dall'ultimo utilizzo.
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.	L'accesso ai sistemi è consentito a più livelli di controllo. In generale gli amministratori con proprie utenze possono operare in libertà ma quando effettuano operazioni tradizionali sono considerati utenti di ruolo "operatore".
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.	Le macchine dell'Amministratore di Sistema e le macchine degli sviluppatori sono utilizzate solo ed esclusivamente per le operazioni ad esse dedicate.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	I livelli di utenza sono gestiti sui prodotti in Pannello di Controllo, utenti e ripartiti in base ai ruoli.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono	In tutti i prodotti Unidos S.r.l. le utenze sono collegate al Codice

				essere nominative e riconducibili ad una sola persona.	Fiscale della persona alle quali sono collegate.
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.	Le utenze di Root dei sistemi Linux alla base delle macchine VPS Cloud dei prodotti Unidos S.r.l. sono a disposizione del solo Amministratore di Sistema.
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).	Non è possibile dotare gli operatori di Unidos S.r.l. di utenze diverse da quelle amministrative. Le operazioni svolte dal personale sono di livello tecnico tale da dover utilizzare per forza di cose il livello amministratore. Ogni macchina è assegnata ad un utente ben preciso.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali sono crittografate e custodite in database a loro destinate.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano certificati digitali.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Negli uffici della Unidos S.r.l. e nei server di smistamento e load balancing sono installati sistemi avanzati di antimalware e antivirus.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Sui server di produzione sono installati potenti firewall hardware e software, quelli di tipo hardware sono controllati e configurati da Aruba Business Spa.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Tutte le diagnostiche che registrano errori sono rinviati ad una registrazione sui LOG e portati all'attenzione dell'Amministratore di Sistema.
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Tutte le configurazioni sono gestite dall'Amministratore di sistema e non sono modificabili dagli utenti.
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun	I sistemi di antivirus e anti-malware sono aggiornati su ogni postazione attraverso un sistema di scripting sviluppato dal team

				dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	developer. I risultati sono riportati in una console di controllo in Html5.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	I malware vengono rintracciati e distrutti. Non esiste una quarantene zone.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Nessun operatore utilizza dispositivi esterni.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Sono vietati e non è possibile inserirli nelle macchine server.
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Le funzioni sono gestite e controllate dall'Amministratore di Sistema
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Le funzioni sono gestite e controllate dall'Amministratore di Sistema
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Le funzioni sono gestite e controllate dall'Amministratore di Sistema
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Le funzioni sono gestite e controllate dall'Amministratore di Sistema
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Le funzioni avanzate del Firewall sono gestite dall'Amministratore di Sistema
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Sulle macchine Server non sono presenti dispositivi removibili.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Sui sistemi UNIX non sono previste macro.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	I server e i sistemi Unidos S.r.l. non dispongono di propri account di posta ma si appoggiano alle Gsuite di Google.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Sui sistemi UNIX non sono previste anteprime dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Le funzioni sono gestite e controllate dall'Amministratore di Sistema
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	n.d.
8	9	2	M	Filtrare il contenuto del traffico web.	n.d.

8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	n.d.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Le funzioni sono gestite e controllate dall'Amministratore di Sistema

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.	Le copie di sicurezza sono effettuate giornalmente.
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.	Le copie di sicurezza riguardano l'intero sistema.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Le copie di sicurezza sono effettuate con 2 diversi servizi e lo stoccaggio del dato avviene su dischi separati.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Alcuni test random sono effettuati dall'Amministratore di Sistema
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.	Tutte le copie di sicurezza sono crittografate e archiviate su dischi criptati. L'accesso è consentito al solo Amministratore di Sistema
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.	Le copie di sicurezza sono stoccate su HDD esterni all'infrastruttura.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Al fine di proteggere la base di dati si è preferito cifrare e minimizzare tutti dati presenti nell'archivio.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	n.d.
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	Nei sistemi Unidos S.r.l. ci sono politiche di riservatezza, protezione e controllo che impediscono di inserire link non confermati. Il traffico entrate e uscente è registrato, controllato e filtrato.
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	Il team di sviluppo effettua periodicamente controlli di tipo OWASP sul codice al fine di evidenziare l'esistenza di bug. Nessun dato è al momento in chiaro.
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	n.d.
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	Solo il team di sviluppo e l'Amministratore di Sistema è autorizzato ad accedere ai server, l'autenticazione avviene mediante identificazione dell'IP delle singole macchine oltre che mediante username e password personalizzate.
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	Gli strumenti di controllo di rete sono configurati e a disposizione del solo Amministratore di Sistema.
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	L'Amministratore di Sistema dispone dei dati di navigazione in formato tabellare e grafico e può operare controlli e statistiche anche off-line.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	n.d
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Le blacklist sono configurate dall'Amministratore di Sistema e

					aggiornate periodicamente.
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	Sulle macchine server è installato un sistema di Access Control List e i dati sono registrati in repository implementate ad hoc.