Terze parti

Identificazione dei requisiti di sicurezza per l'accesso di fornitori/clienti ad informazioni o beni aziendali	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, ad opera di soggetti esterni.
Contromisure	Devono essere considerati e identificati tutti i requisiti di sicurezza prima di concedere ai partners, fornitori/clienti, anche in fase di trattativa, l'accesso a informazioni o beni dell'organizzazione ospitati nel sistema/piattaforma. Effettuare un'analisi dei rischi per valutare l'impatto sul business aziendale (a livello economico, d'immagine, di continuità operativa, eccetera) nel caso di violazioni della sicurezza, divulgazione non autorizzata (es. a concorrenti), illecito trattamento delle informazioni, effettuati da tali soggetti che accedono ad informazioni.

Identificazione dei requisiti di sicurezza negli accordi con i fornitori/clienti	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, ad opera di soggetti esterni.
Contromisure	Gli accordi con terze parti che prevedono accesso, elaborazione, comunicazione, aggiunte o, in generale, gestione delle informazioni ospitate nel sistema/piattaforma dell'organizzazione, devono considerare tutti i requisiti di sicurezza pertinenti. Prevedere, in particolare, misure preventive per evitare violazioni o illeciti delle terze parti nella gestione delle informazioni. Definire con precisione le attività, le modalità, le responsabilità e la periodicità, per l'esercizio di diritti di audit o comunque di verifiche sull'attività dei fornitori/clienti. Gli accessi logici privilegiati da parte di soggetti esterni devono essere subordinati alla nomina di tali soggetti ad amministratori di sistema, e tale nomina deve essere a sua volta legata ad uno specifico contratto con la ditta di appartenenza comprendente accordi di riservatezza e regole per il corretto uso delle risorse informatiche vincolanti per il fornitore e per i suoi dipendenti. Ovviamente gli accessi logici devono essere monitorati da parte di fornitori devono essere completamente monitorati. In ogni caso gli accessi privilegiati da parte di soggetti esterni non devono mai avvenire da sedi esterne (es. sede fornitore).

5.1.2 Autenticazione

Gestione delle informazioni segrete di autenticazione degli utenti	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	L'assegnazione agli utenti delle informazioni segrete di autenticazione (es. password) deve essere controllata attraverso un processo di gestione. Il processo dovrebbe prevedere: - l'uso di user ID e password individuali per sostenere il principio di accountability; - le modalità di assegnazione temporanea delle informazioni segrete di autenticazione, da cambiare al primo uso; - procedure per verificare l'identità di un utente, prima di fornire, modificare o sostituire nuove informazioni; - le modalità per assicurare il rispetto dell'utente della riservatezza delle informazioni segrete di autenticazione. Per quest'ultimo punto l'organizzazione dovrebbe informare l'utente delle sue responsabilità ed acquisire dallo stesso un formale impegno a mantenere riservate le informazioni (ad es. mediante specifica lettera da sottoscrivere).

Criteri per l'autenticazione mediante password	
Minaccia	- Accesso non autorizzato alle informazioni. - Furto di credenziali di autenticazione (ad es. con attacchi in grado di sfruttare l'eventuale inadeguatezza delle password). - Uso non autorizzato di privilegi (ad es. mediante tecniche di "escalation" verticali su un target o orizzontali).
Contromisure	Configurare le funzioni di controllo della qualità delle password per l'accesso ai sistemi, affinché la composizione rispetti i criteri di lunghezza, complessità e univocità necessari per avere una robustezza elevata. Ovvero, la password: - deve essere composta da un numero crescente di caratteri (almeno 8) in funzione della criticità delle informazioni da difendere (es. 15 caratteri per utenze amministrative); - deve contenere caratteri di almeno tre delle quattro categorie seguenti: a. lettere maiuscole dell'alfabeto latino (dalla A alla Z); b. lettere minuscole dell'alfabeto latino (dalla a alla z); c. numeri in base 10 (da 0 a 9); d. caratteri speciali non alfanumerici, ad esempio punto esclamativo (!); - non si deve riferire a qualcosa che qualcun altro possa facilmente indovinare od ottenere utilizzando informazioni relative alla persona (ad esempio: nomi, numeri di telefono e date di nascita, etc.); Inoltre devono essere rispettate le seguenti regole: - Vietare nomi di account predefiniti e rinominare account standard come, ad esempio, l'account amministratore; - Non mostrare a video la password (ma neanche PIN, passphrase, ecc., in generale: chiavi segrete) quando viene inserita e non dare indicazioni sulla sua lunghezza; - La password temporanea deve essere obbligatoriamente cambiata al primo log-on; - Deve essere forzato per tutti gli utenti, e particolarmente per gli amministratori, il cambiamento periodico della password; - La procedura di cambiamento della password deve impedire il riutilizzo di tutte le password precedentemente utilizzate e includere una procedura efficace che tenga conto di errori di inserimento; - Limitare il numero di tentativi consentiti in un determinato periodo di tempo o, alternativamente, effettuare il blocco dell'account per l'accesso da parte degli utenti finali dopo un determinato numero di tentativi; - Non consentire l'accesso fino a quando il processo di log-on sia stato completato con successo; - Convalidare le informazioni del log-on solo al completamento di tutti i dati di input. Se una condizione di errore si presenta, il sistema non deve indicare quale dato è corretto o incorretto; - Limitare il tempo entro il quale la procedura di log-on deve ultimarsi. In caso di eccesso, la procedura deve terminare; - Considerare di visualizzare le informazioni seguenti a valle di log-on con successo: a. data e ora del precedente log-on di successo; b. dettagliare ogni tentativo di log-on di insuccesso dall'ultimo log-on di successo; - La persistenza e la trasmissione delle password deve avvenire in modo protetto. Per quanto concerne la persistenza, la forma "hash salted" rappresenta la best practices; - Per contrastare la possibilità fornita dalla cache del browser nel consentire l'accesso, implementare un criterio che consente all'utente di scegliere di non

	salvare le credenziali o di forzare tale criterio come predefinito; - Tracciare sia gli accessi riusciti sia i tentativi di accesso falliti; - Eseguire l'Audit degli accessi non andati a buon fine per rilevare tentativi di hacking delle password; - Controllare e validare sempre l'indirizzo IP sorgente del client usato dall'utente: a. Se l'applicazione è destinata alla sola intranet, impedire accessi provenienti da indirizzi IP esterni alla propria LAN; b. Se l'applicazione è destinata ad utenti Internet ma la connessione arriva da IP esteri, prevedere un livello di controllo maggiore (es. una convalida via SMS su un numero di cellulare italiano, oppure più in generale per applicazioni critiche l'uso di meccanismi di autenticazione a due fattori); c. Se l'applicazione è destinata ad utenti Internet italiani, quando risulti tecnicamente fattibile si dovrebbe rilevare e impedire l'eventuale accesso da IP esteri basato su un servizio di Proxy Server situato in Italia. Tali requisiti dovrebbero essere periodicamente riesaminati per mantenere o rendere più sicura la password.

Altri criteri per l'autenticazione	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	La password costituisce la protezione minima obbligatoria per tutti gli accessi logici che richiedono l'identificazione dell'utente. Forme alternative più robuste di autenticazione quali one-time password o autenticazione forte a due fattori detta anche 2FA (pine e token o pin e impronta biometrica) o a tre fattori (pin, token e biometria) devono essere utilizzate per gli accessi amministrativi e per l'accesso a dati e sistemi critici secondo un approccio basato sull'analisi dei rischi. Per semplificare l'adozione dei meccanismi di autenticazione forte è possibile adottare soluzioni basate su sistemi gatekeepers che permettono di intermediare l'accesso privilegiato ai sistemi target senza che su di essi sia necessario alcun intervento. Per sistemi isolati o in ambiti IT ristretti, è opportuno preferire l'amministrazione di sistema esclusivamente attraverso l'accesso fisico locale al sistema, restringendo la possibilità di accesso remoto al minimo. In contesti più estesi la gestione remota è in genere indispensabile; in tal caso, a causa della sensibilità dei dati passati sulle interfacce amministrative, è necessario utilizzare canali crittografati, ad esempio, con tecnologia VPN o SSL, e nel caso del Remote Desktop di Windows è necessario abilitare la crittografia del protocollo RDP. Per ridurre ulteriormente il rischio, va considerato anche l'impiego di politiche IPSec per limitare la gestione remota dei computer collegati nella rete interna. In tutti i casi, il numero delle interfacce di amministrazione deve essere ridotto al minimo, disabilitando quelle non in uso.

Corretto utilizzo delle informazioni segrete di autenticazione	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	Tutti gli utenti devono essere informati dall'organizzazione sul corretto utilizzo delle informazioni segrete di autenticazione. Tutti gli utenti dovrebbero essere avvisati di: - evitare di tenere una registrazione (per esempio su carta, documenti software) delle informazioni segrete di autenticazione, salvo indicazione di un metodo di memorizzazione sicura; - modificare le informazioni segrete di autenticazione ogni qualvolta vi sia un'indicazione della loro possibile compromissione.