POLICY
ACCESSI PRIVILEGIATI

COD. C.21
VERSIONE N. 01 DEL 05.2022

CONTIENE:

1. **POLICY**

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE

PREMESSA

Con la dicitura "accessi privilegiati" si intende descrivere accessi o poteri speciali, conferiti ad uno o più soggetti (o macchine) che vanno ben oltre quelli garantiti al resto del personale. Gli accessi privilegiati consentono alle organizzazioni di proteggere la propria infrastruttura e le proprie applicazioni e di operare con efficienza, mantenendo comunque la riservatezza dei dati sensibili e dell'infrastruttura critica. Tutto ciò si traduce in pratiche che portano a consentire l'accesso ai soli dati di cui un utente ha davvero necessità per lo svolgimento della propria mansione. Allo stesso tempo, l'implementazione di un corretto sistema di gestione dei privilegi, porta alla individuazione di soggetti con "super privilegi" capaci quindi di gestire da una posizione di elevato grado gerarchico (in termini di sicurezza) gli account altrui.

TIPOLOGIE DI PRIVILEGI

I privilegi, come si accennava più sopra possono riguardare un utente fisico o un programma. Anche i software hanno quindi dei privilegi che consentono loro di scavalcare altri software nell'accesso ai dati e alle risorse. I tipi di account privilegiato solitamente rinvenibili in una scuola sono i seguenti:

- ACCOUNT RELATIVI AD AMMINISTRATORI DI SISTEMA: sono account con privilegi amministrativi nel contesto di un singolo sistema operativo od applicazione. Questi account sono utilizzati regolarmente dallo staff IT per la gestione di postazioni di lavoro, server, dispositivi di rete ed altri sistemi IT.
- ACCOUNT DI EMERGENZA: consentono di accedere ad uno o più sistemi con i privilegi di amministratore in caso di assenza dell'amministratore incaricato o qualora sia necessario sostituirsi a quest'ultimo.
- ACCOUNT DI APPLICATIVI: questi sono account utilizzati dalle applicazioni per accedere a database, mandare in esecuzione programmi o fornire accesso ad altre applicazioni.
- ACCOUNT PER UTENTI CON PRIVILEGI: sono account relativi ad utenti che dispongono di privilegi maggiori, oppure semplicemente diversi, rispetto a quelli di un utente ordinario.

ADEMPIMENTI

Al fine di gestire adeguatamente gli accessi è quindi necessario che ogni istituzione scolastica esegua una mappatura del personale e dei collaboratori esterni che accedono o che possono accede in via incidentale ai dati trattati (es: tecnico informatico dei computer). Una volta raccolti tutti i nomi sarà necessario individuare la mansione e il tipo di programmi e database a cui il soggetto deve necessariamente accedere per poter effettuare in modo autonomo ed efficace il proprio lavoro. Eseguito anche tale passaggio, sarà quindi necessario raggruppare, ove possibile, il personale in gruppi omogenei a cui attribuire i medesimi privilegi di accesso (es: i docenti), escludendo quindi, anche con gli strumenti informatici in uso presso la scuola, l'accesso ai database non necessari per la realizzazione della mansione lavorativa. Ultimati tutti i passaggi di cui sopra, sarà necessario pubblicare il mansionario in luogo digitalmente accessibile da tutto il personale al fine di consentire continui aggiornamenti e modifiche le quali, in base alle designazioni a soggetto autorizzato al trattamento, dovranno ritenersi vincolanti per tutti i destinatari. Si riporta in allegato un modello per la mappatura in questione.

PERICOLI

La creazione di privilegi di accesso è quindi una necessità per garantire la sicurezza e il rispetto della normativa.
Tuttavia, di contro, l'esistenza stessa di utenti con alti privilegi genera ulteriori rischi derivanti dal fatto che se un malintenzionato entra in possesso di credenziali privilegiate ottiene il potere di agire indisturbatamente sul sistema. Diventa quindi fondamentale proteggere in modo adeguato le credenziali e gli accessi dei soggetti privilegiati. Ma come?
A tal proposito, la letteratura di settore consiglia l'adozione di Sistemi di Gestione degli Account Privilegiati (PAM) così da ridurre i principali rischi a cui si potrebbe andare incontro. Gli esseri umani sono del resto il punto più debole di una infrastruttura informatica.
Si tratti di utenti privilegiati interni che utilizzano illegittimamente il proprio livello di accesso, oppure di aggressori informatici esterni che prendono di mira e si appropriano dei privilegi degli utenti per operare di nascosto come "interni privilegiati", gli esseri umani sono sempre

il punto più debole nella catena della sicurezza informatica. La gestione degli accessi privilegiati aiuta a fare in modo che gli operatori dispongano solo del livello di accesso richiesto per adempiere alle proprie mansioni. Una strategia PAM consente inoltre ai team di sicurezza di identificare le attività nocive legate all'utilizzo illegittimo dei privilegi e di reagire rapidamente per contrastarle.
Gli aggressori informatici, in particolare, aggrediscono i device e gli account in quanto ognuno di essi (laptop, smartphone, tablet, desktop, server, ecc.) contiene privilegi per impostazione predefinita. Gli account amministrativi incorporati consentono ai team IT di risolvere eventuali problemi a livello locale, ma come dicevamo introducono anche enormi rischi. Gli aggressori possono violare un "account admin" e sfruttarlo per saltare da una workstation all'altra, trafugare ulteriori credenziali, elevare i privilegi e spostarsi lateralmente nella rete finché non trovano quello che stanno cercando. Un programma PAM proattivo deve prevedere tra le altre cose l'approfondita rimozione dei diritti amministrativi locali dalle workstation, proprio per ridurre tali rischi. Come visto, quindi, un programma PAM è fondamentale per ottenere maggiore sicurezza. La capacità di monitorare e rilevare gli eventi sospetti in un ambiente è molto importante, ma l'azienda resterà vulnerabile in assenza di una chiara focalizzazione sul rischio maggiore: gli accessi privilegiati non gestiti, non monitorati e non protetti. Implementare un programma PAM nell'ambito di una più ampia strategia di sicurezza e gestione dei rischi consente alle organizzazioni di registrare tutte le attività correlate all'infrastruttura IT critica e alle informazioni sensibili, contribuendo così a semplificarne la verifica e i requisiti di conformità.

GESTIONE ACCOUNT PRIVILEGIATI

L'organizzazione deve proteggere l'accesso con privilegi alla priorità di sicurezza, a causa del potenziale impatto aziendale significativo (e alta probabilità) degli utenti malintenzionati che potrebbero compromettere questo livello di accesso.
Gli utenti malintenzionati, come si diceva, sfruttano spesso i punti deboli nella sicurezza dell'accesso con privilegi durante gli attacchi ransomware gestiti dall'uomo e il furto di dati mirati. Gli account di accesso con privilegi e i device sono così attraenti per gli utenti malintenzionati perché questi obiettivi consentono loro di ottenere rapidamente un ampio accesso alle risorse della scuola, spesso con un impatto aziendale rapido e significativo.
Per questo è necessario che ogni scuola, dopo aver individuato i soggetti con privilegi, proceda a tutelare i loro account.
Si riportano quindi le principali attività da eseguire così come indicate nella letteratura di settore (network):

1. Mantenere un inventario aggiornato di tutti gli account privilegiati. Assicurati di eseguire l'inventario degli account di gruppi così come sopra descritto ma ricorda anche di includere gli amministratori di sistema per i tuoi sistemi mainframe; banche dati; applicazioni di didattica a distanza e cloud. L'inventario dovrebbe identificare il proprietario di ciascun account privilegiato e le relative informazioni di contatto, nonché i componenti di sistema a cui è associato l'account e le loro posizioni principali nell'organigramma. Mantieni aggiornato il tuo inventario di account privilegiati e documenta tutte le modifiche.
2. Non consentire agli amministratori di condividere account. Rendi gli amministratori responsabili delle loro azioni personalizzando i loro account privilegiati. Utilizzare l'amministratore predefinito, gli account root e simili solo quando assolutamente necessario; è meglio rinominarli o disabilitarli a seguito del primo utilizzo.
3. Riduci al minimo il numero di account privilegiati. Idealmente, ogni amministratore dovrebbe avere un solo account privilegiato per tutti i sistemi.
4. Segui la policy password di cui al presente Sistema di Gestione di EUservice. In particolare, con riferimento agli account privilegiati, è opportuno richiedere la modifica delle password con frequenza maggiore rispetto a quella prevista per gli account ordinari.
5. Ove possibile, è opportuno prevedere l'autenticazione a più fattori per gli account con privilegi.
6. Utilizzare le best practice per l'elevazione dei privilegi. Quando gli utenti necessitano di diritti di accesso aggiuntivi devono seguire un processo di richiesta e approvazione documentato, su carta o utilizzando un ticket in un sistema di gestione degli accessi privilegiati. Dopo l'approvazione, elevare i privilegi dell'utente solo per il periodo di tempo necessario per eseguire l'attività specificata. Allo stesso modo, gli amministratori IT dovrebbero utilizzare i loro account privilegiati solo quando hanno bisogno delle autorizzazioni elevate per un'attività specifica, altrimenti dovrebbero usare i loro account regolari.
7. Monitora e registra tutte le attività privilegiate, senza abusarne. Per ridurre il rischio di violazioni dei dati e tempi di inattività, prestare attenzione alle azioni intraprese dagli utenti privilegiati utilizzando una varietà di tecniche di registrazione e monitoraggio. Implementa i controlli di sicurezza tradizionali, come i firewall e i controlli di accesso alla rete, che limitano l'accesso ai sistemi, in particolare i sistemi critici come il sistema di rilevamento delle intrusioni o la soluzione di gestione dell'identità e dell'accesso (IAM). Tutti questi sistemi dovrebbero avere la registrazione abilitata e dovresti anche abilitare la registrazione di sistema di eventi di

accesso/disconnessione e altre azioni di utenti privilegiati. È inoltre necessario il monitoraggio in tempo reale dell'attività degli utenti privilegiati e la capacità di allertare il personale appropriato in merito alle azioni critiche. La creazione di questi avvisi richiede che le informazioni nei registri siano chiare e comprensibili, il che non è nativamente il caso per molte piattaforme informatiche; tuttavia, puoi utilizzare un software di controllo IT che risolverà questo problema.

8. Estendi la protezione dell'accesso privilegiato oltre il firewall. Non dimenticare gli account associati a social media, applicazioni SaaS, partner, appaltatori e clienti; dovrebbero anche essere protetti in base alla politica di gestione dell'account privilegiato.

ALLEGATO 1
MODELLO DI MANSIONARIO CON PRIVILEGI

(da compilare a cura di DS, DSGA, Animatore Digitale)

COGNOME	NOME	MANSIONE	LIVELLO DI PRIVILEGIO	SISTEMI ACCESSIBILI
Tizio	Rosso	Docente	Livello 1	
Caio	Verde	DSGA	Livello 2	
Sempronio	Giallo	DS	Livello 3	

N.B: I campi sopra compilati sono meramente indicativi.