LICEO CLASSICO STATALE "G.M. DETTORI"
Cambridge International School
Via Pasquale Cugia, 2 – 09129 CAGLIARI

Tel. 070/308257–304270
Email capc03000v@istruzione.it Pec capc03000v@pec.istruzione.it
Codice univoco Ufficio UFT836 Codice Fiscale 80013430923

POLICY
ACCESSI PRIVILEGIATI

COD. C.20
VERSIONE N. 02 DEL 07.2024

CONTIENE:

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE
02	25.07.2024	REVISIONE E INTEGRAZIONE DEI TESTI CON MINORI CORREZIONI

PREMESSA

Con la dicitura **"accessi privilegiati"** si intende descrivere accessi o privilegi speciali, conferiti ad uno o più soggetti (ma anche macchine o software), che si estendono oltre quelli normalmente garantiti al resto del personale. Gli accessi privilegiati consentono alle organizzazioni di proteggere la propria infrastruttura informatica e le applicazioni, permettendo di operare in maniera efficiente mantenendo la riservatezza dei dati più sensibili e la sicurezza degli elementi critici della stessa. Ciò si traduce in pratiche che consentono l'accesso ai soli dati di cui un utente ha davvero necessità per lo svolgimento delle proprie mansioni. Allo stesso tempo, l'implementazione di un corretto sistema di gestione dei privilegi porta all'individuazione di soggetti con privilegi "superiori" in grado di gestire, da una posizione di più elevato grado gerarchico, gli account altrui.

TIPI DI PRIVILEGI

I privilegi, come precedentemente accennato, possono riguardare un utente ma anche un software: in questo caso i privilegi consentono loro di scavalcare altri software nell'accesso ai dati e alle risorse. I tipi di account con privilegi solitamente rinvenibili in una scuola sono i seguenti:

- **ACCOUNT RELATIVI AD AMMINISTRATORI DI SISTEMA:** account con privilegi amministrativi nel contesto di un singolo sistema operativo o 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 privilegi di amministratore in caso di assenza dell'amministratore incaricato o qualora sia necessario sostituirsi a quest'ultimo.
- **ACCOUNT DI APPLICATIVI:** account utilizzati dalle applicazioni per accedere a database, mandare in esecuzione programmi o fornire accesso ad altre applicazioni.
- **ACCOUNT PER UTENTI CON PRIVILEGI:** 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 dunque necessario che ogni istituzione scolastica esegua una mappatura del personale e dei collaboratori esterni che accedono o che possono accedere in via incidentale ai dati trattati (ad esempio: il tecnico informatico di una ditta esterna). Una volta raccolti tutti i nominativi, sarà necessario individuare la mansione e il tipo di programmi e database ai quali il soggetto deve necessariamente accedere per poter effettuare in modo autonomo ed efficace il proprio lavoro. Compiuto tale passaggio, sarà necessario raggruppare tali soggetti in gruppi omogenei (ad esempio: i tecnici informatici, i docenti, il personale amministrativo, ecc.) escludendo, anche tramite gli strumenti IT in uso presso la scuola, l'accesso ai database non necessari per lo svolgimento delle rispettive mansioni lavorative. Ultimati tali passaggi, 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.

RISCHI

La creazione di privilegi di accesso differenziati risulta una necessità per garantire la sicurezza e il rispetto della normativa. Tuttavia, l'esistenza stessa di utenti con privilegi elevati 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.
A tal proposito, la letteratura di settore consiglia l'adozione di sistemi di gestione degli account privilegiati (PAM) in modo 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 fa in modo che gli operatori dispongano solo del livello di accesso

richiesto per adempiere alle proprie mansioni. Una strategia PAM, inoltre, consente allo staff IT di identificare le attività dannose legate all'utilizzo illegittimo dei privilegi e di reagire rapidamente per contrastarle.
Gli aggressori informatici, in particolare, aggrediscono i dispositivi e gli account in quanto ognuno di essi (laptop, smartphone, tablet, desktop, server, ecc.) contiene privilegi per impostazione predefinita. Gli account amministrativi incorporati consentono allo staff IT di risolvere eventuali problemi a livello locale, ma come dicevamo introducono anche grandi 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 sistema PAM proattivo deve prevedere, tra le altre cose, l'approfondita rimozione dei diritti amministrativi locali dalle workstation, proprio per ridurre tali rischi.
In definitiva, un sistema PAM consente di ridurre i significativi rischi connessi al mancato monitoraggio e all'assenza di protezione, in sintesi alla cattiva gestione, degli accessi privilegiati. Tuttavia, ciò va implementato nell'ambito di una più ampia strategia di sicurezza delle informazioni e gestione dei rischi informatici, caratterizzata tanto da misure di carattere tecnico quanto di natura organizzativa, all'interno dell'istituzione scolastica.

GESTIONE DEGLI ACCOUNT PRIVILEGIATI

L'organizzazione deve proteggere gli account dotati di privilegi a causa del potenziale impatto che una loro violazione potrebbe avere sul proprio patrimonio informativo e sui dati personali archiviati. Gli utenti malintenzionati, come accennato, sfruttano spesso i punti deboli dell'infrastruttura IT nel condurre i propri attacchi. In questo senso, gli account di accesso con privilegi risultano attraenti per gli attaccanti in quanto consentono loro di ottenere in tempi rapidi un ampio accesso alle risorse e ai dati della scuola. Per questo è necessario che ogni istituzione, dopo aver individuato i soggetti con privilegi, proceda a tutelare i loro account.
Si riportano quindi le principali misure da mettere in atto secondo la letteratura di settore, prendendo come riferimento le reti interne ma non solo:

1. Mantenere un inventario aggiornato di tutti gli account privilegiati, includendo gli amministratori di sistema della rete scolastica, delle banche dati, delle piattaforme per la didattica digitale e delle applicazioni in 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. L'inventario va mantenuto aggiornato e tutte le modifiche documentate.
2. Non consentire agli amministratori di condividere gli account. Questi devono essere nominativi in modo da identificare univocamente i soggetti che li utilizzano responsabilizzandoli. Gli account di amministratore predefiniti (*admin* o *root*) vanno impiegati solo quando assolutamente necessario; sarebbe inoltre meglio rinominarli o disabilitarli successivamente al primo utilizzo.
3. Ridurre al minimo il numero di account privilegiati. Idealmente, ciascun amministratore dovrebbe avere un solo account privilegiato per tutti i sistemi.
4. Seguire la policy sulla gestione delle 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 tecnicamente 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, magari tramite 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 più elevate per una specifica attività, altrimenti dovrebbero usare i loro account ordinari.
7. Monitorare e registrare tutte le attività privilegiate limitatamente a quanto strettamente necessario. Per ridurre il rischio di violazioni dei dati, attenzionare le azioni intraprese dagli utenti privilegiati utilizzando una varietà di tecniche di registrazione e monitoraggio. Vanno dunque implementati componenti di sicurezza tradizionali, come i firewall e i controlli di accesso alla rete, che possono limitare l'accesso ai sistemi, in particolare quelli critici come il sistema di rilevamento delle intrusioni. Tutti questi sistemi dovrebbero registrare (*logging*) le attività di sistema, gli accessi degli utenti privilegiati, le operazioni di rete e altri eventi significativi dal punto di vista della sicurezza informatica, al fine di identificare minacce, vulnerabilità, anomalie e comportamenti

pericolosi, in seguito ai quali, se necessario, avvisare il personale competente.

8. Estendere le misure di sicurezza applicate agli accessi privilegiati al di fuori della rete interna. Non vanno dimenticati gli account dei profili social, delle piattaforme e applicazioni SaaS (*Software as a Service*) fruite in cloud, ecc.

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.