## Assessment Moderate

### Access Control

* **AC-2(1): *ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*** 
  + L’organizzazione impiega meccanismi automatizzati per supportare la gestione degli account del sistema
    - **Tale funzionalità non è implementata, ma sarebbe possibile inviare una notifica a seguito dell’eliminazione di un account.**
* **AC-2(2) :*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*** 
  + Il sistema informativo deve automaticamente rimuovere account temporanei/di emergenza dopo un intervallo di tempo definito dalla organizzazione
    - **Tale funzionalità non è implementata in quanto non è stato previsto l’uso di account temporanei / di emergenza.**
* **AC-2(3) :*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*** 
  + Il sistema informativo disabilita automaticamente account inattivi dopo un certo periodo di tempo stabilito
    - **Tale funzionalità non è implementata. Si potrebbe implementare tuttavia una serie di controlli automatici**
* **AC-2(4) :*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*** 
  + Il sistema informativo realizza automaticamente la valutazione per la creazione di account, la loro modifica, l’abilitazione, la disabilitazione e la rimozione, nonché le notifiche del personale.
* **AC-4 : INFORMATION FLOW ENFORCEMENT** 
  + Il sistema informativo fa l’enforcement di autorizzazioni approvate per controllare il flusso delle informazioni all’interno del sistema e tra i sistemi interconnessi in base al flusso di controllo stabilito dall’organizzazione
    - **Il sistema gestisce l’autorizzazione delle informazioni interne ed esterne in ingresso al sistema stesso, così come in accordo alle policy stabilite**
* **AC-5: SEPARATION OF DUTIES** 
  + L’organizzazione separa i vari compiti che spettano ai singoli individui, ne separa dunque i doveri e definisce le autorizzazioni di accesso del sistema al fine di supportare la separation of duties
    - **Il sistema separa i vari compiti che spettano ai singoli individui, nonché i doveri. Avendo solo due tipologie di utenti, la distinzione è netta in termini di autorizzazione, ed è quindi implementata.**
* **AC -6: LEAST PRIVILEGE**
  + L’organizzazione implementa il criterio del privilegio minimo, al fine di fornire le autorizzazioni e i privilegi minimi per permettere ad un dato utente di adempiere alle proprie funzionalità
    - **Il sistema prevede di assegnare ad ogni utente solo i permessi che gli sono strettamente necessari. L’amministratore ha infatti i permessi necessari a modificare solo quanto gli compete. Gli utenti della web app hanno i permessi necessari al normale utilizzo della web app e possono modificare solo gruppi e liste che gli appartengono.**
* **AC-6(1): *LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*** 
  + L’organizzazione autorizza esplicitamente l’accesso a funzionalità di sicurezza, sviluppate in hardware o software, per accedere ad informazioni protette.
    - **I file d’informazioni protette (Password e chiavi) sono opportunamente cifrati, e nessuno vi può accedere esplicitamente, se non il webserver stesso. Gli utenti dunque non dispongono di tale accesso.**
* **AC-6(2): *LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*** 
  + L’organizzazione richiede che gli utenti degli account del sistema, con un determinato ruolo, e con accesso ad informazioni o funzioni di sicurezza, utilizzino account non privilegiati per accedere ad informazioni non privilegiate
    - **È sicuramente vero che un utente registrato non ha permessi per accedere ad informazioni classificate. Al contempo un amministratore non ha accesso ad un suo profilo, o ad una selezione di giochi / piani tariffari. Un amministratore può solo accedere al pannello di amministrazione, ma per usufruire dei servizi non critici dell’utente, dovrebbe a sua volta essere un utente registrato.**
* **AC-6(5): *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*** 
  + L’organizzazione restringe gli account privilegiati unicamente a personale con ruolo ben definito nell’organizzazione
    - **Ciò risulta implementato, dato che solo i membri fidati dell’organizzazione accedono ai ruoli d’amministrazione (noi stessi)**
* ***AC-6(9): LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS***
  + *L’organizzazione proibisce accessi privilegiati a utenti non organizzativi*
    - ***Questo requisito è soddisfatto, in quanto, da consegna, solo membri appartenenti all’organizzazione, e fidati, possono rivestire ruoli amministrativi, e quindi privilegiati.***
* ***AC - 6(10): LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*** 
  + Il sistema informativo impedisce che utenti non privilegiati eseguano funzioni non privilegiate, come disabilitare o alterare misure di sicurezze
    - **Tale requisito è garantito dal fatto che utenti comuni non hanno accesso ad alcuna informazione o funzionalità di sicurezza che espongano il back-end. Questo sempre assumendo che gli account amministrativi non siano violati***.*
* **AC – 11: SESSION LOCK**
  + Il sistema informativo previene ulteriori accessi bloccando la sessione di un utente, a meno che esso non richieda di terminare la sessione. Una volta che l’utente decide di riaccedere, una nuova sessione viene ristabilita e mantenuta.
    - **Questo requisito viene implementato grazie alla gestione dei cookies. Se l’utente decide di fare il log-out i suoi cookies vengono però eliminati.**
* **AC – 11(1): *SESSION LOCK | PATTERN-HIDING DISPLAYS (no use)***
  + Il sistema nasconde tramite il blocco di sessione, informazioni precedentemente visibili tramite immagini pubbliche
* **AC – 12: SESSION TERMINATION**
  + Il sistema termina automaticamente una sessione utente dopo una richiesta dell’utente.
    - **Il sistema chiude la sessione di un utente solo se questo esplicita il log out**
* **AC – 17(1): *REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*** 
  + Il sistema informativo monitora e controlla metodi di accesso remoto
    - **Nella sua semplicità applicativa, il sistema controlla metodi di accesso remoto, tuttavia non ne traccia un log adeguato, per ogni tipo di comunicazione.**
* **AC – 17(2): *REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*** 
  + Il sistema informativo implementa meccanismi di cifratura per proteggere la confidenzialità e l’integrità dell’accesso remoto
    - **Questo è garantito dai protocolli SSH e OpenVPN, nonché LDAPS messi in gioco.**
* **AC – 17(3): *REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*** 
  + Il sistema informativo indirizza tutti gli accessi remoti attraverso un certo numero di punti di controllo della rete.
    - **Non è stata realizzata una estensiva gestione dei punti di accesso alla rete**
* **AC – 17(4): *REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*** 
  + L’organizzazione autorizza l’esecuzione di comandi privilegiati e accessi a informazioni di sicurezza tramite accessi remoti solo a chi ne necessita e documenta la ratio secondo cui tali accessi avvengono in un piano di sicurezza.
    - **L’accesso remoto è garantito solo ad utenti privilegiati, e il tutto è documentato nei requisiti non funzionali di sicurezza del sistema. Bisognerebbe tuttavia estendere i controlli di sicurezza nello sharing remoto, unico punto di accesso remoto per un utente non amministrativo**
* **AC-18(1):*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*  (no use)**
* **AC-19(5): *ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION (no use)***
* **AC – 21: INFORMATION SHARING** 
  + Il sistema facilita la condivisione di informazioni abilitando solo utenti autorizzati a determinare se l’accesso ad egli richiesto sia effettivamente garantito, e ne utilizza personale incaricato in caso
    - **Il sistema di sharing è parzialmente monitorato dall’amministratore di sistema di quella macchina. Naturalmente il sancire della sessione tramite un programma remoto, tramite VPN, è possibile solo se l’utente è effettivamente autorizzato.**

### Identification and authentication control

* **IA -2(2): *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*** 
  + Il sistema informativo implementa più fattori di autenticazione per l’accesso alla rete da parte di utenti non privilegiati
    - **Il sistema al momento richiede solo un fattore di autenticazione per accedere al webserver, ma vengono richiesti due fattori di autenticazione (credenziali e certificato/configurazione) per accedere all’host server.**
* **IA – 2(3): *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*** 
  + Il sistema informativo richiede più fattori per l’autenticazione locale di utenti privilegiati
    - **Il sistema implementa solo un fattore di autenticazione per accessi locali privilegiati (amministratori di sistema.)**
* **IA-2(8): *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*** 
  + Il sistema informativo implementa autenticazioni resistenti ad attacchi di replay in caso di accesso di utenti privilegiati
    - **L’autenticazione del webserver non è mutuamente autenticata, ma comunque cifrata su SSL. Il punto debole è in tal senso il webserver, mentre la comunicazione cifrata con host server, sia su SSH, che con openVPN dovrebbe garantire robustezza contro attacchi di Replay.**
* **IA-2(11): *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS - SEPARATE DEVICE*** 
  + Il sistema è in grado di implementare più meccanismi di autenticazione per utenti privilegiati e non, richiedendo una autenticazione tramite un dispositivo, e la seconda per mezzo di un secondo dispositivo
    - **Non è implementato tale requisito. Si potrebbe pensare di generare una otp tramite un oscillatore locale.**
* **IA-3 : DEVICE IDENTIFICATION AND AUTHENTICATION** 
  + Il sistema informativo identifica univocamente l’utente tramite identificativo e autenticazione tramite un particolare dispositivo prima di stabilire una connessione
    - **I protocolli basati su SSL garantiscono una fase di Handshaking prima di garantire la connessione, tuttavia questo avviene prima che l’utente stesso venga autenticato al sistema in quanto tale**
* **IA – 5(2): *AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*** 
  + Il sistema informativo realizza una autenticazione basata su PKI, validando i certificati ed eventualmente costruendoli, garantendo solo accessi a chi detiene i certificati distribuiti, associando l’identità del detentore al certificato rilasciato.
    - **Il sistema implementa una PKI, con CA, RA e certificati rilasciati.**
* **IA – 5(3): *AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION*** 
  + L’organizzazione richiede che il processo di registrazione atto a ottenere le credenziali sia condotto in persona o da una terza parte fidata.
    - **Attualmente la registrazione è gestita dalla stessa PKI, che si potrebbe definire un ente fidato, ma naturalmente in uno scenario reale dovremmo affidarci ad una infrastruttura standardizzata e certificata**

### System and communications protection control

* **SC- 2: APPLICATION PARTITIONING** 
  + Il sistema informativo separa le funzionalità utente, incluse interfacce utente, dalle funzionalità di gestione del sistema
    - **Il sistema informativo fornisce determinate viste per l’utente e determinate per l’amministratore. Ciò però deve essere completamente configurato per l’hostserver, e per la sessione che l’utente instaura con l’host server stesso.**
* **SC – 4: INFORMATION IN SHARED RESOURCES** 
  + Il sistema informativo previene trasferimenti di informazioni non autorizzate e non previste tramite la sessione di sharing
    - **Tale requisito è soddisfatto dal momento che l’unico punto d’accesso remoto disponibile, per l’utente, è la condivisione visiva. Tuttavia nel caso di SSH ci si affida sempre agli amministratori di sistema che ne fanno uso.**
* **SC – 7(3): *BOUNDARY PROTECTION | ACCESS POINTS*** 
  + L’organizzazione limita il numero di connessioni esterne al sistema informativo
    - **Tale requisito non è implementato, si potrebbe però inserire un controllo relativo all’accesso al sistema (lato webserver). Per l’hostserver tale limite sarebbe implementabile assumendo un massimo numero di richiedenti per macchina, in base alla banda e alle specifiche della macchina host.**
* **SC – 7(4): *BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*** 
  + L’organizzazione implementa una interfaccia di gestione per ogni servizio di telecomunicazione e ne stabilisce delle policy di flusso. Bisogna mantenere confidenzialità e integrità nella trasmissione di dati da tali interfacce e documentare ogni possibile eccezione per le policy di flusso
    - **Tale requisito non è implementato in quanto non è prevista una policy di gestione di flussi di informazioni, ne tantomeno sono previste particolari interfacce di gestione, se non quella amministratore webserver.**
* **SC – 7(5): *BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*** 
  + Il sistema informativo impedisce connessioni ad interfacce di default, ma concede solamente connessioni tramite eccezioni (deny all permit exceptions)
    - **Requisito non implementato. Avrebbe poco senso per un webserver, almeno dall’interfacciamento utente. Tuttavia non sono implementati particolari accessi selettivi per l’interfacciamento d’amministrazione, se non tramite credenziali.**
* **SC – 7(7): *BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*** 
  + Il sistema informativo, in congiunzione ad un dispositivo remoto, previene il dispositivo dall’accedere contemporaneamente al sistema e trasmettere le informazioni su di una rete esterna
    - **Tale requisito non è implementato**
* **SC – 8: TRANSMISSION CONFIDENTIALITY AND INTEGRITY** 
  + Il sistema informativo protegge la confidenzialità e l’integrità delle informazioni trasmesse
    - **Il sistema realizza tale requisito grazie ai protocolli sicuri implementati basati su SSL.**
* **SC – 8 (1): *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*** 
  + Il sistema implementa meccanismi crittografici per prevenire divulgazione non autorizzata di informazioni durante la trasmissione, a meno che non siano protetti in qualche modo
    - **Il sistema realizza tale requisito grazie ai protocolli sicuri implementati basati su SSL.**
* **SC – 10: NETWORK DISCONNECT** 
  + Il sistema informativo termina la connessione automaticamente quando termina la sessione di un utente
    - **Al momento non è implementato questo requisito**
* **SC – 17: PUBLIC KEY INFRASTRUCTURE CERTIFICATES** 
  + L’organizzazione implementa una PKI nella quale emette certificati e ne richiede da altre CA certificate
    - **Il sistema emette certificati e al momento non ne richiede, in quanto la CA è self signed. Tuttavia dovremmo implementare una catena fidata**
* **SC – 23: SESSION AUTHENTICITY** 
  + Il sistema protegge l’autenticità della comunicazione sulla sessione
    - **Il sistema al momento non prevede una doppia autenticazione su webserver (HTTPS), però i protocolli usati garantiscono autenticità sulla comunicazione**

|  |  |
| --- | --- |
|  |  |