**Ministero dell'Istruzione Università e Ricerca**
ISTITUTO COMPRENSIVO STATALE "G. PIOLA"
Via M. d'Azeglio, 41 – 20833 Giussano
Tel. 0362/850674 Fax 0362/850614 e mail MIIC83500A@pec.istruzione.it
e mail MIIC83500A@istruzione.it - C. F. 83012160152



ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

| ABSC_ID | | | Livello | Descrizione | Modalità di implementazione |
|---|---|---|---|---|---|
| 1 | 1 | 1 | M | Implementare un inventario delle risorse attive correlato a quello ABSC 1.4 | Inventario delle attrezzature informatiche: filtro basato sul mac-address dei dispositivi |
| 1 | 1 | 2 | S | Implementare ABSC 1.1.1 attraverso uno strumento automatico | |
| 1 | 1 | 3 | A | Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie. | |
| 1 | 1 | 4 | A | Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico. | |
| 1 | 2 | 1 | S | Implementare il "logging" delle operazione del server DHCP. | |
| 1 | 2 | 2 | S | Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite. | |
| 1 | 3 | 1 | M | Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete. | Aggiornare l'inventario quando nuovi pc vengono inseriti nella rete |
| 1 | 3 | 2 | S | Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete. | |
| 1 | 4 | 1 | M | Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP. | Se i pc hanno indirizzi IP fissi, prendere nota nell'inventario; se ottengono l'indirizzo IP da un server DHCP, riservare gli indirizzi IP nel server;<br>Per i dispositivi mobili autorizzati ad accedere alla rete, implementare in ordine di sicurezza:<br>• Un captive portal (inventario e comportamento degli utenti) |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | • Un filtro basato su Mac-address (inventario) |
| 1 | 4 | 2 | S | Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale. | |
| 1 | 4 | 3 | A | Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione. | |
| 1 | 5 | 1 | A | Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati. | |
| 1 | 6 | 1 | A | Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale. | |

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

| ABSC_ID | | | Livello | Descrizione | Modalità di implementazione |
|---|---|---|---|---|---|
| 2 | 1 | 1 | M | Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco. | Definire un elenco dei software che possono essere installati sui computer che accedono alla rete (tenendo conto delle licenze e della sicurezza).<br>Impedire l'installazione di software da parte di utenti non autorizzati (permettendo di usare SOLO utenze senza diritti amministrativi).<br>Privilegiare software open source.<br>Tra i software installi è indispensabile che ci sia un Antivirus che si aggiorni automaticamente.<br>Per i dispositivi personali questo non è possibile, per cui ci sono due possibilità:<br>• impedire l'uso di dispositivi personali o<br>• rendere rintracciabile il comportamento di chi li utilizza (captive portal) |
| 2 | 2 | 1 | S | Implementare una "whitelist" delle applicazioni autorizzate, | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi. | |
| 2 | 2 | 2 | S | Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale). | |
| 2 | 2 | 3 | A | Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate. | |
| 2 | 3 | 1 | M | Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. | L'utente amministratore del sistema controlla a scadenze regolari i computer per verificare che non siano stati installati software non previsti nell'elenco di cui al punto 2.1.1.M |
| 2 | 3 | 2 | S | Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop. | |
| 2 | 3 | 3 | A | Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch. | |
| 2 | 4 | 1 | A | Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete. | |

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

| ABSC_ID | | | Livello | Descrizione | Modalità di implementazione |
|---|---|---|---|---|---|
| 3 | 1 | 1 | M | Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi. | Gli utenti non hanno diritti amministrativi, è compito dell'utente amministratore impostare dei criteri di sicurezza. Definire dotazione software standard e criteri di gruppo nel domain controller attraverso l'active directory per gestire le richieste di autenticazione per la sicurezza |
| 3 | 1 | 2 | S | Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate. | |
| 3 | 1 | 3 | A | Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco. | |
| 3 | 2 | 1 | M | Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione. | Effettuare la configurazione tramite domain controller attraverso l'active directory<br>Indicare i criteri di sicurezza stabiliti:<br>• criteri di sicurezza sulla password (lunghezza, complessità, durata, ecc...)<br>• assegnazione diritti (quali applicazioni sono accessibili e quali no)<br>• opzioni di protezione sull'account administrator, guest |
| 3 | 2 | 2 | M | Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard. | Effettuare controlli periodici per individuare pc con problemi software (malware) e ripristinare la configurazione originale tramite "immagine d'installazione". Se un virus o qualunque azione malevola infetti la macchina questa va riformatta e portata ai valori standard. |
| 3 | 2 | 3 | S | Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti. | |
| 3 | 3 | 1 | M | Le immagini d'installazione devono essere memorizzate offline. | Creare e conservare su supporti locali come pen-drive, DVD, disco di rete e server, cartelle di rete accessibili solo a utenti amministratori, le immagini di installazione. Per i computer privi di immagine di installazione, poiché le postazioni non prevedono particolari installazioni, in caso di necessità saranno riformattate e successivamente saranno installati i software necessari. |
| 3 | 3 | 2 | S | Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati. | |
| 3 | 4 | 1 | M | Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli | Protocollo SSH, da attivare sulla connessione remota |

| | | | | | |
|---|---|---|---|---|---|
| | | | | intrinsecamente sicuri, ovvero su canali sicuri). | |
| 3 | 5 | 1 | S | Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati. | |
| 3 | 5 | 2 | A | Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert. | |
| 3 | 5 | 3 | A | Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica. | |
| 3 | 5 | 4 | A | I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle. | |
| 3 | 6 | 1 | A | Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate. | |
| 3 | 7 | 1 | A | Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard. | |

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

| ABSC_ID | | | Livello | Descrizione | Modalità di implementazione |
|---|---|---|---|---|---|
| 4 | 1 | 1 | M | Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche. | Utilizzare uno o più strumenti (gratuiti) di scansione delle vulnerabilità, per esempio:<br>• MBSA per sistemi windows<br>• OpenVAS per le reti<br><br>o equivalenti |
| 4 | 1 | 2 | S | Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura. | |
| 4 | 1 | 3 | A | Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project). | |
| 4 | 2 | 1 | S | Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità. | |
| 4 | 2 | 2 | S | Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità | |
| 4 | 2 | 3 | S | Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile. | |
| 4 | 3 | 1 | S | Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione. | |
| 4 | 3 | 2 | S | Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente. | |
| 4 | 4 | 1 | M | Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza. | Utilizzare sempre versioni aggiornate |
| 4 | 4 | 2 | S | Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione | |
| 4 | 5 | 1 | M | Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni. | Impostare gli aggiornamenti automatici di SO e sw |
| 4 | 5 | 2 | M | Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità. | Aggiornare manualmente e periodicamente i dispositivi non connessi alla rete per cui non è possibile impostare l'aggiornamento automatico. |
| 4 | 6 | 1 | S | Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite. | |
| 4 | 7 | 1 | M | Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio. | In base ai risultati delle scansioni, operare con i rimedi necessari. Nel caso fossero riscontrati dei problemi questi saranno risolti attraverso l'installazione di patch o ripristinando il dispositivo |
| 4 | 7 | 2 | S | Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | sono cambiate, con la conseguente modifica del livello di rischio. | |
| 4 | 8 | 1 | M | Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.). | Stabilire un piano di gestione dei rischi (chi fa cosa e quando). Sono state adottate tutte le precauzioni per abbassare al minimo il rischio di sicurezza di ciascun dispositivo utilizzato dall'amministrazione |
| 4 | 8 | 2 | M | Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche. | Il pericolo è molto basso avendo già previsto che ogni dispositivo si aggiorni automaticamente applicando in tal modo anche le eventuali patch di sicurezza. |
| 4 | 9 | 1 | S | Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione. | |
| 4 | 10 | 1 | S | Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio. | |

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. | Gli account utilizzati per accedere al dispositivo non sono di tipo amministrativo. Nel caso lo fossero questi vanno cambiati con accessi di livello più basso.<br>Axios: i prodotti Axios consentono, per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile (CRUD).<br>Il sistema Axios Cloud consente le medesime funzionalità. |
| 5 | 1 | 2 | M | Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. | L'accesso amministrativo ai dispositivi sarà utilizzato solo per operazioni di manutenzione.<br>Non comunicare le password di utenze amministrative a persone diverse dagli amministratori (tenere una copia delle password in busta chiusa in cassaforte)<br>Axios: i prodotti Axios registrano in automatico ogni accesso effettuato al sistema.<br>Il sistema Axios Cloud possiede un log puntuale di tutte le operazioni effettuate e consente l'accesso allo stesso a qualsiasi richiesta proveniente dall'utente o dalle autorità preposte |

| | | | | | |
|---|---|---|---|---|---|
| 5 | 1 | 3 | S | Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa. | Axios: per Axios Cloud vedi punto 5.1.1.M |
| 5 | 1 | 4 | A | Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento. | Axios: i prodotti Axios registrano su tabella di log ogni singola operazione effettuata sui dati. La conservazione di tale log dipende dallo spazio presente sul disco del server della scuola e dalle impostazioni fornite dalla scuola stessa sulla grandezza massima del file di LOG.<br>Il LOG gestito da Axios Cloud viene storicizzato ogni 3 mesi e collocato in stato di READONLY. Dopo 12 mesi viene cancellato |
| 5 | 2 | 1 | M | Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. | Tenere un registro delle utenze amministrative: predisporre un elenco degli utenti amministrativi e relativa password assegnata. Tale elenco dovrà essere custodito in cassaforte e messo a disposizione solo al personale addetto alla manutenzione dei dispositivi. Le password dovranno essere non banali e di almeno 14 caratteri di lunghezza.<br>Axios: Tramite la gestione utenti di Axios è possibile verificare in qualsiasi momento lo status delle utenze, non ultima la data di ultimo accesso.<br>Axios Cloud consente in ogni istante, da parte dell'amministratore di sistema, di verificare lo status delle utente. |
| 5 | 2 | 2 | A | Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga. | |
| 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. | Sui nuovi computer disattivare o sostituire la password dell'utente administrator (al suo posto utilizzare le utenze con diritti amministrativi creati in base al punto 5.1.1.M) |
| 5 | 4 | 1 | S | Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa. | Axios: Vedi punto 5.1.4.A<br>L'aggiunta o la soppressione di un'utenza amministrativa sono operazioni che vengono svolte sul DB e quindi regolarmente registrate nel file di LOG.<br>Anche in Axios Cloud l'operazione viene regolarmente tracciata all'interno del file LOG. |
| 5 | 4 | 2 | S | Generare un'allerta quando viene aggiunta un'utenza amministrativa. | |
| 5 | 4 | 3 | S | Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa. | |
| 5 | 5 | 1 | S | Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa. | |

| | | | | | |
|---|---|---|---|---|---|
| 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. | |
| 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). | Impostare degli adeguati criteri di sicurezza delle password amministrative (lunghezza)<br>Axios: consente di definire una serie di parametri che possono rendere sicure le credenziali di accesso ai propri programmi fornite:<br>1. Verifica o meno del doppio accesso<br>2. Inserimento data generale di scadenza password<br>3. Numero di gg massimi per la validità del codice di accesso<br>4. Numero massimo di gg da ultimo accesso per consentire ancora lo stesso<br>5. Lunghezza minima del codice di accesso (in questo caso 14)<br>6. Numero minimo dei caratteri minuscoli<br>7. Numero minimo dei caratteri maiuscoli<br>8. Numero minimo dei caratteri numerici<br>9. Numero minimo dei caratteri speciali<br>In Axios Cloud verranno a breve implementate le stesse funzioni |
| 5 | 7 | 2 | S | Impedire che per le utenze amministrative vengano utilizzate credenziali deboli. | Axios: i parametri definiti in Axios al punto precedente (5.7.1.M) consentono di effettuare questo controllo in automatico impedendo di fatto l'utilizzo di credenziali deboli. |
| 5 | 7 | 3 | M | Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging). | Impostare degli adeguati criteri di sicurezza delle password amministrative (sostituzione frequente)<br>Axios: Vedi parametri indicati nel punto 5.7.1.M |
| 5 | 7 | 4 | M | Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history). | Impostare degli adeguati criteri di sicurezza delle password amministrative (rendere impossibile il riutilizzo)<br>Axios: gestisce lo storico password impedendo di fatto che possa essere riutilizzato un codice di accesso già utilizzato in precedenza.<br>In Axios Cloud sarà a breve implementata le medesima funzione<br>Impostare degli adeguati criteri di sicurezza delle password amministrative (rendere impossibile il riutilizzo) |
| 5 | 7 | 5 | S | Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova. | |
| 5 | 7 | 6 | S | Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi. | |

| | | | | | |
|---|---|---|---|---|---|
| 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. | Axios consente, per le funzioni particolarmente delicate, di inserire un ulteriore codice di accesso. L'utente quindi dopo aver effettuato il login dovrà inserire anche un ulteriore codice di accesso per poter effettuare la funzione scelta. |
| 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. | |
| 5 | 10 | 1 | M | Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse. | Creare per gli amministratori utenze senza diritti amministrativi da utilizzare nelle attività che non li richiedono<br>Axios: la gestione degli amministratori rispetto alle normali utenze viene fatta, in Axios, tramite la gestione dei livelli (1-9 9=amministratore) e le tipologie di accesso per ogni utente/funzione (5.1.1M) |
| 5 | 10 | 2 | M | Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. | Impostare degli adeguati criteri di sicurezza delle password amministrative (rendere impossibile il riutilizzo)<br>Come da punto 5.1.1M<br>Axios: In Axios, ad ogni utenza, è legata la relativa anagrafica del personale gestita all'interno dei programmi stessi<br>Anche in Axios Cloud le utenze di accesso sono legate a precise anagrafiche presenti nel sistema |
| 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. | Fare in modo che tali password siano a conoscenza di una sola persona per volta (conservare le password in busta chiusa in cassaforte per emergenze) |
| 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). | |
| 5 | 11 | 1 | M | Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza. | Le credenziali amministrative sono conservate in un luogo sicuro<br>Come da punto 5.10.3M<br>Axios: tali credenziali sono gestite all'interno della base dati, l'accesso alla stessa è consentito solo tramite i programmi Axios e quindi secondo le regole di sicurezza enunciate in questo documento.<br>Anche per Axios Cloud vale lo stesso principio con l'aggiunta che la base dati non è in alcun modo accessibile a nessuno se non tramite programmi Axios e quindi secondo le regole indicate nel presente |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | documento. |
| 5 | 11 | 2 | M | Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette. | Non di competenza in quanto non si utilizzano per l'accesso 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. | Utilizzare sempre Antivirus (e tenerli aggiornati) |
| 8 | 1 | 2 | M | Installare su tutti i dispositivi firewall ed IPS personali. | Firewall personale già presente in windows<br>Installare sui computer uno strumento (gratuito) IPS (Intrusion Prevention System) personali |
| 8 | 1 | 3 | S | Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati. | |
| 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. | |
| 8 | 2 | 2 | S | È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale. | |
| 8 | 2 | 3 | A | L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud. | |
| 8 | 3 | 1 | M | Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali. | BYOD, utilizzo di dispositivi personali dei docenti registrati nel filtro mac-address o nel captive portal |
| 8 | 3 | 2 | A | Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni. | |
| 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. | |
| 8 | 4 | 2 | A | Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi. | |
| 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. | |
| 8 | 5 | 2 | A | Installare sistemi di analisi avanzata del software sospetto. | |
| 8 | 6 | 1 | S | Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione. | |
| 8 | 7 | 1 | M | Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. | Sulle ultime versioni di windows (da windows 7 in poi) è disattivato. |
| 8 | 7 | 2 | M | Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. | Modificare le impostazioni di sicurezza dei software che utilizzano macro (es. MS Office) |
| 8 | 7 | 3 | M | Disattivare l'apertura automatica dei messaggi di posta elettronica. | Utilizzare versioni aggiornate di client di posta elettronica<br>Modificare le impostazioni |
| 8 | 7 | 4 | M | Disattivare l'anteprima automatica dei contenuti dei file. | Utilizzare versioni aggiornate di client di posta elettronica<br>Modificare le impostazioni |
| 8 | 8 | 1 | M | Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione. | Scoraggiare l'utilizzo di supporti rimovibili, utilizzare piuttosto il cloud.<br>Alcuni antivirus permettono la scansione automatica, ma se è disabilitato l'avvio automatico non dovrebbe essere necessario |
| 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. | Utilizzare filtri antispam (ad esempio Spamfighter)<br>Filtrato il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, attraverso l'impiego di strumenti antispam |
| 8 | 9 | 2 | M | Filtrare il contenuto del traffico web. | Utilizzare servizi DNS filtrati, come OpenDNS (208.67.222.123 e 208.67.220.123)<br>Utilizzare a livello centralizzato un Firewall/proxy opportunamente configurato |
| 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). | Utilizzare a livello centralizzato un Firewall/proxy opportunamente configurato |
| 8 | 10 | 1 | S | Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento. | |
| 8 | 11 | 1 | S | Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate. | |

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. | Creare immagini del disco dei computer da conservare offline come punto 3.3.1<br>Utilizzare un NAS (Network Attached Storage) sul quale effettuare automaticamente i backup tramite software come Cobian backup (gratuito)<br>Axios: prevede un sistema automatico e non presidiato di copie del proprio DB presente localmente sul server della scuola.<br>Il sistema prevede inoltre l'invio automatico a tre indirizzi mail e/o a tre numeri di cellulare, di un messaggio sull'esito dell'esecuzione delle copie.<br>Il sistema di backup Axios prevede anche la possibilità di effettuare un backup non solo della base dati ma anche di una specifica cartella condivisa sul server della scuola stessa e tutte le sue sottocartelle.<br>Axios Cloud effettua<br>- Backup del logo delle transazioni ogni 30 minuti<br>- Backup completo ogni giorno alle 2.00 circa<br>- Retention dei backup 8/10 gg |
| 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. | Axios: il sistema di backup effettua il salvataggio della base dati. L'installazione dei programmi è possibile in qualsiasi momento dal sito internet di Axios, così come l'eventuale ripristino del motore di database utilizzato (Sybase ver. 8.0.2.4495)<br>Axios Cloud oltre ad esser dotato di un sistema di backup con retention di 8/10gg dei dati ed un sistema di retention di 2/4 gg delle immagini dell'intera infrastruttura e configurato con un sistema di DR Real Time che consente il ripristino di un subset depotenziato dell'infrastruttura madre entro 24/48 ore dal Fault completo del sistema principale garantendo, quindi, la continuità di servizio con uno SLA del 98.98 % circa |
| 10 | 1 | 3 | A | Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore. | Axios: consente alle scuole di poter effettuare, nella medesima sessione di copie ed in modo completamente automatico, oltre alla copia sul disco del server, anche una copia su unità fisica esterna e, qualora la scuola abbia acquistato il servizio, anche un backup cloud che garantisce l'assoluta salvaguardia e recuperabilità dei dati.<br>I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery |
| 10 | 2 | 1 | S | Verificare periodicamente l'utilizzabilità delle copie mediante | Axios: effettua una verifica al termine della creazione del file |

| | | | | | |
|---|---|---|---|---|---|
| | | | | ripristino di prova. | compresso contenente le copie. La simulazione del ripristino dei dati è comunque buona pratica da adottare con frequenza almeno mensile. |
| 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. | Prevedere la cifratura dei dati durante la creazione del backup (Cobian lo permette)<br>Utilizzare uno spazio sul cloud per effettuare la copia settimanale automatica dei dati<br>Axios: Il backup effettuato è un file ZIP criptato che può essere ripristinato solo dalla scuola che lo ha generato. Questo consente di rimanere a norma anche con l'utilizzo di Backup Cloud di Axios. Axios Cloud consente l'accesso ai dati solo ai legittimi proprietari degli stessi. Tutte le transazioni Axios Cloud sono cifrate e protette da protocollo HTTPS |
| 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. | È possibile utilizzare per il backup un supporto rimovibile (disco esterno usb) ma ciò rende l'operazione non automatica perché richiede intervento umano.<br>In alternativa impostare nel software di backup che il backup venga effettuato con le credenziali di un altro utente in modo che un virus non possa poi accedere alle copie<br>Axios: vedi quanto indicato nel punto 10.1.3.A, in particolare è possibile effettuare una copia su un disco esterno, ad esempio, e poi isolare quest'ultimo dal sistema semplicemente scollegando il cavo dal server.<br>I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery |

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 | Effettuare la cifratura su tutti i dati |
| 13 | 2 | 1 | S | Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti | |
| 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. | |
| 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. | |
| 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. | |
| 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. | |
| 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. | |
| 13 | 6 | 2 | A | Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line. | |
| 13 | 7 | 1 | A | Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto. | |
| 13 | 8 | 1 | M | Bloccare il traffico da e verso url presenti in una blacklist. | Utilizzare a livello centralizzato un Firewall/proxy opportunamente configurato |
| 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. | |

IL DIRIGENTE SCOLASTICO
Prof. Roberto Di Carlo