LICEO STATALE " G. Milli "

Via G.Carducci, 38 – TERAMO

Misure minime di sicurezza ICT

PROT. N.7630/VI.9 **ANNULLA SOSTITUISCE IL PRECEDENTE DI PARI NUMERO E DATA**

Controlli ABSC (AgID Basic Security Controls)

che devono essere implementati per ottenere un determinato livello di sicurezza.

Si identificano 3 livelli:

1. M (Minimo) al di sotto il quale nessuna amministrazione può scendere
2. S (Standard) che costituisce la base di riferimento nella maggior parte dei casi
3. A (Alto) che potrebbe essere un obiettivo a cui tendere

Sulla base della circolare MIUR.AOODGCASIS.REGISTRO UFFICIALE(U).0003015.20-12-2017 nella quale si legge:

"Livelli di applicazione

Le misure di sicurezza, in funzione della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, possono essere implementate in modo graduale facendo riferimento ai livelli di seguito riportati.

- *Minimo: è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.*

***Questo livello può ritenersi sufficiente per gli istituti scolastici**…"*

le misure minime che si intende adottare appartengono tutte al livello M (Minimo)

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

Il livello minimo prevede l'implementazione, l'aggiornamento e la gestione dell'inventario di tutti i sistemi di rete (compresi i dispositivi di rete stessi) registrando almeno l'indirizzo IP.

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Realizzazione di una web application con link al sito istituzionale dell'Istituto e accesso riservato, per la gestione di un database sul quale registrare tutti i dispositivi fissi connessi alla rete. Attualmente i dispositivi sono inventariati ciascuno con il numero IP di rete e suddivisi per subnet di appartenenza.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	La web application prevede un facile aggiornamento manuale dell'inventario e dei dispositivi connessi 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.	Per tutti i dispositivi inventariati viene indicato. oltre al nome della macchina, l' indirizzo IP. Viene inoltre chiarito se il dispositivo è un pc fisso oppure portatile.

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

Il livello minimo prevede la realizzazione dell'elenco dei software autorizzati (e relative versioni), con regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzati. L'installazione di software non presenti nell'elenco è vietata.

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.	Sullo stesso database che gestisce i dispositivi hardware saranno registrati i software utilizzati sui dispositivi informatici in dotazione dell'istituto.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	E' una misura già implementatadai responsabili dei servizi di assistenza tecnica

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

Il livello minimo di questa classe di controlli prevede le definizione di configurazioni standard per tutti i sistemi e il rispetto di tali standard nelle fasi di installazione o ripristino dei sistemi. Le immagini di installazione dei sistemi devono essere memorizzate offline e tutte le operazioni di amministrazione remota devono essere eseguite tramite connessioni protette.

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Per la protezione delle configurazioni hardware e software dei dispositivi informatici sono già adottate misure adeguate al fine di evitare interventi di manomissione delle configurazioni stesse. Su gran parte dei computer utilizzati per la didattica viene utilizzato un software specifico di freezing.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	E' impossibile definire ed impiegare un'unica configurazione standard. Alcune configurazioni, relative ad apparati di tipo e tecnologie differenti, sono già esistenti.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	In caso di malfunzionamenti e/o guasti vengono ripristinate le configurazioni standard.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini di installazione, alcune eseguite con software proprio del Sistema Operativo, altre eseguite con software esterno, sono conservate su un disco rigido esterno.
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 intrinsecamente sicuri, ovvero su canali sicuri).	La sicurezza informatica riguardo a possibili intrusioni viene assicurata da un sistema rigoroso di amministrazione remota attuato attraverso robuste credenziali di accesso. Sarà una raccomandazione contenuta nelle best practices che saranno rivolte agli utenti che a vario titolo hanno necessità di essere autenticati quella di: • utilizzare password complesse • non condividere mai le credenziali • disattivare le credenziali relative ad account non più in uso • cambiare, laddove non previsto dalla procedura, frequentemente la password.

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

Il livello minimo prevede la ricerca delle vulnerabilità tramite strumenti automatici ad ogni modifica della configurazione; detti strumenti devono fornire agli amministratori di sistema report con indicazione delle vulnerabilità più critiche. Non solo i sistemi devono essere aggiornati, ma anche gli stessi strumenti di scansione. Questa classe di controlli impone l'installazione sistematica di patch e contromisure idonee a contrastare le vulnerabilità riscontrate. Va inoltre implementato un adeguato piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati; tale piano deve anche prevedere le azioni da svolgere per la risoluzione delle vulnerabilità individuate.

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.	La rete informatica dell'Istituto è costituita da due sottoreti ciascuna indipendente dalle altre. Due reti riguardano la didattica e una l'amministrazione. Nelle due sottoreti già attualmente è previsto l'aggiornamento dei sistema operativo e dei programmi applicativi, non appena l'aggiornamento è disponibile. Questa policy consente di prevenire i rischi derivanti dall'obsolescenza del software, dei bug in esso contenuti e dagli attacchi che utilizzino le vulnerabilità che ne derivano. Per la sicurezza informatica della rete dell'area amministrativa, evidentemente quella più critica, ci vogliamo dotare di un software per la scansione di vulnerabilità e stiamo valutando un software in ambiente Windows in grado di individuare potenziali problematiche di sicurezza.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Il software che stiamo valutando e di cui intendiamo dotarci viene aggiornato costantemente. Esso prevede l'installazione automatica di patch e aggiornamenti software sia per il sistema operativo sia per le applicazioni.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	
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.	Nel nostro Sistema informativo, non sono presenti sistemi separati dalla rete per quel che riguarda l'area amministrativa. Nell'area didattica si presentano situazioni in cui un certo numero di docenti e alunni si collegano alla rete wifi con i propri dispositivi. La vulnerabilità, essendo le connessioni occasionali, sono limitate.
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.	Sarà una raccomandazione contenuta nelle best practices che saranno rivolte al personale tecnico incaricato. Tutte le best practices riguardanti le misure di sicurezza delle ICT saranno pubblicate sul sito istituzionale della Scuola.

ABSC_ID			Livello	Descrizione	Modalità di implementazione
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.).	La valutazione della vulnerabilità sarà realizzata con riunioni periodiche del personale tecnico e amministrativo incaricato. Nel corso di tali riunioni verranno programmati gli interventi di manutenzione periodica e l'aggiornamento dei software in uso. Già attualmente si dà grande importanza all'aggiornamento dei sistemi operativi da effettuare non appena gli aggiornamenti si rendono disponibili.Successivamente i controlli saranno calendarizzati (ad esempio con periodicità mensile) e si attribuirà un unico livello di priorità elevato a tutte le vulnerabilità, considerando la difficoltà oggettiva di riconoscere il loro grado di criticità
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.	

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Il livello minimo della classe di controlli relativa agli amministratori di sistema definisce una specifica policy di gestione degli utenti con diritti amministrativi, che disciplini i limiti nei privilegi attribuiti e l'inventario dei profili abilitati. Tale policy prevede tutte le accortezze che si rendono necessarie per l'adeguata gestione degli amministratori di sistema, dai controlli sulle scadenze delle password alla creazione di profili nominativi e individuali (non generici). E' curioso rilevare come in questa classe di controlli, le azioni relative al tracciamento dei log degli amministratori siano definite come livello "standard", mentre rappresentano un obbligo di legge sancito da un provvedimento del Garante Privacy sugli amministratori di sistema del 2008.

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.	Misura attualmente già implementata. I privilegi di amministratore sono riservati esclusivamente a personale autorizzato dal Dirigente e di comprovata competenza tecnica. La gestione delle password è affidata sempre a personale competente. Le password saranno riportate in un apposito registro conservato in cassaforte presso l'ufficio amministrativo.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	È necessario identificare il personale incaricato in modo chiaro. Tutto il Personale amministrativo ha partecipato al Corso sulla sicurezza ICT organizzato dal MIUR.
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.	Procedura già prevista.
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).	Procedura già prevista, bisogna adeguare alla lunghezza di 14 caratteri. Quest'ultima specifica sarà oggetto di una apposita raccomandazione nelle best practices e sarà applicata, salvo nei casi in cui si verifichi un impedimento da parte del software applicativo (ad esempio, uin programma che prevede una password con al massimo 8 caratteri).
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Procedura già prevista. Nel caso dei pacchetti software utilizzati in segreteria, il password aging viene gestito automaticamente.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Sarà una raccomandazione contenuta nelle best practices che saranno rivolte al personale incaricato.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Procedura già prevista.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Procedura già prevista.
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.	Procedura già prevista.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le password saranno riportate in un apposito registro conservato in cassaforte presso l'ufficio amministrativo.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non vengono utilizzati certificati digitali.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

Il livello minimo impone l'installazione e l'aggiornamento automatico di sistemi antimalware, firewall e Intrusion Prevention Systems (IPS). Si deve disabilitare inoltre l'esecuzione automatica di tutti quei sistemi che potrebbero inavvertitamente attivare una minaccia (es. apertura degli allegati delle email, esecuzione di macro, eseguibili lanciati da chiavette USB, ecc). Sempre in chiave preventiva, si deve prevedere l'adozione di strumenti filtraggio dei contenuti, sia sulla navigazione internet che sulla posta elettronica.

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.	La difesa contro il malware è attuata oltre che con un antivirus con le funzionalità di prevenzione di vari tipi di codice dannosi, con l'installazione di appositi software anti-malware di scansione periodica dei dispositivi. Antivirus e software di scansione saranno aggiornati costantemente.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Le versioni recenti di Windows hanno tutte un firewall attivo perdefault. Per quanto riguarda gli IPS (Intrusion Prevention System), fanno parte integrante di molti sistemi antivirus.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L'uso limitato e responsabile di dischi esterni e/o penne USB sarà una raccomandazione delle best practices.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Raccomandazioni che saranno contenute nelle best practices. Per il contrasto al malware si punterà molto sulla formazione degli addetti, al fine di diffondere la cultura della sicurezza informatica e favorire una maggiore consapevolezza dei rischi (istruzioni per l'apertura dei messaggi email e dei loro allegati, segretezza e custodia delle password, blocco schermo, divieto di installazione software ecc.)
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	La maggior parte delle funzioni anti-malware viene svolta dai programmi antivirus. Ad abundantiam sarà utilizzato un software antispam.
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.	
8	9	2	M	Filtrare il contenuto del traffico web.	
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).	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

Il livello minimo di sicurezza contempla una copia almeno settimanale delle informazioni strettamente necessarie per il completo ripristino del sistema. Si pone una certa attenzione anche alla riservatezza delle informazioni contenute nelle copie di sicurezza, tramite adeguata protezione fisica o mediate cifratura delle informazioni sottoposte a salvataggio. Infine, è necessario garantire che almeno una delle copie non sia permanentemente accessibile dal sistema stesso, onde evitare che eventuali attacchi al sistema possano coinvolgere anche le sue 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.	La copia degli archivi gestiti con la piattaforma AXIOS in locale viene già attuata automaticamente con frequenza giornaliera. Di altri dati riguardanti le attività dell'Istituto o archivi gestiti in remoto da fornitori di software (p.e. Argo-Registro elettronico) viene effettuato backup automatico periodico.
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.	Le copie interne vengono custodite in locali riservati e accessibili solo a personale selezionato. Le web application in uso della Scuola, utilizzano connessioni sicure (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.	Viene utilizzato il sistema delle copie pari-dispari. Un eventuale attacco può coinvolgere una sola tipologia di copia di sicurezza

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

Il livello minimo da garantire stabilisce di effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza, ai quali applicare una protezione crittografica. Inoltre, si deve prevedere il blocco del traffico da e verso url presenti in una blacklist.

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	Non si individuano all'interno del sistema informativo dell'Istituto dati con particolari requisiti di riservatezza. I dati del registro elettronico che vengono gestiti online sono protetti tramite una connessione HTTPS.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Questa misura verrà implementata nell'area didattica con un sistema di content filtering OpenDns. Non si ritiene al momento necessario attuare questa misura nell'area amministrativa.

Teramo 23 dicembre 2017

Il Dirigente Scolastico

Prof.ssa Stefania Nardini