CERTIFICAZIONE DELLA SUSSISTENZA DELLE MISURE MINIME DI SICUREZZA PREVISTE AGLI ARTT. 33 ss. D.Lgs 196/2003 ALL'INTERNO DI UNA INFRASTRUTTURA INFORMATICA DEPUTATA AL TRATTAMENTO DIGITALE DI DATI PERSONALI

L'azienda scrivente Studio AG.I.COM. S.r.l.

- Vista l'esistenza, tra Studio AG.I.COM. S.r.l. ed il Titolare del trattamento di seguito meglio identificato, di un rapporto contrattuale sottostante denominato "AMMINISTRATORE DI SISTEMA".

- Letto il contenuto del Punto 25 del Capitolato tecnico (Allegato B al D.Lgs. 196/2003) recante: "Il Titolare che adotta le misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente capitolato tecnico."

Rilascia la presente certificazione, che costituirà allegato al Documento Programmatico sulla Sicurezza del Titolare, per le finalità previste dalla legge.

Data di esecuzione del sopralluogo: 22/03/2018

Personale Intervenuto: Marco Gallerini (gallerini)

Dati Identificativi del Titolare del trattamento:

ISTITUTO COMPRENSIVO ANTONELLI
Via Vescovo Bovio 7/9
Bellinzago Novarese
noic813002@istruzione.it

Descrizione Infrastruttura Informatica oggetto del sopralluogo/ Intervento:
Segreteria e Server

In considerazione del fatto che, mediante l’impiego delle apparecchiature informatiche costituenti l’infrastruttura descritta in copertina, si effettua trattamento di dati personali, si procede alla verifica puntuale delle seguenti modalità tecniche :

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

1.1.1 Implementare un inventario delle risorse attive correlato a quello ABSC 1.4: Inventario di tutte le risorse collegate all'infrastruttura depositato in segretria

1.3.1 Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.: Si

1.4.1 Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.: Registrazione e aggiornamento manuale

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

2.1.1 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.: Elenco depositato in segreteria controllo manuale

2.3.1 Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.: Scansione dei sistemi per la rilevazione di software non autorizzato manuale con cadenza semestrale

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

3.1.1 Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.: L'amministratore di rete ha definito misure standard sicure per ogni sistemi operativi

3.2.1 Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.: Le configurazioni standard sono definite da active directory

3.2.2 Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.: In caso di di ripristino tutti i sistemi saranno ripristinati secondo le misure di sicurezza standard

3.3.1 Le immagini d'installazione devono essere memorizzate offline.: Si

3.4.1 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).: Si

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

4.1.1 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.: Sistema di ricerca vulnerabilità sistema operativo e antivirus effettuato almeno semestralmente dall'amministratore di rete.

4.4.1 Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.: Si

4.5.1 Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.: Si

4.5.2 Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.: Al momento non presenti nell'infrastruttura

4.7.1 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.: Gestione dell'amministratore di rete il quale controllerà periodicamente il corretto aggiornamento delle criticità.

4.8.1 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.).: Verra? aggiornato il DPP (documento programmazione privacy) per la gestione del rischio informatico dal consulente privacy

4.8.2 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.: Le priorità sull'adeguamento alle vulnerabilità saranno disposte dall'amministratore di rete in collaborazione con l'amministratore di sistema.

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

5.1.1 Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.: I privilegi di amministratore sono limitati ad utenti con requisiti tecnici appropriati.

5.1.2 Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.: Implementazione a breve.

5.2.1 Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.: Inventario gestito da active directory.

5.3.1 Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.: No

5.7.1 Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).: L'autenticazione viene gestita da active directory con 8 caratteri e numeri speciali (almeno una maiuscola-una minuscola e /o numeri e simboli).

5.7.3 Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).: Gli utenti modificano le proprie password entro i 120 giorni.

5.7.4 Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).: Gestito da active directory

5.10.1 Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.: La distinzione tra utente privilegiate e non privilegiate è gestita da active directory

5.10.2 Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.: Tutte le utenze sono riconducibili alla persona fisica.

5.10.3 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.: L?utenza amministrativa generica sarà mantenuta esclusivamente dall?amministratore di rete

5.11.1 Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.: Password utenze conservate dal responsabile del trattamento dei dati sensibili.

5.11.2 Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano

adeguatamente protette.: Si

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

8.1.1 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.: Sistema di controllo virus locale

8.1.2 Installare su tutti i dispositivi firewall ed IPS personali.: Tutti i dispositivi hanno attivo sistema firewall integrato di Windows.

8.3.1 Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.: Disposizione impartita dalla direzione.

8.7.1 Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.: Si

8.7.2 Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.: Si

8.7.3 Disattivare l'apertura automatica dei messaggi di posta elettronica.: Si

8.7.4 Disattivare l'anteprima automatica dei contenuti dei file.: Si

8.8.1 Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.: Impostazione gestita da antivirus

8.9.1 Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.: Filtro posta elettronica da sistema antivirus.

8.9.2 Filtrare il contenuto del traffico web.: Implementazione a breve

8.9.3 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).: Filtro Download e smtp gestito da firewall.

ABSC 10 (CSC 10): COPIE DI SICUREZZA

10.1.1 Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.: Il backup di tutti i dati viene effettuato almeno una volta a settimana.

10.3.1 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.: Implementazione a breve

10.4.1 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.: Tutti i backup locali o cloud sono protetti da password e non sono accessibili dalla rete lan.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

13.1.1 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: Sono gestite cartelle sul server con permition differenti attraverso police group su ogni cartella distinguendo dati sensibili da dati riservati.

13.8.1 Bloccare il traffico da e verso url presenti in una blacklist.: Implementazione a breve

In seguito all’analisi eseguita è emerso che l’infrastruttura informatica ove avviene il trattamento dei dati personali oggetto del presente accertamento alle prescrizioni di cui agli Artt. 33 ss. del D.Lgs. 196/2003 (Codice della Privacy).

Data: 22/03/2018

Tecnico: Marco Gallerini (gallerini)

Nome Cognome Personale Intervenuto:
N° Documento:

Studio AG.I.COM. S.r.l.
Via XXV Aprile 12 , 20070 San Zenone al Lambro MI
Tel. 02.98.60.13.24 Fax. 02.700.52.71.80 info@agicomstudio.it
capitale sociale i.v.