Città di
Rivalta
di Torino

ALLEGATO 15
alla deliberazione della Giunta Comunale
n. 264 del 30/12/2021

Misure minime di sicurezza

Prot. 35845 del 28/12/2017

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	IMPLEMENTATO da CSI PIEMONTE **PC** L'inventario di tutte le risorse (attive e disponibili) è gestito tramite il modulo REMEDY ASSET, gestito da CSI, dove viene conservata l'informazione dei nome assegnatario, host , ufficio , direzione di appartenenza, caratteristiche HW, etc **SERVER E FIREWALL DI FRONTIERA, FIREWALL PERIMETRALI , ROUTER WAN** L'inventario delle risorse è a carico del CSI Piemonte ed è implementato nel CMDB aziendale (CMDbuild) **Tutte le parte relative all'elettronica di rete sono inventariate dal Comune**
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	IMPLEMENTATO da CSI PIEMONTE Viene utilizzato REMEDY ASSET e CMDBuild (vedi punto precedente)
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	NON IMPLEMENTATO in automatico da CSI PIEMONTE Periodici controlli manuali
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	NON IMPLEMENTATO
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	NON APPLICABILE Non si fa uso di 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.	NON APPLICABILE Non si fa uso di DHCP
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	IMPLEMENTATO da CSI PIEMONTE Quando un nuovo PC o periferiche viene acquisito , l'Ente richiede l'inserimento in remedy asset del nuovo hardware acquistato e a chi è stato assegnato.

1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	NON IMPLEMENTATO
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.	IMPLEMENTATO da CSI PIEMONTE Nell'inventario è presente se assegnato l'IP statico di riferimento. Nell'inventario CSI non sono presenti le apparecchiature di rete. Per le pdl in remedy asset è stato inserito l'ip dove fornito dall'ente. E' possibile utilizzare remedy asset per registrare i dispositivi connessi via rete.
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.	IMPLEMENTATO da CSI PIEMONTE In remedy asset è possibile gestite tali informazioni. Per le pdl attualmente inserite le informazioni sono già presenti.
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.	IMPLEMENTATO da CSI PIEMONTE Si possono inserire all'interno dell'asset, ad oggi sono presenti i pc portatili, tablet, hard disk esterni.
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.	NON IMPLEMENTATO
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	NON IMPLEMENTATO L'autenticazione avviene tramite uso di credenziali di domino

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.	La white list dei software autorizzati sui PC è implementata tramite excel. La white list degli applicativi presenti sui server è a carico del CSI Piemonte L'elenco dei middleware è implementato tramite excel (in corso porting su DB) è gestito da CSI PIEMONTE

					L’elenco dei software realizzati da CSI è disponibile sul servizio Anagrafica Prodotti Sui PC non sono assegnati agli utenti i profili di amministrazione, tranne per utenti censiti e autorizzati dall’ENTE Sui server di produzione l’accesso è consentito unicamente ai sistemisti autorizzati e viene applicata la metodologia DEVOPS con creazione ed esecuzione di ricette automatizzate
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.	NON IMPLEMENTATO
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).	NON APPLICABILE
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	NON IMPLEMENTATO
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	PARZIALMENTE IMPLEMENTATO da CSI PIEMONTE Il servizio di scansione viene realizzato tramite OCS e verificato manualmente con l’ENTE
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.	L’inventario degli applicativi è implementato tramite excel.
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.	NON IMPLEMENTATO

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.	NON APPLICABILE

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.	IMPLEMENTATO da CSI PIEMONTE Per quanto riguarda la gestone dei PC e server in cloud, vengono utilizzate immagini standard e seguite operazioni standard di configurazione
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.	IMPLEMENTATO da CSI PIEMONTE Procedura standard a carico del CSI. Per le pdl le attività vengono svolte se richieste dall'ente, le patch del s.o. per le pdl vengono gestite dai sistemi centrali in datacenter.
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.	IMPLEMENTATO da CSI PIEMONTE Procedura standard a carico del CSI. Per le pdl l'attività non è prevista..
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	IMPLEMENTATO da CSI PIEMONTE Si è stata definita una policy (configurazione) standard per i middleware utilizzati in azienda (Database, Web server, Applications Server, etc) in accordo con L'ENTE
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	IMPLEMENTATO da CSI PIEMONTE Si il sistema compromesso viene ripristinato utilizzando la configurazione standard con ripristino manuale dell'immagine
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	IMPLEMENTATO da CSI PIEMONTE

					Si , le modifiche rilevanti alle configurazioni standard vengono esaminate dal Responsabile dei sistemi informativi , insieme al Responsabile della Sicurezza ed il gestore Datacenter.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	IMPLEMENTATO da CSI PIEMONTE Le immagini vengono conservate in ambiente separato (NAS) e in modalità protetta.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	IMPLEMENTATO Le immagini vengono conservate in ambiente separato (NAS) e in modalità protetta
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).	IMPLEMENTATO da CSI PIEMONTE PC La gestione remota avviene tramite appositi strumenti (Damware di Solarwinds) SERVER e APPARATI DI RETE La gestione remota avviene sempre tramite connessioni SSH e RDP
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.	NON IMPLEMENTATO
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.	NON IMPLEMENTATO
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.	NON IMPLEMENTATO
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	PC NON IMPLEMENTATO PARZIALMENTE IMPLEMENTATO da CSI PIEMONTE SERVER WEB Periodicamente viene eseguita una scansione dei permessi di tutti i file presenti sui server esposti in internet per la verifica ed il controllo di variazioni (modifica a 777)

3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	NON IMPLEMENTATO
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	NON IMPLEMENTATO

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.	PARZIALMENTE IMPLEMENTATO Se viene identificata una modifica di file di configurazione vien attivato un processo manuale di verifica della causa e viene ricercato , tramite script, la presenza di altri file modificati
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	IMPLEMENTATO da CSI PIEMONTE: Per le PDL è attivato l'antivirus. Per gli altri sistemi nel contratto di gestione non sono al momento inseriti i test di vulnerabilità
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).	NON IMPLEMENTATO
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	NON IMPLEMENTATO
4	2	2	S	[redacted]	
4	2	3	S		
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.	NON IMPLEMENTATO

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.	NON IMPLEMENTATO
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 comune sta valutando l'implementazione al termine del procedimento di outsourcing incorso con CSI PIEMONTE
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	IMPLEMENTATO da CSI PIEMONTE Il CSI Piemonte è registrato al servizio di alerting del CERT-PA, Inoltre riceve aggiornamenti dal CNAIPIC
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	IMPLEMENTATO da CSI PIEMONTE PC Il Sistema operativo e le principali applicazioni delle postazioni di lavoro sono aggiornate automaticamente tramite WSUS di Microsoft SERVER Prima dell'installazione delle patch vengono effettuati dei test di compatibilità dai fornitori
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.	NON APPLICABILE
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.	NON IMPLEMENTATO
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.	Il comune sta valutando l'implementazione al termine del procedimento di outsourcing in corso con CSI PIEMONTE
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.	NON IMPLEMENTATO

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.).	Il comune sta valutando l'implementazione al termine del procedimento di outsourcing in corso con CSI PIEMONTE
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.	IMPLEMENTATO da CSI PIEMONTE Il CSI adotta processo standard di aggiornamento patch per le PDL
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.	IMPLEMENTATO da CSI PIEMONTE Implementato per le PDL e per i sistemi operativi della parte server gestita da CSI
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.	NON IMPLEMENTATO

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.	IMPLEMENTATO da CSI PIEMONTE Utenti non hanno privilegi di amministratore e non possono installare componenti sul cloud. Attività di amministrazione è limitata a responsabile CED ed ai sistemisti CSI. Per le pdl i privilegi di amministrazione sono assegnati ai tecnici pdl e al responsabile del CED.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	IMPLEMENTATO da CSI PIEMONTE Attivita di amministrazione è limitata a responsabile CED, ai sistemisti CSI, ai tecnici di pdl per le pdl.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	IMPLEMENTATO da CSI PIEMONTE
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	IMPLEMENTATO da CSI PIEMONTE

					I log degli amministratori di sistema vengono conservati per un periodo non inferiore a 6 mesi all'interno del repository della piattaforma SIEM. Periodicamente vengono effettuati gli audit di analisi delle anomalie di comportamento (Provvedimento del 2008 del Garante Privacy)
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	IMPLEMENTATO da CSI PIEMONTE Tutti gli amministratori di sistema CSI sono nominati ai fini provvedimento 2008 del Garante Privacy e l'elenco è pubblicato sulla intranet aziendale
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	NON IMPLEMENTATO
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.	IMPLEMENTATO da CSI PIEMONTE Tramite policy di dominio o processo formalizzato per PDL.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	IMPLEMENTATO da CSI PIEMONTE PC Viene generato un evento nel log dell'event del Dominio
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	NON IMPLEMENTATO
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	NON IMPLEMENTATO
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	IMPLEMENTATO da CSI PIEMONTE PC Si i tentativi vengono tracciati nell'event viewer del dominio SERVER IMPLEMENTATO Tracciati nel log di accesso al portale Cloud
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.	NON IMPLEMENTATO

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).	IMPLEMENTATO da CSI PIEMONTE Le password rispondono a criteri di complessità (uguali o superiori a 8 caratteri , diversa dalle 4 precedenti ,con caratteri speciali , numerici ed almeno una lettera maiuscola) definite a livello di dominio IMPLEMENTATO dal comune per i server in ambiente CLOUD
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	IMPLEMENTATO da CSI PIEMONTE Il sistema non permette la creazione di password non rispondenti alle policy definite al punto precedente.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	IMPLEMENTATO da CSI PIEMONTE PC Le password vengono sostituite ogni tre mesi
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	IMPLEMENTATO da CSI PIEMONTE PC Il sistema tiene memoria delle ultime 4 password inserite. Non è possibile ripristinare una precedente password se questa compresa nell'history.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	NON IMPLEMENTATO
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	NON IMPLEMENTATO
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.	IMPLEMENTATO da CSI PIEMONTE Gli amministratori UNIX si autenticano ad un primo servizio di identità e solo successivamente si possono collegare ai server abilitati in base al loro profilo Sui PC non è implementata
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.	IMPLEMENTATA da CSI PIEMONTE Le PDL degli amministratori di sistema del CSI si trovano su una sottorete di gestione separata
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	IMPLEMENTATA da CSI PIEMONTE

5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	IMPLEMENTATO da CSI PIEMONTE Tutte le utenze sono riconducibili alla persona che detiene i privilegi, tranne le utenze di servizio (vedi es. ANTIVIRUS)
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.	IMPLEMENTATO da CSI PIEMONTE Il CSI ha realizzato una soluzione custom di gestione delle profilazioni di accesso al sistema . In corso valutazione adozione strumento commerciale di gestione accessi privilegiati
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).	IMPLEMENTATO da CSI PIEMONTE
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	IMPLEMENTATO da CSI PIEMONTE Tutti gli amministratori CSI hanno ricevuto nomina di incarico con relativa assunzione di responsabilità
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	NON APPLICABILE Non vengono utilizzati certificati

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.	IMPLEMENTATO da CSI PIEMONTE Sui server Windows e sulle PDL è presente la versione di antivirus McAfee End Point Security 10.5.1
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Tutti i PC sono comunque in classe 10. , protetti da firewall e IDP/IPS perimetrale.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	IMPLEMENTATO da CSI PIEMONTE PC Tutti gli eventi generati dall'antivirus sono inviati al repository centrale (consolle EPO)
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.	IMPLEMENTATO da CSI PIEMONTE Non è possibile , come definito in policy Windows, cambiare la configurazione degli antivirus

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.	IMPLEMENTATO da CSI PIEMONTE E possibile dalla console EPO McAfee forzare gli aggiornamenti
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	IMPLEMENTATO da CSI PIEMONTE E' stata predisposta una send box separata dalla rete , per la verifica dei malware
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	I dispositivi sono separati dalla rete comunale tramite uso di firewall
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	NON IMPLEMENTATO
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.	NON IMPLEMENTATO
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	NON IMPLEMENTATO
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.	IMPLEMENTATO da CSI PIEMONTE In azienda è adottato il WEB Content Gateway di Force Point
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	NON IMPLEMENTATO
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	IMPLEMENTATO da CSI PIEMONTE Tramite Web Content Gateway.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	IMPLEMENTATO da CSI PIEMONTE Tramite policy di Dominio
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	PARZIALMENTE IMPLEMENTATO Dipendente dalla versione di office automation installato
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	IMPLEMENTATO da CSI PIEMONTE L'apertura dei messaggi di posta avviene solo a seguito di autenticazione . Le notifiche automatiche sono bloccate.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	IMPLEMENTATO da CSI PIEMONTE

					Il Sistema di posta adottato Unified Communicaton non permette anteprima automatica dei contenuti dei file
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	IMPLEMENTATA da CSI PIEMONTE Tramite policy dell'antivirus, vengono scansionati i file presenti sulla chiavetta. Sono disabilitati gli autorun ed i setup automatici.
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.	IMPLEMENTATO da CSI PIEMONTE La posta aziendale viene protetta da filtri antispam e ani -fishing. E in corso di adozione standard DMARC
8	9	2	M	Filtrare il contenuto del traffico web.	IMPLEMENTATO da CSI PIEMONTE Il contenuto è filtrato da WEB Content Gateway di Forcepoint
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).	IMPLEMENTATO da CSI PIEMONTE Il sistema di posta UC Communication è protetto con l'utilizzo di filtri antispam e anti-malware. E sono definite le estensioni pericolose (es. EXE, CAB)
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	NON IMPLEMENTATO
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.	NON IMPLEMENTATO

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.	IMPLEMENTATO da CSI PIEMONTE PC Come policy aziendale è data indicazione che i file di lavoro devono essere salvati su gli share di rete. Per cui non viene eseguito il backup dei singoli PC. SERVER Il backup è effettuato giornalmente
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.	IMPLEMENTATO da CSI PIEMONTE I backup vengono eseguiti tramite la piattaforma SIMPANA

10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	NON IMPLEMENTATO
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	NON IMPLEMENTATO
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.	IMPLEMENTATO da CSI PIEMONTE Simpana e Veeam (strumenti di Backup utilizzati) cifrano le copie. La codifica viene effettuata sulla rete locale (Rupar)
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.	IMPLEMENTATO da CSI PIEMONTE Sì i backup sono conservati in palazzina fisicamente separata dal datacente

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	Il comune sta valutando l'implementazione al termine del procedimento di outsourcing in corso con CSI PIEMONTE
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	NON IMPLEMENTATO
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 exfiltrazione di informazioni.	NON IMPLEMENTATO
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.	NON IMPLEMENTATO

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.	NON IMPLEMENTATO
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.	NON IMPLEMENTATO
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.	NON IMPLEMENTATO
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	IMPLEMENTATO
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	NON IMPLEMENTATO
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	IMPLEMENTATO da CSI PIEMONTE Tramite web content Gateway
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.	NON IMPLEMENTATO