C O M U N E di U R B I S A G L I A
Provincia Di Macerata

P.O.n° 2" Edilizia ed Urbanistica

Oggetto : circolare AgID del 18 aprile 2017, n.2-2017 sulle misure minime di sicurezza ICT per per le pubbliche amministrazioni Dashboard Bb/servizi /agent]

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
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.	Mantengono un inventario del software installato tramite la Dashboard Halley, le Workstation ed i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity

					Cloud White Box Ced Remoto Antivirus Web Protection Contenet Filtering
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.	Registrano le versioni del sistema operativo e le applicazioni installate, le Workstation ed i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Cloud White Box Ced Remoto Antivirus Web Protection Contenet Filtering I servizi White Box e Ced Remoto, invece, registrano anche il livello di patch.

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.	Utilizzano le configurazioni standard per la protezione dei sistemi operativi le Workstation ed i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Disaster Recovery Cloud White Box Ced Remoto
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.	Hanno implementato l'hardening per eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Cloud
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Hanno una configurazione standard definita i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service

					Server Continuity Cloud
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Hanno una configurazione standard definita i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Cloud White Box
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).	Ricevono dati nelle nostre dashboard in modo sicuro, I Server e le Workstation che hanno attivo uno dei seguenti servizi (per i server tramite tunnel crittografato ssh mentre per le workstation tramite protocollo https): Black Box Full Service Server Continuity Disaster Recovery Cloud White Box Ced Remoto Antivirus Web Protection Contenet Filtering

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.	Eseguono una scansione delle vulnerabilità ed installano le patch critiche ed importanti dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Eseguono una scansione delle vulnerabilità ed installano le patch critiche ed importanti dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Hanno attivo il log delle scansioni vulnerabilità le Workstation con attivo il servizio di: White Box Ced Remoto
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Registrano le attività dei sistemi di scanning delle vulnerabilità le Workstation con attivo il servizio di: White Box Ced Remoto

4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Vengono regolarmente aggiornati con le più rilevanti vulnerabilità di sicurezza dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto
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	Sono in grado di riconoscere le patch critiche ed importanti dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Installano le patch critiche ed importanti dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto
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.	La nostra Dashboard riceve un alert se una patch critica ed importante dei prodotti Microsoft fallisce durante un'installazione per le Workstation con attivo il servizio di: White Box Ced Remoto
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.	Eseguono una scansione delle vulnerabilità ed installano le patch critiche e importanti dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto

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.	Limitano gli accessi ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Cloud Storage dati non Halley Servizio Firewall Timbrature Sicure
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Registrano gli accessi effettuati i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Cloud

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.	Vengono sostituite le password standard di amministratore con password complesse i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Servizio Firewall Timbrature Sicure Storage dati non Halley
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Tracciano i log di tentativi di accesso e le registrano sulla nostra Dashboard i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Hanno password amministrative complesse i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Servizio Firewall Timbrature Sicure Storage dati non Halley
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Vengono sostituite con sufficiente frequenza le password dei Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity
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.	Le credenziali amministrative anonime vengono utilizzate per provvedere alla manutenzione ordinaria e/o straordinaria dei Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Conservano le credenziali amministrative in modo da garantirne disponibilità e riservatezza i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Servizio Firewall Timbrature Sicure Storage dati non Halle Disaster recovery

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.	Bloccano l'esecuzione di malware e sono mantenuti sempre aggiornati i Server e le Workstation che hanno attivo uno dei seguenti servizi: Servizio Antivirus
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Hanno sempre il firewall di sistema i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity White Box Ced Remoto
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.	Il servizio antivirus è gestito centralmente tramite la nostra Dashboard e non è consentito agli utenti di alterarne la configurazione per i Server e le Workstation che hanno attivo il servizio: Servizio 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.	Per i Server e le Workstation che hanno attivo il Servizio Antivirus è possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo e 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.	Viene effettuata un' analisi dei potenziali malware in un'infrastruttura dedicata, basata sul cloud i Server e le Workstation che hanno attivo il servizio: Servizio Antivirus
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.	Usano strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host i Server e le Workstation che hanno attivo il servizio: Servizio Web Protection
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Bloccano siti con cattiva reputazione i Server e le Workstation che hanno attivo il servizio: Servizio Web Protection
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Eseguono una scansione anti-malware dei supporti rimuovibili al momento della loro connessione i Server e le Workstation che hanno attivo il servizio:

					Servizio Antivirus
8	9	2	M	Filtrare il contenuto del traffico web.	Filtrano il contenuto del traffico web i Server e le Workstation che hanno attivo il servizio: Servizio Web Protection

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.	Effettuano una copia locale quotidiana mantenendo uno storico di 60 giorni e dove previsto la stessa copia viene ridondata su storage i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Cloud Effettuano una sicronia del database in tempo reale mantenendo i dati sempre aggiornati tra server di produzione e server Continuity i Server che hanno attivo il servizio: Server Continuity Effettuano una copia a Roma e Trento crittografando i dati e mantenendo uno storico di 60 giorni i Server che hanno attivo il servizio: Disaster Recovery Tutte queste copie mantengono le informazioni strettamente necessarie per il completo ripristino del sistema. Copiano giornalmente le cartelle condivise scelte dal cliente mantenendo uno storico di 60 giorni le Workstation che hanno attivo il servizio: Servizio Storage Oltre a copiare giornalmente le cartelle condivise scelte dal cliente mantenendo uno storico di 60 giorni effettuano una copia a Roma e Trento crittografando i dati e mantenendo uno storico di 60 giorni delle cartelle scelte per il Disaster recovery le Workstation che hanno attivo il servizio: Disaster recovery dati non halley

10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Viene verificata periodicamente l'utilizzabilità delle copie mediante ripristino di prova sulle Workstation e i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Disaster Recovery Cloud
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.	Effettuano una copia a Roma e Trento crittografando i dati e mantenendo uno storico di 60 giorni i Server che hanno attivo il servizio: Disaster Recovery Tutte queste copie mantengono le informazioni strettamente necessarie per il completo ripristino del sistema
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.	Effettuano una copia a Roma e Trento crittografando i dati e mantenendo uno storico di 60 giorni rendendoli inaccessibili dal sistema i Server che hanno attivo il servizio: Disaster Recovery Tutte queste copie mantengono le informazioni strettamente necessarie per il completo ripristino del sistema

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Bloccano il traffico da e verso url presenti in una blacklist o in categorie concordate le Workstation e i Server che hanno attivo il servizio: Content Filtering

Il Responsabile della Posizione Organizzativa n° 2
Edilizia ed Urbanistica
(geom. Massimo Rastelli)